IP ルーティング：BGP コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

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/

目 次

第 1 章 最初にお読みください 1

第 2 章 Cisco BGP 概要 3

機能情報の確認 3

Cisco BGP の前提条件 4

Cisco BGP の制約事項 4

Cisco BGP に関する情報 4

BGP バージョン 4 4

BGP バージョン 4 機能の概要 5

BGP 自律システム 6

BGP 自律システム番号の形式 7

クラスレス ドメイン間ルーティング 10

マルチプロトコル BGP 10

BGP に対しマルチプロトコル BGP を使用する利点 11

IP マルチキャストのマルチプロトコル BGP 拡張 11

NLRI コンフィギュレーション CLI 13

Cisco BGP アドレス ファミリ モデル 14

IPv4 アドレス ファミリ 17

IPv6 アドレス ファミリ 17

CLNS アドレス ファミリ 17

VPNv4 アドレス ファミリ 18

L2VPN アドレス ファミリ 19

BGP CLI 削除の考慮事項 20

その他の参考資料 21

Cisco BGP 概要の機能情報 23

第 3 章 BGP 4 25

機能情報の確認 25

BGP 4 に関する情報 25

BGP バージョン 4 機能の概要 25

BGP ルータ ID 27

BGP スピーカーとピア関係 27

BGP ピア セッションの確立 27

BGP セッションのリセット 28

BGP ルート集約 29

BGP ルート集約の AS_SET 情報生成 30

ルーティング ポリシーの変更管理 30

BGP ピア グループ 32

BGP バックドア ルート 32

BGP 4 の設定方法 33

BGP ルーティング プロセスの設定 33

トラブルシューティングのヒント 37

BGP ピアの設定 37

トラブルシューティングのヒント 40

IPv4 VRF アドレス ファミリ用に BGP ピアを設定 40

トラブルシューティングのヒント 44

BGP ピアのカスタマイズ 45

再配布を使用した BGP コンフィギュレーション コマンドの削除 50

基本的な BGP のモニタリングとメンテナンス 52

ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定 52

基本 BGP 情報のリセットと表示 55

BGP を使用したルート プレフィックスの集約 57

BGP へのスタティック集約ルートの再配布 57

BGP を使用した条件付き集約ルートの設定 58

BGP を使用した集約ルートのアドバタイズメントの抑制および抑制解除 60

BGP ルートの条件付きアドバタイズ 61
BGP ルートの開始 64
BGP を使用したデフォルト ルートのアドバタイジング 65
バックドア ルートを使用した BGP ルートの開始 66
BGP ピア グループの設定 68
BGP 4 の設定例 70
例：BGP プロセスの設定とピアのカスタマイズ 70
例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除 71
例：BGP ソフト リセット 72
例：基本 BGP 情報のリセットおよび表示 72
例：BGP を使用したプレフィックスの集約 74
例：BGP ピア グループの設定 75
その他の参考資料 76
BGP 4 の機能情報 77

第 4 章 基本 BGP ネットワークの設定 79
機能情報の確認 79
基本 BGP ネットワーク設定の前提条件 80
基本 BGP ネットワーク設定の制約事項 80
基本 BGP ネットワーク設定の概要 80
BGP バージョン 4 80
BGP ルータ ID 80
BGP スピーカーとピア関係 81
BGP 自律システム番号の形式 81
シスコが採用している 4 バイト自律システム番号 84
BGP ピア セッションの確立 85
シスコが採用している BGP グローバル コマンドとアドレス ファミリ コンフィギュレーション コマンド 86
BGP セッションのリセット 87
BGP ルート集約 88
BGP 集約ルートの AS_SET 情報生成 89

ルーティング ポリシーの変更管理 89
条件付き BGP ルートの挿入 91
BGP ピア グループ 92
BGP バックドア ルート 92
ピア グループおよび BGP アップデート メッセージ 93
BGP アップデート グループ 93
BGP ダイナミック アップデート グループのコンフィギュレーション 94
BGP Peer テンプレート 94
ピア テンプレートでの継承 95
ピア セッション テンプレート 96
ピア ポリシー テンプレート 97
IPv4 アドレス ファミリの下での BGP IPv6 ネイバーのアクティブ化 99
基本 BGP ネットワークの設定方法 99
BGP ルーティング プロセスの設定 100
トラブルシューティングのヒント 103
BGP ピアの設定 103
トラブルシューティングのヒント 107
次の作業 107
BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定 107
トラブルシューティングのヒント 110
4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更 110
IPv4 VRF アドレス ファミリ用に BGP ピアを設定 114
トラブルシューティングのヒント 118
BGP ピアのカスタマイズ 118
再配布を使用した BGP コンフィギュレーション コマンドの削除 123
基本的な BGP のモニタリングとメンテナンス 125
ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定 126
基本 BGP 情報のリセットと表示 129
BGP を使用したルート プレフィックスの集約 130
BGP へのスタティック集約ルートの再配布 131

BGP を使用した条件付き集約ルートの設定 132
BGP を使用した集約ルートのアドバタイズメントの抑制および抑制解除 133
BGP を使用した非アクティブなルート アドバタイズメントの抑制 135
BGP ルートの条件付きアドバタイズ 137
BGP ルートの開始 140
BGP を使用したデフォルト ルートのアドバタイジング 141
BGP ルートの条件付き挿入 142
バックドア ルートを使用した BGP ルートの開始 147
BGP ピア グループの設定 148
ピア セッション テンプレートの設定 150
基本的なピア セッション テンプレートの設定 151
inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定 153
neighbor inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定 155
ピア ポリシー テンプレートの設定 157
基本的なピア ポリシー テンプレートの設定 157
inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定 159
neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定 162
BGP ダイナミック アップデート グループのモニタリングとメンテナンス 165
トラブルシューティングのヒント 166
基本 BGP ネットワークの設定例 166
例：BGP プロセスの設定とピアのカスタマイズ 166
例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定 167
例：4 バイトの BGP 自律システム番号を使用した VRF および拡張コミュニティの設定 170
例：NLRI から AFI へのコンフィギュレーション 171
例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除 173
例：BGP ソフト リセット 174
例：4 バイト自律システム番号を使用した BGP ピアのリセット 175
例：基本 BGP 情報のリセットおよび表示 176
例：BGP を使用したプレフィックスの集約 177

例：BGP ピア グループの設定 178
例：ピア セッション テンプレートの設定 179
例：ピア ポリシー テンプレートの設定 179
例：BGP ダイナミック アップデート ピア グループのモニタリングおよびメンテナンス 180
次の作業 181
その他の参考資料 182
基本 BGP ネットワーク設定の機能情報 184

第 5 章 BGP 4 ソフト構成 187
機能情報の確認 187
BGP 4 ソフト構成に関する情報 187
BGP セッションのリセット 187
BGP 4 ソフト構成の設定方法 188
ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定 188
BGP 4 ソフト構成の設定例 192
例：BGP ソフト リセット 192
その他の参考資料 193
BGP 4 ソフト構成の機能情報 193

第 6 章 4 バイト ASN に対する BGP サポート 195
機能情報の確認 195
4 バイト ASN に対する BGP サポートに関する情報 196
BGP 自律システム番号の形式 196
シスコが採用している 4 バイト自律システム番号 198
4 バイト ASN に対する BGP サポートの設定方法 199
BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定 199
トラブルシューティングのヒント 202
4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更 202
4 バイト ASN に対する BGP サポートの設定例 207

例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定 207
例：4 バイトの BGP 自律システム番号を使用した VRF および拡張コミュニティの設定 210
4 バイト ASN に対する BGP サポートに関する追加情報 211
4 バイト ASN に対する BGP サポートの機能情報 212

第 7 章 IPv6 ルーティング：マルチプロトコル BGP for IPv6 拡張 215
機能情報の確認 215
IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張に関する情報 215
Multiprotocol BGP Extensions for IPv6 215
マルチプロトコル BGP for IPv6 の設定方法 216
IPv6 BGP ルーティング プロセスおよび BGP ルータ ID の設定 216
2 つのピア間での IPv6 マルチプロトコル BGP の設定 217
IPv6 BGP ピア間での IPv4 ルートのアドバタイズ 219
外部 BGP ピアのクリア 221
BGP IPv6 アドミニストレーティブ ディスタンスの設定 221
マルチプロトコル BGP for IPv6 の設定例 222
例：BGP プロセス、BGP ルータ ID、IPv6 マルチプロトコル BGP ピアの設定 222
例：IPv6 マルチプロトコル BGP ピア グループの設定 222
例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ 223
例：IPv6 マルチプロトコル BGP プレフィックスのルート マップの設定 223
例：IPv6 マルチプロトコル BGP へのプレフィックスの再配布 223
例：IPv6 ピア間での IPv4 ルートのアドバタイズ 223
その他の参考資料 224
IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張の機能情報 225

第 8 章 IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリング 227
機能情報の確認 227
IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングに関する情報 228
リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアリング 228

IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定方法 228
Configuring an IPv6 Multiprotocol BGP Peer Using a Link-Local Address 228
IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定例 233
例：リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定 233
その他の参考資料 234
IPv6 ルーティング マルチプロトコル BGP リンクローカル アドレス ピアリングの機能情報 235

第 9 章 IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポート 237
機能情報の確認 237
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する情報 238
IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 238
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの実装方法 239
IPv6 ピア グループでマルチキャスト BGP ルーティングを実行するための設定 239
IPv6 マルチプロトコル BGP へのルートのアドバタイズ 240
IPv6 マルチプロトコル BGP へのプレフィックスの再配布 242
BGP のアドミニストレーティブ ディスタンスの割り当て 244
IPv6 マルチキャスト BGP の変換アップデートの生成 245
IPv6 BGP セッションのリセット 246
外部 BGP ピアのクリア 246
IPv6 BGP ルート減衰情報のクリア 247
IPv6 BGP フラップ統計情報のクリア 247
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの設定例 248
例：IPv6 マルチプロトコル BGP ピア グループの設定 248
例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ 248
例：IPv6 マルチプロトコル BGP へのプレフィックスの再配布 249
例：IPv6 マルチキャスト BGP の変換アップデートの生成 249
その他の参考資料 249

IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する機能情報 250

第 10 章 CLNS に対するマルチプロトコル BGP（MP-BGP）サポートの設定 251

機能情報の確認 251

CLNS に対する MP-BGP サポートの設定に関する制約事項 252

CLNS に対する MP-BGP サポートの設定の概要 252

アドレス ファミリ ルーティング情報 252

CLNS に対する MP-BGP サポートの設計機能 252

汎用 BGP CLNS ネットワーク トポロジ 253

DCN ネットワーク トポロジ 254

CLNS に対する MP-BGP サポートの利点 256

CLNS に対する MP-BGP サポートの設定方法 257

CLNS をサポートするための BGP ネイバーの設定とアクティブ化 257

IS-IS ルーティング プロセスの設定 258

BGP ネイバーに接続するインターフェイスの設定 260

ローカル OSI ルーティング ドメインと接続されているインターフェイスの設定 262

ネットワーキング プレフィックスのアドバタイジング 263

BGP から IS-IS へのルートの再配布 265

IS-IS から BGP への再配布ルート 267

BGP ピア グループおよびルート リフレクタの設定 268

NSAP プレフィックスに基づくインバウンド ルートのフィルタリング 270

NSAP プレフィックスに基づくアウトバウンド BGP アップデートのフィルタリング 272

ネイバー ルーティング ドメインのデフォルト ルートの送信 274

CLNS に対する MP-BGP サポートの確認 276

CLNS に対する MP-BGP サポートのトラブルシューティング 278

CLNS に対する MP-BGP サポートの設定例 279

例：CLNS をサポートするための BGP ネイバーの設定とアクティブ化 279

例：IS-IS ルーティング プロセスの設定 280

インターフェイスの設定の例 280

ネットワーキング プレフィックスのアドバタイジングの例 280

例：BGP から IS-IS へのルートの再配布 281
例：IS-IS から BGP への再配布ルート 281
BGP ピア グループおよびルート リフレクタの設定の例 282
NSAP プレフィックスに基づくインバウンド ルートのフィルタ処理の例 282
例：NSAP プレフィックスに基づくアウトバウンド BGP アップデートのフィルタ処理 282
例：デフォルト ルートの発信およびアウトバウンド ルート フィルタリング 283
CLNS に対する MP-BGP サポートの実装の例 283
自律システム AS65101 284
自律システム AS65202 285
自律システム AS65303 286
自律システム AS65404 287
その他の参考資料 289
CLNS に対する MP-BGP サポートの設定に関する機能情報 289
用語集 292

第 11 章 **BGP IPv6 アドミニストレーティブ ディスタンス 295**
BGP IPv6 アドミニストレーティブ ディスタンスの概要 295
BGP IPv6 アドミニストレーティブ ディスタンスの利点 295
BGP IPv6 アドミニストレーティブ ディスタンスの設定 296
BGP アドミニストレーティブ ディスタンス設定の確認 297
BGP IPv6 アドミニストレーティブ ディスタンスに関する追加情報 298
BGP IPv6 アドミニストレーティブ ディスタンスの機能情報 298

第 12 章 **外部BGP を使用したサービスプロバイダーとの接続 301**
機能情報の確認 301
外部 BGP を使用したサービス プロバイダーとの接続の前提条件 302
外部BGP を使用したサービスプロバイダーとの接続の制約事項 302
外部 BGP を使用したサービス プロバイダーとの接続の概要 302
外部 BGP ピアリング 302
BGP 自律システム番号の形式 304

BGP 属性 307
マルチホーミング 309
MED 属性 309
中継トラフィックと非中継トラフィック 310
BGP ポリシー設定 310
BGP COMMUNITIES 属性 311
拡張コミュニティ 312
拡張コミュニティ リスト 313
アドミニストレーティブ ディスタンス 313
BGP ルート マップ ポリシー リスト 314
外部 BGP を使用したサービス プロバイダーとの接続方法 315
インバウンド パス選択の変更 315
AS_PATH 属性の変更によるインバウンド パス選択の変化 315
MED 属性の設定によるインバウンド パス選択の変化 319
アウトバウンド パス選択への影響 323
Local_Pref 属性を使用したアウトバウンド パス選択の変更 324
アウトバウンド BGP ルート プレフィックスのフィルタリング 327
ISP との BGP ピアリングの設定 330
2 つの ISP とのマルチホーミングの設定 331
単一 ISP とのマルチホーミング 335
マルチホーミングのフル インターネット ルーティング テーブル受信設定 342
BGP ポリシーの設定 346
プレフィックス リストによる BGP プレフィックスのフィルタリング 346
AS-Path フィルタを使用した BGP プレフィックスのフィルタ処理 351
4 バイト自律システム番号を使用した AS-path フィルタによる BGP プレフィックスのフィルタリング 353
コミュニティ リストを使用したトラフィック フィルタリング 358
拡張コミュニティ リストを使用したトラフィック フィルタリング 362
BGP ルート マップ ポリシー リストを使用したトラフィック フィルタリング 367
BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング 371
外部 BGP を使用したサービス プロバイダーとの接続の設定例 375

例：インバウンド パス選択の変化 375
例：4 バイト AS 番号を使用した AS-path 属性の変更によるインバウンド パス選択の変化 376
例：プレフィックス リストによる BGP プレフィックスのフィルタ処理 377
例：シングル プレフィックス リストを使用した BGP プレフィックスのフィルタ処理 378
例：プレフィックスのグループを使用した BGP プレフィックスのフィルタ処理 378
例：プレフィックス リスト エントリの追加と削除 379
例：COMMUNITIES 属性を使用したトラフィックのフィルタ処理 380
例：AS-Path フィルタを使用したトラフィックのフィルタ処理 380
例：4 バイト自律システム番号を使用した AS-path フィルタによるトラフィックのフィルタ処理 381
例：4バイト自律システム番号と拡張コミュニティ リストを使用したトラフィックのフィルタ処理 382
例：BGP ルート マップを使用したトラフィックのフィルタ処理 385
次の作業 385
その他の参考資料 385
外部 BGP を使用したサービス プロバイダーとの接続の機能情報 387

第 13 章 BGP ルート マップ継続 391
機能情報の確認 391
BGP ルート マップ継続に関する情報 392
continue 句を使用した BGP ルート マップ 392
continue 句を使用しないルート マップの動作 392
continue 句を使用したルート マップの動作 392
continue 句を使用した match 動作 392
continue 句を使用した Set 動作 393
BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理の方法 393
BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング 393
BGP ルート マップ継続の設定例 397
例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理 397
その他の参考資料 399

BGP ルート マップ継続の機能情報 399

第 14 章 アウトバウンド ポリシーに対する BGP ルート マップ継続のサポート 401

機能情報の確認 401

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートに関する情報 402

continue 句を使用した BGP ルート マップ 402

continue 句を使用しないルート マップの動作 402

continue 句を使用したルート マップの動作 402

continue 句を使用した match 動作 402

continue 句を使用した Set 動作 403

BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理の方法 403

BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング 403

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートの設定例 407

例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理 407

その他の参考資料 409

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートの機能情報 410

第 15 章 BGP の AS パスからプライベート AS 番号の削除 411

機能情報の確認 411

AS パスからプライベート ASN の削除および交換の制約事項 412

AS パスからプライベート ASN の削除および交換に関する情報 412

パブリックおよびプライベート AS 番号 412

AS パスからプライベート ASN の削除および交換の利点 412

AS パスからプライベート ASN の削除に関する過去の制約事項 412

AS パスからプライベート ASN の削除の拡張機能 413

AS パスからプライベート ASN を削除および交換する方法 414

AS パスのプライベート ASN の削除および置換（Cisco IOS XE Release 3.1S 以降） 414

AS パスからプライベート ASN を削除および交換する設定例 417

プライベート ASN の削除の例（Cisco IOS XE Release 3.1S） 417

プライベート ASN の削除および置換の例（Cisco IOS XE Release 3.1S） 418

プライベート ASN の置換の例（Cisco IOS XE Release 2S） 419

その他の参考資料 421

AS パスからプライベート ASN の削除および交換の機能情報 422

第 16 章 BGP ネイバーセッションオプションの設定 425

機能情報の確認 425

BGP ネイバー セッション オプションの設定に関する情報 426

BGP ネイバー セッション 426

高速ピアリング セッションの非アクティブ化に対する BGP サポート 426

BGP ホールド タイマー 426

BGP の高速ピアリング セッションの非アクティブ化 426

BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング 426

BGP IPv6 ネイバーの BFD サポート 427

BGP ネイバー セッションの TTL セキュリティ チェック 427

TTL セキュリティ チェックに対する BGP サポート 427

BGP ネイバー セッションの TTL セキュリティ チェック 428

マルチホップ BGP ネイバー セッションに対する TTL セキュリティ チェックのサポート 428

TTL セキュリティ チェックに対する BGP サポートの利点 428

セッションごとの TCP の PMTUD に対する BGP サポート 429

パス MTU 検出 429

BGP ネイバー セッションの TCP の PMTUD 429

BGP ネイバー セッションのオプションの設定方法 430

高速セッションの非アクティブ化の設定 430

BGP ネイバー の高速セッションの非アクティブ化の設定 430

高速セッションの非アクティブ化の選択的アドレス トラッキングの設定 432

BGP IPv6 ネイバーの BFD の設定 434

BGP ネイバー セッションの TTL セキュリティ チェックの設定 437

セッションごとの TCP の PMTUD に対する BGP サポートの設定 441

すべての BGP セッションに対する TCP の PMTUD のグローバルな無効化 441

単一の BGP ネイバーに対する TCP の PMTUD の無効化 444

すべての BGP セッションに対する TCP の PMTUD のグローバルな有効化 446

単一の BGP ネイバーに対する TCP の PMTUD の有効化 448
BGP ネイバー セッション オプションの設定例 451
例：BGP ネイバーの高速セッションの非アクティブ化の設定 451
例：高速セッションの非アクティブ化の選択的アドレス トラッキングの設定 451
例：BGP IPv6 ネイバーの BFD の設定 451
例：TTL セキュリティ チェックの設定 452
例：セッションごとの TCP の PMTUD に対する BGP サポートの設定 452
例：すべての BGP セッションに対する TCP の PMTUD のグローバルな無効化 452
例：単一の BGP ネイバーに対する TCP の PMTUD の無効化 453
例：すべての BGP セッションに対する TCP の PMTUD のグローバルな有効化 453
例：単一の BGP ネイバーに対する TCP の PMTUD の有効化 453
次の作業 453
その他の参考資料 454
BGP ネイバー セッションのオプション設定の機能情報 455

第 17 章 **BGP ネイバー ポリシー** 457
機能情報の確認 457
BGP ネイバー ポリシーに関する情報 458
BGP ネイバー ポリシー機能の利点 458
BGP ネイバー ポリシー情報の表示方法 458
BGP ネイバー ポリシー情報の表示 458
その他の参考資料 459
BGP ネイバー ポリシーの機能情報 459

第 18 章 **BGP ダイナミック ネイバー** 461
機能情報の確認 461
BGP ダイナミック ネイバーに関する情報 462
BGP ダイナミック ネイバー 462
BGP ダイナミック ネイバーの設定方法 462
サブネット範囲を使用する BGP ダイナミック ネイバーの実装 462
VRF のサポートを含む BGP IPv6 ダイナミック ネイバー サポートの設定 469

BGP IPv6 ダイナミック ネイバー設定の確認 471
BGP ダイナミック ネイバーの設定例 472
例：サブネット範囲を使用する BGP ダイナミック ネイバーの実装 472
例：VRF のサポートを含む BGP IPv6 ダイナミック ネイバー サポートの設定 474
その他の参考資料 475
BGP ダイナミック ネイバーの機能情報 476

第 19 章 ネクストホップ アドレス トラッキングに対する BGP サポート 479
機能情報の確認 479
ネクストホップ アドレス トラッキングに対する BGP サポートに関する情報 480
BGP ネクストホップ アドレス トラッキング 480
BGP ネクストホップ ダンプニングのペナルティ 480
BGP スキャナのデフォルトの動作 480
BGP Next_Hop 属性 481
選択的 BGP ネクストホップ ルート フィルタリング 481
高速ピアリング セッションの非アクティブ化に対する BGP サポート 482
BGP ホールド タイマー 482
BGP の高速ピアリング セッションの非アクティブ化 482
BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング 482
ネクストホップ アドレス トラッキングに対する BGP サポートの設定方法 482
BGP ネクストホップ アドレス トラッキングの設定 482
BGP 選択的ネクストホップ ルート フィルタリングの設定 483
BGP ネクストホップ アドレス トラッキングの遅延間隔の調整 486
BGP ネクストホップ アドレス トラッキングの無効化 488
高速セッションの非アクティブ化の設定 489
BGP ネイバー の高速セッションの非アクティブ化の設定 489
高速セッションの非アクティブ化の選択的アドレス トラッキングの設定 491
ネクストホップ アドレス トラッキングに対する BGP サポートの設定例 493
例：BGP ネクストホップ アドレス トラッキングの有効化と無効化 493
例：BGP ネクストホップ アドレス トラッキングの遅延間隔の調整 493
例：BGP 選択的ネクストホップ ルート フィルタリングの設定 494

例：BGP ネイバーの高速セッションの非アクティブ化の設定 494
例：高速セッションの非アクティブ化の選択的アドレス トラッキングの設定 495
その他の参考資料 495
ネクストホップ アドレス トラッキングに対する BGP サポートの機能情報 497

第 20 章 最大プレフィックス制限到達後の BGP ネイバー セッション再起動 501
機能情報の確認 501
最大プレフィックス制限到達後の BGP ネイバー セッション再起動に関する情報 502
プレフィックス制限および BGP ピアリング セッション 502
最大プレフィックス制限による BGP ネイバー セッションの再起動 502
BGP 中止通知のサブコード 502
最大プレフィックス制限を超えた後にネイバー セッションを再確立するためのデバイスの設定方法 503
最大プレフィックス制限到達後にネイバー セッションを再確立するためのルータの設定 503
トラブルシューティングのヒント 507
最大プレフィックス制限到達後の BGP ネイバー セッション再起動の設定例 507
例：最大プレフィックス制限到達後にネイバー セッションを再確立するためのルータの設定 507
最大プレフィックス制限到達後の BGP ネイバー セッション再起動に関する追加情報 508
最大プレフィックス制限後の BGP ネイバー セッション再起動の機能情報 509

第 21 章 ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポート 511
機能情報の確認 511
ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートに関する情報 512
BGP ネットワークの自律システムの移行 512
BGP ネットワーク自律システムの移行に対するデュアル自律システムのサポート 512
BGP ネットワークの 4 バイト自律システム番号への移行 513
ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの設定方法 514
ネットワーク移行のためのデュアル AS ピアリングの設定 514
ネットワーク移行のためのデュアル AS ピアリングの設定例 516
例：デュアル AS の設定 516

例：デュアル AS コンフェデレーションの設定 517
例：ルーティング アップデートでの AS の置換 518
その他の参考資料 518
ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの機能情報 518

第 22 章 内部 BGP 機能の設定 521
機能情報の確認 521
内部 BGP 機能に関する情報 522
BGP ルーティング ドメイン コンフェデレーション 522
BGP ルート リフレクタ 522
ルーティング ループを回避するルート リフレクタのメカニズム 525
iBGP ピアに対する IP ネクスト ホップを設定するルート リフレクタの BGP アウトバウンド ルート マップ 526
BGP ルート ダンプニング 526
ルート ダンプニングによるルート フラッピングの最小化 527
BGP ルート ダンプニングの用語 527
BGP ルート マップ ネクスト ホップ セルフ 528
内部 BGP 機能の設定法 528
ルーティング ドメイン コンフェデレーションの設定 528
ルート リフレクタの設定 529
iBGP ピアのネクスト ホップを設定するルート マップを使用するルート リフレクタの設定 530
BGP タイマーの調整 533
削除された MED を最も条件の悪いパスと見なすようにルータを設定 534
MED が副自律システム パスからパスを選択すると見なすようにルータを設定 534
コンフェデレーションのパスの選択に MED を使用するようにルータを設定 535
BGP ルート ダンプニングのイネーブル化と設定 535
BGP ルート ダンプニングのモニタリングおよびメンテナンス 537
BGP ルート マップの next-hop self の設定 538
内部 BGP 機能の設定例 542
例：ルート マップのある BGP コンフェデレーション設定 542

例：BGP コンフェデレーション　543
例：iBGP ピアのネクスト ホップを設定するルート マップを使用するルート リフレクタ　544
例：BGP ルート マップの next-hop self の設定　545
内部 BGP 機能に関する追加情報　545
内部 BGP 機能設定用の機能情報　547

第 23 章　ルート リフレクタでの BGP VPLS 自動検出のサポート　549
機能情報の確認　549
ルート リフレクタでの BGP VPLS 自動検出のサポートの概要　550
ルート リフレクタでの BGP VPLS オートディスカバリのサポート　550
ルート リフレクタでの BGP VPLS 自動検出のサポートに関する制約事項　550
ルート リフレクタでの BGP VPLS 自動検出のサポートの設定例　550
例：ルート リフレクタでの BGP VPLS 自動検出のサポート　550
その他の参考資料　551
ルート リフレクタでの BGP VPLS 自動検出のサポートに関する機能情報　552

第 24 章　BGP FlowSpec ルートリフレクタのサポート　553
機能情報の確認　553
BGP FlowSpec ルートリフレクタのサポートに関する制約事項　554
BGP FlowSpec ルートリフレクタのサポートに関する情報　554
FlowSpec の概要　554
マッチング基準　554
BGP FlowSpec ルートリフレクタのサポートの設定方法　555
BGP FlowSpec ルートリフレクタのサポートの設定　555
BGP FlowSpec 検証の無効化　557
BGP FlowSpec ルートリフレクタのサポートの確認　558
BGP FlowSpec ルートリフレクタのサポートの設定例　562
例：BGP FlowSpec ルートリフレクタのサポート　562
BGP FlowSpec ルートリフレクタのサポートに関する追加情報　563
BGP FlowSpec ルートリフレクタのサポートの機能情報　564

第 25 章 BGP フロー スペック クライアント 565

機能情報の確認 565

BGP フロー スペック クライアントの前提条件 566

BGP フロー スペック クライアントの制約事項 566

BGP フロー スペック クライアントに関する情報 566

BGP フロー スペック モデル 566

フロー スペック クライアントの設定例 567

マッチング基準とアクション 567

BGP フロー スペック クライアントの設定方法 568

フロー スペック クライアントとしてのデバイスの設定およびネイバーとの BGP ピア関係の確立 568

デバイスのすべてのインターフェイスでのフロー スペック ポリシーの設定 570

BGP フロー スペック クライアントの確認 572

BGP フロー スペック クライアントの設定例 574

例：フロー スペック クライアントとしてのデバイスの設定およびネイバーとの BGP ピア関係の確立 574

例：デバイスのすべてのインターフェイスでのフロー スペック ポリシーの設定 574

BGP フロー スペック クライアントに関する追加情報 575

BGP フロー スペック クライアントの機能情報 576

第 26 章 BGP NSF 認識 577

機能情報の確認 577

BGP NSF 認識に関する情報 578

Cisco NSF ルーティングと転送操作 578

NSF のシスコ エクスプレス フォワーディング 578

NSF のための BGP グレースフル リスタート 579

BGP NSF 認識 580

BGP NSF 認識の設定方法 580

BGP グレースフル リスタートを使用した BGP ノンストップ フォワーディング認識の設定 580

BGP グレースフル リスタートを使用した BGP グローバル NSF 認識のイネーブル化 581
BGP NSF 認識タイマーの設定 583
BGP ノンストップ フォワーディング認識の設定の確認 585
BGP NSF 認識の設定例 586
例：グレースフル リスタートを使用した BGP グローバル NSF 認識の有効化 586
その他の参考資料 587
BGP NSF 認識の機能情報 587

第 27 章 ネイバーごとの BGP グレースフル リスタート 589
機能情報の確認 589
ネイバーごとの BGP グレースフル リスタートに関する情報 590
ネイバーごとの BGP グレースフル リスタート 590
BGP ピア セッション テンプレート 590
ネイバーごとの BGP グレースフル リスタートの設定方法 591
個々の BGP ネイバーの BGP グレースフル リスタートのイネーブル化 591
BGP ピア セッション テンプレートを使用した BGP グレースフル リスタートのイネーブル化とディセーブル化 594
BGP ピア グループの BGP グレースフル リスタートのディセーブル化 600
ネイバーごとの BGP グレースフル リスタートの設定例 603
例：ネイバーごとの BGP グレースフル リスタートの有効化と無効化 603
その他の参考資料 604
ネイバーごとの BGP グレースフル リスタートの機能情報 605

第 28 章 BFD に対する BGP サポート 607
機能情報の確認 607
BFD に対する BGP サポートに関する情報 608
BGP の BFD 608
BFD を使用した BGP コンバージェンス時間の短縮方法 608
前提条件 608
機能制限 608

BFD を使用した BGP コンバージェンス時間の短縮 609
インターフェイスでの BFD セッション パラメータの設定 609
BGP に対する BFD サポートの設定 610
BFD のモニタリングとトラブルシューティング 611
その他の参考資料 612
BFD に対する BGP サポートの機能情報 613

第 29 章 MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタート 615
機能情報の確認 615
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートに関する情報 616
MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート 616
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定方法 616
IPv6 BGP グレースフル リスタート機能の設定 616
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定例 617
例：IPv6 BGP グレースフル リスタート機能の設定 617
その他の参考資料 618
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの機能情報 619

第 30 章 BGP パーシステンス 621
BGP パーシステンスの制約事項 621
BGP パーシステンスの概要 621
リスタート ルータ 622
ヘルパー ルータ 622
ヘルパー ルータのピア 623
BGP パーシステンスの設定方法 623
BGP パーシステンスの設定 623
BGP パーシステンスの確認 624
BGP パーシステンスの機能情報 626

第 31 章 BGP リンク帯域幅 627

機能情報の確認 627

BGP リンク帯域幅の前提条件 628

BGP リンク帯域幅の制約事項 628

BGP リンク帯域幅に関する情報 628

BGP リンク帯域幅の概要 628

リンク帯域幅拡張コミュニティの属性 629

BGP リンク帯域幅機能の利点 629

BGP リンク帯域幅の設定法 629

BGP リンク帯域幅の設定 629

BGP リンク帯域幅設定の確認 631

BGP リンク帯域幅の設定例 631

BGP リンク帯域幅設定の例 631

BGP リンク帯域幅の確認 634

その他の参考資料 635

BGP リンク帯域幅の機能情報 637

第 32 章 ボーダー ゲートウェイ プロトコル リンクステート 639

機能情報の確認 639

ボーダー ゲートウェイ プロトコル リンクステートに関する情報 640

ボーダー ゲートウェイ プロトコルのリンクステート情報の概要 640

ボーダー ゲートウェイ プロトコルのリンクステート情報の伝送 641

TLV 形式 641

リンクステート NLRI 641

NLRI タイプ 642

ノード記述子 643

リンク記述子 643

プレフィックス記述子 643

BGP-LS 属性 643

ボーダー ゲートウェイ プロトコル リンクステートを使用した OSPF の設定方法 644

ボーダー ゲートウェイ プロトコル リンクステートを使用した OSPF の設定 644
ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定方法 645
ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定 645
BGP の設定 646
例：ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定 646
ボーダー ゲートウェイ プロトコル リンクステート設定の確認 647
ボーダー ゲートウェイ プロトコル リンクステートの debug コマンド 650
ボーダー ゲートウェイ プロトコル リンクステートに関する追加情報 650
ボーダー ゲートウェイ プロトコル リンクステートの機能情報 651

第 33 章 **iBGP マルチパス ロード シェアリング 653**
機能情報の確認 653
iBGP マルチパス ロード シェアリングの概要 653
iBGP マルチパス ロード シェアリングの利点 655
iBGP マルチパス ロード シェアリングに関する制約事項 655
iBGP のマルチパス ロード シェアリングの設定方法 656
iBGP マルチパス ロード シェアリングの設定 656
iBGP のマルチパス ロード シェアリングの確認 656
iBGP のマルチパス ロード シェアリングのモニタリングおよびメンテナンス 659
設定例 659
例：非 MPLS トポロジでの iBGP のマルチパス ロード シェアリング 659
例：MPLS VPN トポロジでの iBGP のマルチパス ロード シェアリング 660
その他の参考資料 661
iBGP のマルチパス ロード シェアリングの機能情報 662

第 34 章 **MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング 663**
機能情報の確認 663
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの前提条件 664
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの制約事項 664

MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングについて 665
eBGP と iBGP 間のマルチパス ロード シェアリング 665
BGP MPLS ネットワークにおける eBGP および iBGP のマルチパス ロード シェアリング 665
ルート リフレクタを使用した eBGP および iBGP のマルチパス ロード シェアリング 666
eBGP および iBGP の両方に対するマルチパス ロード シェアリングの利点 667
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの設定方法 667
eBGP および iBGP に対する BGP マルチパス ロード シェアリングの設定 667
eBGP および iBGP の両方に対するマルチパス ロード シェアリングの設定の確認 669
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの設定例 670
例：eBGP および iBGP のマルチパス ロード シェアリングの設定 670
例：eBGP および iBGP のマルチパス ロード シェアリングの確認 670
次の作業 671
その他の参考資料 671
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの機能情報 673

第 35 章 **6 つを超えるパラレル パスにおける IP パケットのロードシェアリング 675**
機能情報の確認 675
6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの概要 676
その他の参考資料 676
6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの機能情報 677

第 36 章 **BGP ポリシー アカウンティング 679**
機能情報の確認 679
前提条件 679
BGP ポリシー アカウンティングに関する情報 680
BGP ポリシー アカウンティングの概要 680
BGP ポリシー アカウンティングの利点 681

BGP ポリシー アカウンティングの設定方法 681
BGP ポリシー アカウンティングの一致基準の指定 681
IP トラフィックの分類および BGP ポリシー アカウンティングの有効化 682
BGP ポリシー アカウンティングの確認 683
BGP ポリシー アカウンティングのモニタリングおよびメンテナンス 685
BGP ポリシー アカウンティングの設定例 685
例：BGP ポリシー アカウンティングの一致基準の指定 685
例：IP トラフィックの分類および BGP ポリシー アカウンティングの有効化 686
その他の参考資料 686
BGP ポリシー アカウンティングの機能情報 687

第 37 章 BGP ポリシーアカウンティング出力インターフェイス アカウンティング 689
機能情報の確認 689
BGP PA 出力インターフェイス アカウンティングの前提条件 690
BGP PA 出力インターフェイス アカウンティングに関する情報 690
BGP PA 出力インターフェイス アカウンティング 690
BGP PA 出力インターフェイス アカウンティングの利点 691
BGP PA 出力インターフェイス アカウンティングの設定方法 692
BGP PA の一致基準の指定 692
IP トラフィックの分類および BGP PA の有効化 693
BGP ポリシー アカウンティングの確認 695
BGP PA 出力インターフェイス アカウンティングの設定例 698
BGP ポリシー アカウンティングの一致基準の指定例 698
IP トラフィックの分類および BGP ポリシー アカウンティングの有効化の例 699
その他の参考資料 699
BGP ポリシー アカウンティング出力インターフェイス アカウンティングの機能情報 701
用語集 702

第 38 章 BGP コスト コミュニティ 703
機能情報の確認 703
BGP コスト コミュニティ機能の前提条件 704

BGP コスト コミュニティ機能の制約事項 704
BGP コスト コミュニティ機能に関する情報 704
BGP コスト コミュニティの概要 704
BGP コストコミュニティによるベスト パス選択プロセスへの影響 705
集約ルートおよびマルチパスに対するコスト コミュニティのサポート 706
マルチエグジット IGP ネットワークにおけるルート プリファレンスの反映 706
バックドア リンクを持つ EIGRP MPLS VPN Provider Edge-Customer Edge（PE-CE）に対する BGP コスト コミュニティ サポート 707
BGP コスト コミュニティ機能の設定方法 708
BGP コスト コミュニティの設定 708
BGP コスト コミュニティの設定確認 710
トラブルシューティングのヒント 710
BGP コスト コミュニティ機能の設定例 710
例：BGP コスト コミュニティ設定 710
例：BGP コスト コミュニティ検証 711
その他の参考資料 712
BGP コスト コミュニティの機能情報 714

第 39 章 **グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート 715**
機能情報の確認 715
グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの前提条件 716
グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの制限事項 716
グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポートに関する情報 717
IPv4 プレフィックスから VRF へのインポート 717
ブラック ホール ルーティング 717
グローバル トラフィックの分類 717
ユニキャスト リバース パス フォワーディング 718
グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート方法 718

インポートする IPv4 IP プレフィックスの定義 718
VRF およびインポート ルート マップの作成 719
入力インターフェイスのフィルタリング 722
グローバル IP プレフィックス インポートの確認 723
グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの設定例 725
例：グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート 725
例：VRF テーブルへの IP プレフィックス インポートの確認 725
内部 BGP 機能に関する追加情報 726
グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの機能情報 728

第 40 章 VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに対する BGP サポート 729
機能情報の確認 729
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに関する情報 730
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの利点 730
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの仕組み 730
VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート方法 732
VRF およびアドレス ファミリ用エクスポート ルート マップの作成 732
VRF および VRF 用エクスポート ルート マップの作成（IPv4 のみ） 735
VRF からグローバル テーブルへの IP プレフィックス エクスポートに関する情報の表示 737
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの設定例 738
例：IPv6 アドレス ファミリを使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート 738
例：IPv4 アドレス ファミリを使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート 739
例：IP VRF を使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート（IPv4 のみ） 739
その他の参考資料 739
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの機能情報 740

第 41 章 BGP のネイバーごとの SoO 設定 741

機能情報の確認 741

BGP のネイバーごとの SoO 設定の前提条件 742

BGP のネイバーごとの SoO 設定の制約事項 742

BGP のネイバーごとの SoO の設定に関する情報 742

Site of Origin BGP コミュニティ属性 742

ルート識別子 742

BGP によるネイバーごとの Site of Origin の設定 742

BGP のネイバーごとの Site of Origin の利点 744

BGP ピア ポリシー テンプレート 744

BGP のネイバーごとの SoO の設定方法 745

Cisco Express Forwarding の有効化と VRF インスタンスの設定 745

BGP ピア ポリシー テンプレートを使用したネイバーごとの SoO 値の設定 748

BGP ネイバー コマンドを使用したネイバーごとの SoO 値の設定 751

BGP ピア グループを使用したネイバーごとの SoO 値の設定 753

BGP のネイバーごとの SoO 設定の設定例 756

例：BGP ピア ポリシー テンプレートを使用したネイバーごとの SoO 値の設定 756

例：BGP ネイバー コマンドを使用したネイバーごとの SoO 値の設定 756

例：BGP ピア グループを使用したネイバーごとの SoO 値の設定 757

次の作業 757

その他の参考資料 758

BGP のネイバーごとの SoO 設定の機能情報 758

第 42 章 BGP ルータ ID の VRF 単位での割り当て 761

機能情報の確認 761

BGP ルータ ID の VRF 単位での割り当ての前提条件 762

BGP ルータ ID の VRF 単位での割り当てに関する情報 762

BGP ルータ ID 762

VRF 単位でのルータ ID の割り当て 762

ルート識別子 762

BGP ルータ ID の VRF 単位での割り当ての設定方法 763
VRF インスタンスの設定 763
VRF インスタンスとインターフェイスの関連付け 765
VRF 単位での BGP ルータ ID の手動設定 767
VRF 単位での BGP ルータ ID の自動割り当て 773
BGP ルータ ID の VRF 単位での割り当ての設定例 780
VRF 単位での BGP ルータ ID の手動設定例 780
VRF 単位での BGP ルータ ID の自動割り当て例 783
ループバック インターフェイス IP アドレスを使用してグローバルに自動割り当てされるルータ ID の例 783
デフォルト ルータ ID がない場合にグローバルに自動割り当てされるルータ ID の例 784
VRF 単位で自動割り当てされるルータ ID の例 785
その他の参考資料 787
BGP ルータ ID の VRF 単位での割り当てに関する機能情報 788

第 43 章 **BGP ネクスト ホップ非変更 791**
機能情報の確認 791
ネクスト ホップ非変更に関する情報 792
BGP ネクスト ホップ非変更 792
BGP ネクスト ホップ非変更の設定方法 793
eBGP ピアの BGP ネクスト ホップ非変更の設定 793
ルートマップを使用した BGP ネクスト ホップ非変更の設定 794
BGP ネクスト ホップ非変更の設定例 795
例：eBGP ピアの BGP ネクスト ホップ非変更 795
その他の参考資料 796
BGP ネクスト ホップ非変更機能の情報 797

第 44 章 **L2VPN アドレス ファミリに対する BGP サポート 799**
機能情報の確認 799
L2VPN アドレス ファミリに対する BGP サポートの前提条件 800

L2VPN アドレス ファミリに対する BGP サポートの制約事項 800
L2VPN アドレス ファミリに対する BGP サポートに関する情報 800
L2VPN アドレス ファミリ 800
VPLS ID 802
L2VPN アドレス ファミリに対する BGP サポートの設定方法 802
BGP および L2VPN アドレス ファミリを使用した VPLS オートディスカバリの設定 802
次の作業 808
L2VPN アドレス ファミリに対する BGP サポートの設定例 809
例：BGP および L2VPN アドレス ファミリを使用した VPLS 自動検出の設定 809
次の作業 812
その他の参考資料 812
L2VPN アドレス ファミリに対する BGP サポートに関する機能情報 813

第 45 章 **BGP イベントベース VPN インポート 815**
機能情報の確認 815
BGP イベントベース VPN インポートの前提条件 816
BGP イベントベース VPN インポートの概要 816
BGP イベントベース VPN インポート 816
インポート パス選択ポリシー 816
インポート パスの制限 817
BGP イベントベース VPN インポートの設定方法 817
マルチプロトコル VRF の設定 817
BGP パスへのイベントベース VPN インポート処理の設定 820
BGP イベントベース VPN インポート処理のモニタリングとトラブルシューティング 822
BGP イベントベース VPN インポートの設定例 824
例：BGP パスへのイベントベース VPN インポート処理の設定 824
その他の参考資料 824
BGP イベントベース VPN インポートの機能情報 826

第 46 章 **BGP 最良外部 827**
機能情報の確認 827

BGP 最良外部の前提条件 828
BGP 最良外部の制約事項 828
BGP 最良外部に関する情報 829
BGP 最良外部の概要 829
ベスト外部ルートとは 829
BGP 最良外部機能の仕組み 830
BGP 最良外部を有効にするためのコンフィギュレーション モード 831
クラスタ間の RR での BGP ベスト外部パス 831
クラスタ間の RR でのベスト外部パスに関する CLI の違い 832
クラスタ間の RR での BGP ベスト外部パスの計算に使用されるルール 832
BGP 最良外部の設定方法 833
BGP 最良外部機能の設定 833
BGP 最良外部機能の確認 836
クラスタ間の RR でのベスト外部パスの設定 838
BGP 最良外部の設定例 842
例：BGP 最良外部機能の設定 842
例：クラスタ間の RR でのベスト外部パスの設定 843
その他の参考資料 843
BGP 最良外部の機能情報 845

第 47 章 IP および MPLS-VPN 向け BGP PIC エッジ 847
機能情報の確認 847
BGP PIC の前提条件 848
BGP PIC の制約事項 848
BGP PIC の概要 849
利点 849
BGP コンバージェンス 849
コンバージェンスの改善 849
BGP Fast Reroute 851
障害の検出 852
BGP PIC による瞬時でのコンバージェンスの達成 852

BGP PIC による MPLS VPN BGP ローカル コンバージェンスの機能向上 853
BGP PIC の有効化 853
BGP PIC シナリオ 853
CE 側での IP PE-CE リンクおよびノード保護（デュアル PE） 853
CE 側での IP PE-CE リンクおよびノード保護（デュアル CE とデュアル PE のプライマリおよびバックアップ ノード） 854
プライマリまたはバックアップ/代替パスの IP MPLS PE-CE リンク保護 855
プライマリまたはバックアップ/代替パスの IP MPLS PE-CE ノード保護 856
Cisco Express Forwarding の再帰 858
BGP PIC の設定方法 859
BGP PIC の設定 859
BGP PIC コアの無効化 861
BGP PIC の設定例 862
例：BGP PIC の設定 862
例：BGP PIC のバックアップ/代替パスの表示 864
例：BGP PIC コアの無効化 866
その他の参考資料 866
BGP PIC の機能情報 867

第 48 章 **BGP 低速ピアの検出と軽減** 869
機能情報の確認 869
BGP 低速ピアの検出と軽減について 870
BGP 低速ピアの問題 870
BGP 低速ピア機能 870
BGP 低速ピア検出 871
アップデート メッセージのタイムスタンプ 871
BGP 低速ピア検出の利点 871
ダイナミックまたはスタティック BGP 低速ピアの設定の利点 872
スタティック低速ピア 872
ダイナミック低速ピア 872
BGP 低速ピアの検出と軽減の方法 873

低速ピアの検出 873
アドレスファミリ レベルでのダイナミック低速ピアの検出 873
ネイバー レベルでのダイナミック低速ピアの検出 875
ピア ポリシー テンプレートを使用したダイナミック低速ピアの検出 876
ピアをスタティック低速ピアとしてマークする 877
ネイバー レベルでスタティック低速ピアとしてピアをマークする 877
ピア ポリシー テンプレートを使用して、スタティック低速ピアとしてピアをマークする 878
ダイナミック低速ピア保護の設定 880
アドレスファミリ レベルでのダイナミック低速ピアの設定 880
ネイバー レベルでのダイナミック低速ピアの設定 882
ピア ポリシー テンプレートを使用したダイナミック低速ピアの設定 884
ダイナミック低速ピアに関する出力の表示 886
ダイナミック低速ピアを通常のピアとして回復 887
BGP 低速ピアの検出と軽減の設定例 888
例：スタティック低速ピア 888
例：ピア ポリシー テンプレートを使用したスタティック低速ピア 888
例：ネイバー レベルでのダイナミック低速ピア 888
例：ピア ポリシー テンプレートを使用したダイナミック低速ピア 889
例：ピア グループを使用したダイナミック低速ピア 889
その他の参考資料 890
iBGP ローカル AS に対する BGP サポートの機能情報 892

第 49 章 **BGP：RT 制約ルート配布の設定** 893
機能情報の確認 893
BGP：RT 制約ルート配布の前提条件 894
BGP：RT 制約ルート配布の制限事項 894
BGP に関する情報：RT 制約ルート配布 894
BGP：RT 制約ルート配布により解決できる問題 894
BGP の利点：RT 制約ルート配布 895
BGP RT-Constrain SAFI 896

BGP：RT 制約ルート配布の動作 896
RT 制約 NLRI プレフィックス 897
RT 制約ルート配布のプロセス 897
デフォルトの RT フィルタ 898
RT 制約ルート配布の設定方法 898
プロバイダーエッジ（PE）ルータおよびルートリフレクタでのマルチプロトコル BGP の設定 898
トラブルシューティングのヒント 900
MPLS VPN カスタマーの接続 900
カスタマーの接続を可能にするための PE ルータでの VRF の定義 901
各 VPN カスタマー用の PE ルータでの VRF インスタンスの設定 902
BGP を PE ルータと CE ルータ間のルーティング プロトコルに設定 903
PE での RT 制約の設定 905
RR での RT 制約の設定 907
BGP：RT 制約ルート配布の設定例 909
例：PE と RR の間での BGP RT 制約ルート配布 909
その他の参考資料 911
BGP RT 制約ルート配布の機能情報 913

第 50 章 **BGP ルーティング サーバの設定 915**
機能情報の確認 915
BGP ルーティング サーバに関する情報 916
BGP ルーティング サーバにより解決できる問題 916
BGP ルーティング サーバによる SP 相互接続の簡素化 918
BGP ルーティング サーバの利点 919
ルーティング サーバ コンテキストが提供する柔軟なルーティング ポリシー 920
ルーティング サーバ クライアントでの 3 段階のフィルタリング 920
BGP ルーティング サーバの設定方法 921
基本機能を備えたルーティング サーバの設定 921
アップデートを受け入れるためのルーティング サーバ クライアントの設定 923
柔軟なポリシー処理を備えたルーティング サーバの設定 925

BGP ルーティング サーバ情報の表示とルーティング サーバのトラブルシューティング 928
BGP ルーティング サーバの設定例 929
基本機能を備えた BGP ルーティング サーバの例 929
柔軟なポリシーの BGP ルーティング サーバ コンテキストの例（IPv4 アドレス指定） 930
通常のベストパスがルーティング サーバ コンテキストのルートによって上書きされたことを show コマンドで確認する例 930
ポリシーを満たすルートがない BGP ルーティング サーバ コンテキストの例 931
柔軟なポリシーの BGP ルーティング サーバ コンテキストの例（IPv6 アドレス指定） 932
その他の参考資料 933
BGP ルーティング サーバの機能情報 934

第 51 章 ダイバースパス ルート リフレクタを使用した BGP ダイバース パス 937
機能情報の確認 937
ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの前提条件 938
ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの制約事項 938
ダイバースパス リフレクタを使用した BGP ダイバース パスに関する情報 938
BGP ダイバース パスによって解消される制限 938
ダイバースパス ルート リフレクタを使用した BGP ダイバース パス 939
BGP ダイバース パスを計算するためのトリガー 941
IGP メトリック チェック 941
ルート リフレクタの決定 942
BGP ダイバースパス ルート リフレクタの設定方法 942
IGP メトリック チェックの無効化が必要かどうかの判断 942
BGP ダイバース パス用のルート リフレクタの設定 943
ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの設定例 945
例：追加パスがバックアップ パスである BGP ダイバース パスの設定 945
例：追加パスがマルチパスである BGP ダイバース パスの設定 946
例：マルチパスとバックアップ パスの計算がトリガーされる BGP ダイバース パスの設定 947
例：バックアップ パスの計算とインストールをトリガーするための設定 947
その他の参考資料 948

ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの機能情報 949

第 52 章 BGP 拡張ルート リフレッシュ 951

機能情報の確認 951

BGP 拡張ルート リフレッシュに関する情報 951

BGP 拡張ルート リフレッシュ機能 951

BGP 拡張ルート リフレッシュ タイマー 952

BGP 拡張ルート リフレッシュよって生成される Syslog メッセージ 952

BGP 拡張ルート リフレッシュのタイマーの設定方法 953

BGP 拡張ルート リフレッシュのタイマーの設定 953

BGP 拡張ルート リフレッシュの設定例 954

例：BGP 拡張ルート リフレッシュのタイマーの設定 954

その他の参考資料 954

BGP 拡張ルート リフレッシュの機能情報 955

第 53 章 BGP 整合性チェッカの設定 957

機能情報の確認 957

BGP 整合性チェッカに関する情報 958

BGP の整合性チェッカ 958

BGP 整合性チェッカの設定方法 959

BGP 整合性チェッカの設定 959

BGP 整合性チェッカの設定例 960

例：BGP 整合性チェッカの設定 960

その他の参考資料 960

BGP 整合性チェッカの機能情報 962

第 54 章 BGP—起点 AS 検証 963

機能情報の確認 963

BGP 起点 AS 検証に関する情報 964

BGP—起点 AS 検証の利点 964

BGP—起点 AS 検証の仕組み 964

RPKI 検証状態をネイバーに通知するためのオプション 965
BGP ベスト パス決定での検証状態の使用 967
ルート マップを使用した有効および無効なプレフィックスの処理のカスタマイズ 968
BGP 起点 AS 検証の設定方法 968
BGP—起点 AS 検証の有効化 968
iBGP ネイバーへの RPKI 状態の通知 969
BGP プレフィックスの検証を無効化しながら、RPKI 情報をダウンロード 970
無効なプレフィックスをベスト パスとして許可 971
RPKI 状態に基づくルート マップの設定 972
BGP 起点 AS 検証の設定例 975
例：起点 AS に基づいてプレフィックスを検証するための BGP の設定 975
例：ネイバーへの RPKI 状態の通知 976
例：プレフィックス検査の無効化 976
例：無効なプレフィックスをベスト パスとして許可 976
例：RPKI 状態に基づくルート マップの使用 976
その他の参考資料 977
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の機能情報 978

第 55 章 **BGP MIB サポート** 979
機能情報の確認 979
BGP MIB サポートに関する情報 979
BGP MIB サポート 979
BGP MIB サポートを有効にする方法 982
BGP MIB サポートのイネーブル化 982
BGP MIB サポートの設定例 983
例：BGP MIB サポートの有効化 983
その他の参考資料 984
BGP MIB サポートの機能情報 985

第 56 章 **ピアごとの受信ルートに対する BGP 4 MIB サポート** 987
機能情報の確認 987

ピアごとの受信ルートに対する BGP 4 MIB サポートの制約事項 988
ピアごとの受信ルートに対する BGP 4 MIB サポートに関する情報 988
ピアごとの受信ルートに対する BGP 4 MIB サポートの概要 988
BGP 4 ピアごとの受信ルート テーブルの要素とオブジェクト 989
MIB テーブルおよびオブジェクト 989
AFI と SAFI 990
NLRI フィールドのネットワーク アドレス プレフィックスの説明 990
ピアごとの受信ルートに対する BGP 4 MIB サポートの利点 992
最大プレフィックス制限到達後の BGP ネイバー セッション再起動に関する追加情報 992
ピアごとの受信ルートに対する BGP 4 MIB サポートの機能情報 993
用語集 993

第 57 章 **L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート 995**
機能情報の確認 996
NSR with SSO に対する BGP サポートの前提条件 996
ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能に関する情報 996
BGP NSR with SSO の概要 996
BGP NSR with SSO の利点 997
ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の設定方法 998
BGP NSR with SSO をサポートする PE デバイスの設定 998
前提条件 998
BGP NSR with SSO をサポートするピアの設定 999
BGP NSR with SSO をサポートするピア グループの設定 1001
BGP NSR with SSO をサポートするピア セッション テンプレートの設定 1003
次の作業 1004
NSR with SSO の BGP サポートの確認 1004
トラブルシューティングのヒント 1006
ステートフル スイッチオーバー（SSO）による無停止ルーティング（NSR）に対する BGP サポート機能の設定例 1007

L2VPN VPLS を使用した BGP NSR with SSO の設定例 1007
その他の参考資料 1009
NSR with SSO に対する BGP サポートの機能情報 1010

第 58 章 L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート 1013
NSR with SSO に対する BGP サポートの前提条件 1014
ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能に関する情報 1014
BGP NSR with SSO の概要 1014
BGP NSR with SSO の利点 1015
ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の設定方法 1016
BGP NSR with SSO をサポートする PE デバイスの設定 1016
前提条件 1016
BGP NSR with SSO をサポートするピアの設定 1016
BGP NSR with SSO をサポートするピア グループの設定 1018
BGP NSR with SSO をサポートするピア セッション テンプレートの設定 1020
次の作業 1022
NSR with SSO の BGP サポートの確認 1022
トラブルシューティングのヒント 1024
L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポートの設定例 1025
例：L2VPN VPLS を使用した BGP NSR with SSO の設定 1025
その他の参考資料 1027
L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の機能情報 1028

第 59 章 BGP NSR 自動検知 1029
機能情報の確認 1029
BGP NSR 自動検知に関する情報 1030
BGP NSR 自動検知の利点 1030

自動検知のない NSR に戻した場合の結果 1030
BGP NSR 自動検知機能を無効にする方法 1030
BGP NSR 自動検知機能の無効化 1030
BGP NSR 自動検知の設定例 1032
例：BGP NSR 自動検知機能の無効化 1032
その他の参考資料 1032
BGP NSR 自動検知の機能情報 1033

第 60 章 **iBGP ピアの BGP NSR サポート** 1035
機能情報の確認 1035
iBGP ピアの BGP NSR サポートの制約事項 1035
iBGP ピアの BGP NSR サポートに関する情報 1036
iBGP ピアの BGP NSR サポートの利点 1036
iBGP ピアの BGP NSR サポートの設定方法 1036
IPv4 アドレス ファミリでの iBGP ピアの NSR 対応化 1036
VPNv4 アドレス ファミリでの iBGP ピアの NSR 対応化 1037
ルータ レベルでの iBGP ピアの NSR 対応化 1039
iBGP ピアの BGP NSR サポートの設定例 1040
例：iBGP ピアを NSR 対応にするための設定 1040
その他の参考資料 1041
iBGP ピアの BGP NSR サポートの機能情報 1041

第 61 章 **BGP グレースフル シャットダウン** 1043
機能情報の確認 1043
BGP グレースフル シャットダウンに関する情報 1044
BGP グレースフル シャットダウンの目的と利点 1044
GSHUT コミュニティ 1044
BGP GSHUT 拡張機能 1044
BGP グレースフル シャットダウンの設定方法 1045
BGP リンクのグレースフル シャットダウン 1045
GSHUT コミュニティに基づく BGP ルートのフィルタ処理 1047

BGP GSHUT 拡張機能の設定 1049
BGP グレースフル シャットダウンの設定例 1051
例：BGP リンクのグレースフル シャットダウン 1051
例：GSHUT コミュニティに基づく BGP ルートのフィルタ処理 1052
例：BGP GSHUT 拡張機能 1052
その他の参考資料 1053
BGP グレースフル シャットダウンの機能情報 1054

第 62 章 **BGP — mVPN BGP sAFI 129 - IPv4** 1057
機能情報の確認 1057
BGP--mVPN BGP sAFI 129 - IPv4 に関する情報 1058
BGP — mVPN BGP sAFI 129 - IPv4 の概要 1058
BGP -- mVPN BGP sAFI 129 - IPv4 の設定方法 1058
BGP — mVPN BGP sAFI 129 - IPv4 の設定 1058
BGP--mVPN BGPsAFI 129 - IPv4 の設定例 1062
例：BGP - mVPN BGP sAFI 129 - IPv4 の設定 1062
その他の参考資料 1065
BGP - mVPN BGP sAFI 129 - IPv4 の機能情報 1065

第 63 章 **BGP-MVPN SAFI 129 IPv6** 1067
機能情報の確認 1067
BGP-MVPN SAFI 129 IPv6 の前提条件 1068
BGP-MVPN SAFI 129 IPv6 に関する情報 1068
BGP-MVPN SAFI 129 IPv6 の概要 1068
BGP-MVPN SAFI 129 IPv6 の設定方法 1069
BGP-MVPN SAFI 129 IPv6 の設定 1069
BGP-MVPN SAFI 129 IPv6 の設定例 1071
例：BGP-MVPN SAFI 129 IPv6 の設定 1071
その他の参考資料 1074
BGP-MVPN SAFI 129 IPv6 の機能情報 1075

第 64 章 BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モード 1077

機能情報の確認 1077

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの制約事項 1078

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードに関する情報 1078

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モード 1078

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定方法 1080

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定 1080

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定例 1082

例：BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モードの設定 1082

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの確認 1083

その他の参考資料 1084

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モードの機能情報 1084

第 65 章 BGP 属性フィルタと拡張属性エラーの処理 1087

機能情報の確認 1087

BGP 属性フィルタリングに関する情報 1088

BGP 属性フィルタと拡張属性エラーの処理 1088

BGP パス属性をフィルタ処理する方法 1089

指定したパス属性を含む BGP アップデートの取り消し 1089

アップデート メッセージからの特定パス属性の破棄 1090

取り消されたパス属性または破棄されたパス属性の表示 1091

BGP 属性フィルタの設定例 1092

例：パス属性に基づくアップデートの取り消し 1092
例：アップデートからのパス属性の破棄 1093
その他の参考資料 1093
BGP 属性フィルタと拡張属性エラー処理の機能情報 1094

第 66 章 BGP の追加パス 1097
機能情報の確認 1097
BGP 追加パスについて 1098
追加パスで解決できる問題 1098
BGP 追加パスの利点 1100
BGP 追加パスの機能 1100
BGP 追加パスの設定方法 1102
アドレス ファミリごとの追加パスの設定 1102
ネイバーごとの追加パスの設定 1104
ピア ポリシー テンプレートを使用した追加パスの設定 1106
追加パスのフィルタリングおよび設定操作 1109
追加パス情報の表示 1110
ネイバーごとの追加パスの無効化 1111
BGP 追加パスの設定例 1113
例：BGP 追加パスの送受信機能 1113
例：BGP 追加パス 1113
例：ネイバー機能によるアドレス ファミリ機能のオーバーライド 1114
例：ピア ポリシー テンプレートを使用する BGP 追加パス 1115
その他の参考資料 1115
BGP 追加パスの機能情報 1116

第 67 章 BGP-複数のクラスタ ID 1119
機能情報の確認 1119
BGP-複数のクラスタ ID に関する情報 1120
ルート リフレクタごとの複数クラスタ ID の利点 1120
CLUSTER_LIST 属性の使用方法 1120

クライアント間のルート リフレクションを無効にした場合の動作 1121
BGP-複数のクラスタ ID の使用方法 1123
ネイバーごとのクラスタ ID の設定 1123
クラスタ内とクラスタ間のクライアント間リフレクションの無効化 1125
すべてのクラスタ ID のクラスタ内におけるクライアント間リフレクションの無効化 1126
指定したクラスタ ID のクラスタ内におけるクライアント間リフレクションの無効化 1128
BGP-複数のクラスタ ID の設定例 1129
例：ネイバーごとのクラスタ ID 1129
例：クライアント間リフレクションの無効化 1129
その他の参考資料 1130
BGP-複数のクラスタ ID の機能情報 1131

第 68 章 **BGP-VPN 識別子属性 1135**
機能情報の確認 1135
BGP-VPN 識別子属性に関する情報 1136
VPN 識別子属性の役割と利点 1136
VPN 識別子属性の仕組み 1137
BGP-VPN 識別子属性の設定方法 1138
RT を VPN 識別子属性に置き換える 1138
VPN 識別子属性を RT に置き換える 1141
BGP-VPN 識別子属性の設定例 1144
例：RT から VPN 識別子への変換と VPN 識別子 から RT への変換 1144
その他の参考資料 1145
BGP-VPN 識別子属性の機能情報 1146

第 69 章 **BGP-RT および VPN 識別子属性の書き換えワイルドカード 1149**
機能情報の確認 1149
BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する制約事項 1150
BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する情報 1150
RT および VPN 識別子属性のマッピング範囲の利点 1150
範囲を使用してRT を RT にマッピングする方法 1151

RT を RT 範囲に置き換える 1151
RT 範囲を RT に置き換える 1154
BGP-RT および VPN 識別子属性の書き換えワイルドカードの設定例 1157
例：RT を RT 範囲に置き換える 1157
例：RT を VPN 識別子範囲に置き換える 1158
BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する追加情報 1159
BGP—RT および VPN 識別子属性の書き換えワイルドカードに関する機能情報 1159

第 70 章 VPLS BGP シグナリング 1161
機能情報の確認 1161
VPLS BGP シグナリングの前提条件 1161
VPLS BGP シグナリングに関する情報 1162
VPLS BGP シグナリングの概要 1162
VPLS BGP シグナリングの設定方法 1163
VPLS BGP シグナリングの設定 1163
VPLS BGP シグナリングの設定例 1166
例：VPLS BGP シグナリングの設定と確認 1166
VPLS BGP シグナリングの追加情報 1166
VPLS BGP シグナリングの機能情報 1167

第 71 章 マルチキャスト VPN BGP ダンプニング 1169
機能情報の確認 1169
マルチキャスト VPN BGP ダンプニングの前提条件 1170
マルチキャスト VPN BGP ダンプニングに関する情報 1170
マルチキャスト VPN BGP ダンプニングの概要 1170
マルチキャスト VPN BGP ダンプニングの設定方法 1171
マルチキャスト VPN BGP ダンプニングの設定 1171
マルチキャスト VPN BGP ダンプニングのモニタとメンテナンス 1173
マルチキャスト VPN BGP ダンプニングの設定例 1174
例：マルチキャスト VPN BGP ダンプニングの設定 1174
マルチキャスト VPN BGP ダンプニングの追加情報 1174

マルチキャスト VPN BGP ダンプニングの機能情報 1175

第 72 章 BGP—IPv6 NSR 1177

機能情報の確認 1177

BGP—IPv6 NSR の前提条件 1177

BGP-IPv6 NSR に関する情報 1178

BGP—IPv6 NSR の概要 1178

BGP-IPv6 NSR の設定方法 1179

BGP—IPv6 NSR の設定 1179

BGP-IPv6 NSR の設定例 1180

例：BGP—IPv6 NSR の設定 1180

BGP—IPv6 NSR の追加情報 1181

BGP—IPv6 NSR の機能情報 1181

第 73 章 BGP-VRF 認識の条件付きアドバタイズメント 1183

機能情報の確認 1183

BGP VRF 認識条件付きアドバタイズメントに関する情報 1184

VRF 認識条件付きアドバタイズメント 1184

BGP VRF 認識条件付きアドバタイズメントの設定方法 1185

BGP VRF 認識の条件付きアドバタイズメントの設定 1185

BGP VRF 認識条件付きアドバタイズメントの設定例 1188

例：BGP VRF 認識の条件付きアドバタイズメントの設定 1188

例：BGP VRF 認識の条件付きアドバタイズメントの確認 1190

BGP VRF 認識条件付きアドバタイズメントの追加情報 1192

BGP VRF 認識条件付きアドバタイズメントの機能情報 1193

第 74 章 BGP—選択的なルート ダウンロード 1195

機能情報の確認 1195

BGP—選択的ルート ダウンロードに関する情報 1196

専用ルート リフレクタには一部のルートしか必要ない 1196

選択的なルート ダウンロードの利点 1196

BGP ルートを選択的にダウンロードする方法 1197
専用 RR でのすべての BGP ルートのダウンロード抑止 1197
専用 RR での BGP ルートの選択的なダウンロード 1198
BGP—選択的ルート ダウンロードの設定例 1200
例：選択的なルート ダウンロード 1200
選択的なルート ダウンロードの追加情報 1202
選択的なルート ダウンロードの機能情報 1202

第 75 章 **iBGP ローカル AS に対する BGP サポート 1205**
機能情報の確認 1205
iBGP ローカル AS に対するサポートの制約事項 1206
iBGP ローカル AS に対するサポートに関する情報 1206
iBGP ローカル AS に対するサポート 1206
iBGP ローカル AS の利点 1207
iBGP ローカル AS の設定方法 1207
iBGP ローカル AS の設定 1207
iBGP ローカル AS の設定例 1210
例：iBGP ローカル AS の設定 1210
iBGP ローカル AS に対するサポートの追加情報 1211
iBGP ローカル AS に対する BGP サポートの機能情報 1211

第 76 章 **非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6） 1213**
機能情報の確認 1213
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）に関する情報 1214
非 VRF インターフェイスの eiBGP マルチパスの概要 1214
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の設定方法 1214
非 VRF インターフェイスでの IPv4/IPv6 マルチパスの有効化 1214
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の設定例 1215
例：非 VRF インターフェイスでの IPv4/IPv6 マルチパスの有効化 1215
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の機能情報 1216

第 77 章 L3VPN iBGP PE-CE 1217

機能情報の確認 1217

L3VPN iBGP PE-CE の制限 1217

L3VPN iBGP PE-CE に関する情報 1218

L3VPN iBGP PE-CE 1218

L3VPN iBGP PE-CE の設定方法 1218

L3VPN iBGP PE-CE の設定 1218

L3VPN iBGP PE-CE の設定例 1219

例：L3VPN iBGP PE-CE の設定 1219

L3VPN iBGP PE-CE の追加情報 1219

L3VPN iBGP PE-CE の機能情報 1220

第 78 章 MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート 1221

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する制約事項 1222

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する情報 1222

BGP NSR の概要 1222

相互自律システム 1223

MPLS VPNv4 および VPNv6 Inter-AS オプション B の概要 1223

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定方法 1225

Inter-AS オプション B の BGP NSR サポートを有効にするための ASBR の設定 1225

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定例 1227

例：Inter-AS オプション B の BGP NSR サポートを有効にするための ASBR の設定 1227

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する追加情報 1228

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する機能情報 1228

第 79 章 レガシー PE の BGP-RTC 1231

機能情報の確認 1231

レガシー PE の BGP-RTC の前提条件 1231

レガシー PE の BGP-RTC に関する情報 1232
レガシー PE の BGP-RTC の概要 1232
レガシー PE 対応 PE の動作 1232
レガシー PE 対応 RR の動作 1232
レガシー PE の BGP-RTC の設定方法 1233
レガシー PE の BGP-RTC の設定 1233
レガシー PE の BGP-RTC の設定例 1234
例：レガシー PE の BGP-RTC 1234
レガシー PE の BGP-RTC の追加情報 1235
レガシー PE の BGP-RTC の機能情報 1236

第 80 章 **BGP PBB EVPN ルート リフレクタのサポート** 1239
機能情報の確認 1239
BGP PBB EVPN ルート リフレクタのサポートの前提条件 1240
BGP PBB EVPN ルート リフレクタのサポートに関する情報 1240
EVPN の概要 1240
ルート リフレクタでの BGP VPLS 自動検出のサポート 1240
EVPN アドレス ファミリ 1241
BGP PBB EVPN ルート リフレクタのサポートの設定方法 1241
BGP PBB EVPN ルート リフレクタの設定 1241
BGP PBB EVPN ルート リフレクタのサポートの設定例 1243
例：BGP PBB EVPN ルート リフレクタの設定 1243
BGP PBB EVPN ルート リフレクタのサポートに関する追加情報 1243
BGP PBB EVPN ルート リフレクタのサポートの機能情報 1244

第 81 章 **BGP Monitoring Protocol** 1247
機能情報の確認 1247
BGP Monitoring Protocol の前提条件 1248
BGP Monitoring Protocol に関する情報 1248
BGP Monitoring Protocol の概要 1248
BGP Monitoring Protocol の設定方法 1249

BGP Monitoring Protocol セッションの設定 1249
BGP ネイバーでの BGP Monitoring Protocol の設定 1250
BGP Monitoring Protocol サーバの設定 1251
BGP Monitoring Protocol の確認 1254
BGP Monitoring Protocol のモニタ 1255
BGP Monitoring Protocol の設定例 1256
BGP Monitoring Protocol の設定、確認、およびモニタの例 1256
BGP Monitoring Protocol の追加情報 1260
BGP Monitoring Protocol の機能情報 1261

第 82 章 **VRF 認識 BGP 変換アップデート** 1265
機能情報の確認 1265
VRF 認識 BGP 変換アップデートの前提条件 1266
VRF 認識 BGP 変換アップデートの制約事項 1266
VRF 認識 BGP 変換アップデートに関する情報 1266
VRF 認識 BGP 変換アップデートの概要 1266
VRF 認識 BGP 変換アップデートの設定方法 1267
VRF 認識 BGP 変換アップデートの設定 1267
VRF 認識 BGP 変換アップデート設定の削除 1269
VRF 認識 BGP 変換アップデートの設定例 1271
例：VRF 認識 BGP 変換アップデートの設定 1271
例：VRF 認識 BGP 変換アップデート設定の削除 1274
VRF 認識 BGP 変換アップデートの追加情報 1275
VRF 認識 BGP 変換アップデートの機能情報 1275

第 83 章 **MTR に対する BGP サポート** 1277
機能情報の確認 1277
MTR に対する BGP サポートの前提条件 1277
MTR に対する BGP サポートの制約事項 1278
MTR に対する BGP サポートに関する情報 1278
MTR に対するルーティング プロトコル サポート 1278

BGP ネットワーク スコープ 1279
BGP 下の MTR コマンドライン インターフェイス（CLI）階層 1279
クラス固有のトポロジの BGP セッション 1280
BGP を使用したトポロジの変換 1281
BGP を使用したトポロジのインポート 1281
MTR に対する BGP のサポートの設定方法 1281
BGP を使用した MTR トポロジのアクティブ化 1281
次の作業 1286
BGP を使用した MTR トポロジからのルートのインポート 1286
MTR に対する BGP サポートの設定例 1289
例：BGP トポロジ変換コンフィギュレーション 1289
例：BGP のグローバル スコープおよび VRF コンフィギュレーション 1289
例：BGP トポロジの確認 1290
例：BGP を使用した MTR トポロジからのルートのインポート 1291
その他の参考資料 1291
MTR に対する BGP サポートに関する機能情報 1292

第 84 章 **BGP 累積 IGP** 1295
機能情報の確認 1295
BGP 累積 IGP に関する情報 1296
BGP 累積 IGP の概要 1296
BGP 累積 IGP の送受信 1296
累積 IGP を使用したプレフィックスの生成 1297
BGP 累積 IGP の設定方法 1297
AIGP メトリック値の設定 1297
AIGP 属性の送受信の有効化 1299
BGP 累積 IGP の設定 1300
BGP 累積 IGP の設定例 1301
例：AIGP メトリック値の設定 1301
例：AIGP 属性の送受信の有効化 1301
例：BGP 累積 IGP の設定 1301

BGP 累積 IGP の追加情報 1302
BGP 累積 IGP の機能情報 1302

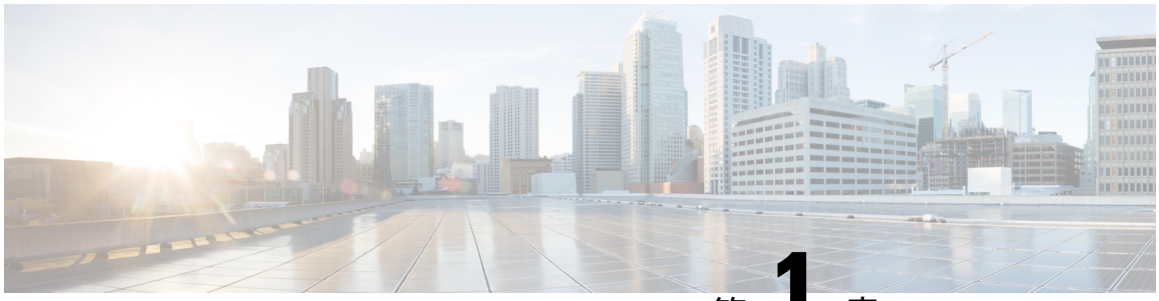
第 85 章 BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング 1305
機能情報の確認 1305
BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングに関する情報 1306
BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの概要 1306
BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定方法 1306
BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの設定 1306
BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定例 1307
例：BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの設定 1307
BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの追加情報 1308
BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの機能情報 1309

第 86 章 BGP AS オーバーライド スプリットホライズン 1311
機能情報の確認 1311
BGP AS オーバーライド スプリットホライズンに関する情報 1312
BGP AS オーバーライド スプリットホライズンの概要 1312
BGP AS オーバーライド スプリットホライズンの設定方法 1312
BGP AS オーバーライド スプリットホライズンの設定 1312
BGP AS オーバーライド スプリットホライズンの確認 1314
BGP AS オーバーライドのスプリットホライズンの設定例 1315
例：BGP AS オーバーライドのスプリットホライズンの設定 1315
例：BGP AS オーバーライドのスプリットホライズンの確認 1315
BGP AS オーバーライドのスプリットホライズンの追加情報 1317
BGP AS オーバーライドのスプリットホライズンの機能情報 1317

第 87 章 再配布ルートごとの複数送信元パスに対する BGP サポート 1319
機能情報の確認 1319
再配布ルートごとの複数送信元パスに対する BGP サポートの制約事項 1320
再配布ルートごとの複数送信元パスに対する BGP サポートに関する情報 1320

再配布ルートごとの複数送信元パスに対する BGP サポートの概要 1320
再配布ルートごとの複数送信元パスに対する BGP サポートの設定方法 1321
複数発信元パスの設定 1321
再配布ルートごとの BGP 複数送信元パスの設定例 1323
例：複数送信元パスの設定 1323
再配布ルートごとの複数送信元パスに対する BGP サポートの追加情報 1325
再配布ルートごとの複数送信元パスに対する BGP サポートの機能情報 1325

第 88 章 メンテナンス機能：BGP ルーティング プロトコル 1327
機能情報の確認 1327
メンテナンス機能：BGP ルーティング プロトコルに関する情報 1328
グローバル コンフィギュレーション モードでの BGP イベント トレースの設定 1328
EXEC モードでの BGP イベント トレースの設定 1329
BGP イベント トレースの確認 1330
メンテナンス機能：BGP ルーティング プロトコルの機能情報 1331



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

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

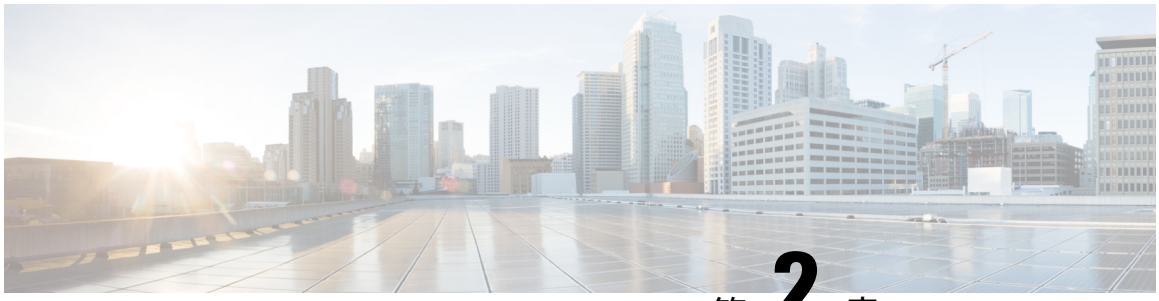
プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- Cisco IOS Command References, All Releases

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

Cisco BGP 概要

ボーダーゲートウェイプロトコル（BGP）は、独立したルーティングポリシーを持つルーティングドメイン（自律システム）の間に、ループのないルーティングを提供するように設計されたドメイン間ルーティングプロトコルです。シスコの BGP バージョン 4 のソフトウェア実装では、4 バイト自律システム番号およびマルチプロトコル拡張がサポートされており、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、バーチャルプライベートネットワーク バージョン 4（VPNv4）、コネクションレス型ネットワークサービス（CLNS）、レイヤ 2 VPN（L2VPN）を含むインターネットプロトコル（IP）マルチキャストルートおよび複数のレイヤ 3 プロトコルアドレスファミリのルーティング情報が BGP により伝送されるようになっています。このモジュールには、BGP がどのようにシスコ ソフトウェアに実装されているかの理解に役立つ概念図が含まれています。

- 機能情報の確認 （3 ページ）
- Cisco BGP の前提条件 （4 ページ）
- Cisco BGP の制約事項 （4 ページ）
- Cisco BGP に関する情報 （4 ページ）
- その他の参考資料 （21 ページ）
- Cisco BGP 概要の機能情報 （23 ページ）

機能情報の確認

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

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

Cisco BGP の前提条件

このマニュアルは、CLNS、IPv4、IPv6、マルチキャスト、VPNv4、および内部ゲートウェイ プロトコル（IGP）の知識を前提としています。各テクノロジーについて必要とされる知識の量は、導入状況によって異なります。

Cisco BGP の制約事項

シスコ ソフトウェアを実行するルータは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスおよび自律システムは、同時に使用する複数の BGP アドレス ファミリおよびサブアドレス ファミリ コンフィギュレーションをサポートできます。

Cisco BGP に関する情報

BGP バージョン 4

ボーダー ゲートウェイ プロトコル（BGP）は、独立したルーティング ポリシーを持つルーティング ドメイン（自律システム）の間に、ループのないルーティングを提供するように設計されたドメイン間ルーティング プロトコルです。BGP バージョン 4 のシスコ ソフトウェア実装では、マルチプロトコル拡張がサポートされており、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、バーチャル プライベート ネットワーク バージョン 4（VPNv4）、コネクションレス型ネットワーク サービス（CLNS）を含むインターネット プロトコル（IP）マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報が BGP により伝送されるようになっています。

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。外部組織への接続時に、外部 BGP（eBGP）ピアリング セッションが作成されます。外部 BGP ピアへの接続に関する詳細については、「外部 BGP を使用したサービス プロバイダーとの接続」の章を参照してください。

BGP は外部ゲートウェイ プロトコル（EGP）と呼ばれますが、組織における多くのネットワークは非常に複雑になりつつあるため、BGP を組織内で使用されている内部ネットワークを簡素化する際にも使用できます。同じ組織内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。内部 BGP ピアに関する詳細については、『*Cisco IOS IP Routing Configuration Guide*』の「Configuring Internal BGP Features」の章を参照してください。

（注） BGP は他のルーティング プロトコルよりも多くの設定を必要としますが、ユーザは設定変更の影響をよく理解しておく必要があります。設定が正しくないと、ルーティング ループが発生し、通常のネットワーク操作に悪影響を及ぼす可能性があります。

BGP バージョン 4 機能の概要

BGP は、組織間にループが発生しないルーティング リンクを実現することを目的としたドメイン間ルーティング プロトコルです。BGP は、信頼性の高いトランスポート プロトコル上で実行できるように設計されています。伝送制御プロトコル（TCP）はコネクション型プロトコルのため、BGP は TCP（ポート 179）をトランスポート プロトコルとして使用します。宛先の TCP ポートは 179 が割り当てられ、ローカル ポートではランダムなポート番号が割り当てられます。シスコ ソフトウェアは、BGP バージョン 4 をサポートしています。このバージョンは、インターネット サービス プロバイダー（ISP）がインターネットを構築するために使用しています。RFC 1771 では、プロトコルをインターネット規模での使用に合わせるため、新機能の BGP への追加や検討が多数行われました。RFC 2858 により、IPv4、IPv6、CLNS を含む IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報を BGP で伝送できるようにする、マルチプロトコル拡張が導入されました。

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。外部組織への接続時に、外部 BGP（eBGP）ピアリング セッションが作成されます。BGP は外部ゲートウェイ プロトコル（EGP）と呼ばれますが、組織における多くのネットワークは非常に複雑になりつつあるため、BGP を組織内で使用されている内部ネットワークを簡素化する際にも使用できます。同じ組織内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

BGP は、パスベクタ ルーティング アルゴリズムを使用して他の BGP 対応ネットワーキング デバイスとネットワーク到着可能性情報を交換します。ネットワーク到着可能性情報は、ルーティング アップデートにより BGP ピア間で交換されます。ネットワーク到着可能性情報には、ネットワーク番号、パス固有の属性、および宛先ネットワークに到達するためにルートが通過する必要がある自律システムの番号リストが含まれます。このリストは、自律システム（AS）属性に含まれます。ルーティング アップデートにローカル自律システム番号が含まれている場合、ルートはその自律システムをすでに通過していることを意味しており、ループが発生する可能性があります。そのため、BGP はローカル自律システム番号を含むすべてのルーティング アップデートを拒否することで、ルーティング ループを回避します。BGP パスベクタ ルーティング アルゴリズムは、ディスタンス ベクタ ルーティング アルゴリズムと AS パス ループ検出を組み合わせたものです。

BGP はデフォルトで、宛先ホストまたはネットワークへのベストパスとして、1 つだけパスを選択します。ベストパス選択アルゴリズムによりパス属性が分析され、BGP ルーティング テーブル内でどのルートがベスト パスとしてインストールされているかが判断されます。各パスは、BGP ベストパス分析で使用される well-known mandatory、well-known discretionary、optional transitive の各属性を伝送します。シスコ ソフトウェアは、コマンドライン インターフェイス（CLI）を通してそのような属性を変更することで、BGP パス選択に影響を与えられるように

なっています。BGP パス選択はまた、標準 BGP ポリシー設定によっても変化させることができます。BGP を使用してパス選択に影響を与えること、およびポリシーを設定してトラフィックをフィルタ処理することの詳細については、「BGP4 プレフィックス フィルタおよびインバウンド ルート マップ」モジュールおよび「BGP プレフィックス ベース アウトバウンド ルート フィルタリング」モジュールを参照してください。

BGP では、ベスト パス選択アルゴリズムを使用して、全体的に良好なルートのセットを検索します。このようなルートは、潜在的なマルチパスです。Cisco IOS Release 12.2(33)SRD 以降のリリースでは、全体的に良好なマルチパスが、許可される最大数よりも多く存在する場合、最も古いパスがマルチパスとして選択されます。

内部ゲートウェイ プロトコル（IGP）とインターフェイスすることで、BGP を複雑な内部ネットワークの管理に役立てることができます。内部 BGP は、ネットワークの効率を維持しながら既存の IGP をトラフィックの要件にあわせてスケーリングするといった問題に役立ちます。

（注） BGP は他のルーティング プロトコルよりも多くの設定を必要としますが、ユーザは設定変更の影響をよく理解しておく必要があります。設定が正しくないと、ルーティング ループが発生し、通常のネットワーク操作に悪影響を及ぼす可能性があります。

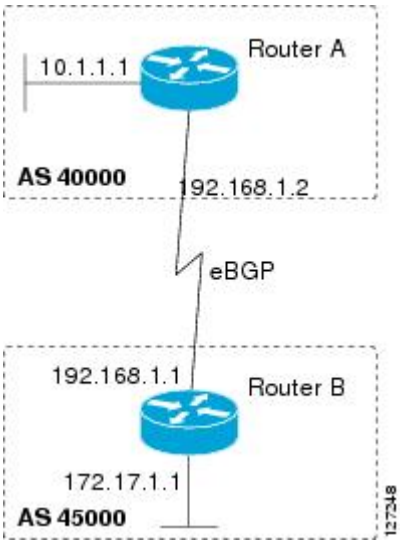
BGP 自律システム

自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。BGP 自律システムは、グローバルな外部ネットワークをローカル ルーティング ポリシーが適用できる個別のルーティング ドメインに分割する場合に使用されます。この構成により、ルーティング ドメインの管理と一貫したポリシー設定が簡素化されます。一貫したポリシー設定は、BGP により宛先ネットワークへのルートが効率的に処理されるようにするために重要です。

各ルーティング ドメインで、複数のルーティング プロトコルをサポートできます。ただし、各ルーティング プロトコルは別々に管理されます。その他のルーティング プロトコルでは、再配布により動的にルーティング情報を BGP と交換できます。別々の BGP 自律システムでは、eBGP ピアリング セッションを通じてルーティング情報が動的に交換されます。同一の自律システム内の BGP ピアでは、iBGP ピアリング セッションを通じてルーティング情報が交換されます。

下の図に、BGP で接続できる別々の自律システム内にある 2 つのルータを示します。ルータ A およびルータ B は、公共自律システム番号を使用する別々のルーティング ドメインにある ISP ルータです。トラフィックは、これらのルータによりインターネット全体に伝送されます。ルータ A およびルータ B は、eBGP ピアリング セッション経由で接続されます。

図 *1*：*2* つの自律システムを持つ *BGP* トポロジ



インターネットに直接接続する各公共自律システムには、BGP ルーティング プロセスおよび自律システムの両方を識別する一意の番号が割り当てられています。

BGP 自律システム番号の形式

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

asdot だけを使用する自律システム番号形式

Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースでは、4 オクテット（4 バイト）の自律システム番号は asdot 表記法だけで入力および表示されます。たとえば、1.10 または 45000.64000 です。4 バイト自律システム番号のマッチングに正規表現を使用する場合、

asdot 形式には正規表現で特殊文字となるピリオドが含まれていることに注意します。正規表現でのマッチングに失敗しないよう、1\.14 のようにピリオドの前にバックスラッシュを入力する必要があります。次の表は、asdot 形式だけが使用できる Cisco IOS イメージで、2 バイトおよび 4 バイト自律システム番号の設定、正規表現とのマッチング、および **show** コマンド出力での表示に使用される形式をまとめたものです。

表 *1: asdot* だけを使用する *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

asplain をデフォルトとする自律システム番号形式

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコ実装の 4 バイト自律システム番号で asplain がデフォルトの自律システム番号表示形式として使用されていますが、4 バイト自律システム番号は asplain および asdot 形式のどちらにも設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力を変更して、4 バイトの自律システム番号を asdot 形式で表示する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式が有効にされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。**show** コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト AS 番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドを有効にした後、**clear ip bgp *** コマンドを入力してすべての BGP セッションに対してハード リセットを開始する必要があります。

（注） 4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

表 *2 : asplain* をデフォルトとする *4* バイト自律システム番号形式

書式	設定形式	showコマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295

表 *3 : asdot* を使用する *4* バイト自律システム番号形式

書式	設定形式	showコマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

予約済みおよびプライベートの自律システム番号

Cisco IOS Release 12.0(32)S12、12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、12.4(24)T、およびそれ以降のリリースでは、RFC 4893 がシスコの BGP 実装でサポートされています。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。新しい予約済み（プライベート）自律システム番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を自律システム番号として設定できません。

RFC 5398『*Autonomous System (AS) Number Reservation for Documentation Use*』では、文書化を目的として新たに予約された自律システム番号について説明されています。予約済み番号を使用することで、設定例を正確に文書化しつつ、その設定がそのままコピーされた場合でも製品ネットワークに競合が発生することを防止できます。予約済み番号は IANA 自律システム番号レジストリに記載されています。予約済み 2 バイト自律システム番号は 64496 ～ 64511 の連続したブロック、予約済み 4 バイト自律システム番号は 65536 ～ 65551 をその範囲としています。

64512 ～ 65534 を範囲とするプライベートの 2 バイト自律システム番号は依然有効で、65535 は特殊な目的のために予約されています。プライベート自律システム番号は内部ルーティングドメインで使用できますが、インターネットにルーティングされるトラフィックについては変換が必要です。プライベート自律システム番号を外部ネットワークへアドバタイズするように BGP を設定しないでください。Cisco IOS ソフトウェアは、デフォルトではルーティング アップデートからプライベート自律システム番号を削除しません。ISP がプライベート自律システム番号をフィルタリングすることを推奨します。

（注） パブリック ネットワークおよびプライベート ネットワークに対する自律システム番号の割り当ては、IANA が管理しています。予約済み番号の割り当てや自律システム番号の登録申込など、自律システム番号についての情報については、http://www.iana.org/ を参照してください。

クラスレス ドメイン間ルーティング

BGP バージョン 4 では、クラスレス ドメイン間ルーティング（CIDR）がサポートされています。CIDR により、クラスフル ネットワーク境界が排除され IPv4 アドレス空間をより効率的に使用できるようになります。CIDR では、集約ルート（スーパーネット）を設定することでルーティング テーブルのサイズを縮小できます。CIDR では、プレフィックスが IP アドレスおよびビットマスク（ビットは左から右へ処理される）として処理され、各ネットワークが定義されます。プレフィックスはネットワーク、サブネットワーク、スーパーネット、または単一のホスト ルートを表すことができます。

たとえば、クラスフル IP アドレッシングを使用して、IP アドレス 192.168.2.1 はクラス C ネットワーク 192.168.2.0 内の単一のホストと定義されます。CIDR を使用すると、IP アドレスは 192.168.2.1/16 のように表示されます。これにより、192.168.0.0 のネットワーク（またはスーパーネット）が定義されます。

シスコ ソフトウェアのすべてのルーティング プロトコルでは、CIDR はデフォルトで有効になっています。CIDR を有効にするとパケットの転送方法に影響がありますが、BGP の動作は変更されません。

マルチプロトコル BGP

シスコ ソフトウェアは、RFC2858『*Multiprotocol Extensions for BGP-4*』で定義されているマルチプロトコル BGP 拡張をサポートしています。この RFC で導入された拡張により、BGP は CLNS、IPv4、IPv6、および VPNv4 を含む複数のネットワーク層プロトコルのルーティング情報を伝送できるようになりました。これらの拡張は下位互換性となっており、マルチプロトコル拡張をサポートしていないルータが、マルチプロトコル拡張をサポートしているルータと通信できるようになっています。マルチプロトコル BGP は、複数のネットワーク層プロトコルおよび IP マルチキャスト ルートに関するルーティング情報を伝送します。プロトコルに応じて、さまざまなルートのセットが BGP により伝送されます。たとえば、IPv4 ユニキャスト ルーティング用に 1 セットのルート、IPv4 マルチキャスト ルーティング用に 1 セットのルート、MPLS VPNv4 ルート用に 1 セットのルートを BGP で伝送することが可能です。

（注） マルチプロトコル BGP ネットワークは BGP ネットワークと下位互換ですが、マルチプロトコル拡張をサポートしていない BGP ピアはマルチプロトコル拡張が伝送するアドレス ファミリ識別情報などのルーティング情報を転送できません。

BGP に対しマルチプロトコル BGP を使用する利点

複数のネットワーク層プロトコルを持つ複雑なネットワークでは、マルチプロトコル BGP を使用する必要があります。あまり複雑ではないネットワークでは、次の利点があるためマルチプロトコル BGP を使用することを推奨します。

- すべての BGP コマンドおよび BGP のルーティング ポリシー機能はマルチプロトコル BGP に適用できる。
- RFC 1700『*Assigned Numbers*』で指定されているように、複数のネットワーク層プロトコル アドレス ファミリ（たとえば IP バージョン 4 または VPN バージョン 4）のルーティング情報をネットワークで伝送できる。
- 不一致のユニキャストおよびマルチキャスト トポロジをネットワークでサポートできる。
- マルチプロトコル BGP ネットワークは下位互換性となっており、マルチプロトコル拡張をサポートするルータと拡張をサポートしていないルータとの相互運用が可能。

つまり、複数のネットワーク層プロトコル アドレス ファミリに対する BGP のマルチプロトコル サポートにより、独立したポリシーおよびピアリング コンフィギュレーションをアドレス ファミリ単位で定義できる、柔軟でスケーラブルなインフラストラクチャが実現できます。

IP マルチキャストのマルチプロトコル BGP 拡張

マルチキャスト ルーティングと関連付けられたルートは、データ分散ツリーを構築するためにプロトコル独立マルチキャスト（PIM）機能で使用されます。マルチプロトコル BGP は、トラフィックの種類別に使用するリソースを制限するなどの目的で、マルチキャスト トラフィック専用のリンクが必要な場合に役立ちます。たとえば、すべてのマルチキャスト トラフィックを 1 つのネットワーク アクセス ポイント（NAP）で交換する場合です。マルチプロトコル BGP を使用すると、マルチキャスト ルーティング トポロジとは異なるユニキャスト ルーティング トポロジによって、ネットワークおよびリソースをより良く制御できるようになります。

BGP でドメイン間マルチキャスト ルーティングを実行する唯一の方法は、ユニキャスト ルーティングに対応できる BGP インフラストラクチャを使用することです。ルータがマルチキャスト対応でない場合、またはマルチキャスト トラフィック フローが必要な箇所に対して異なるポリシーがある場合は、マルチキャスト ルーティングはマルチプロトコル BGP なしではサポートされません。

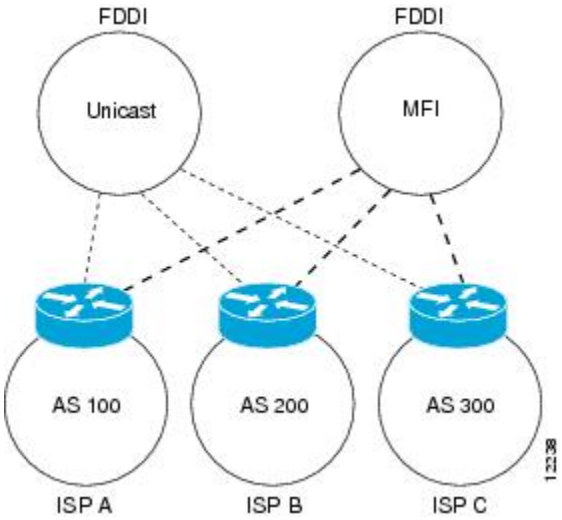
PIM などのマルチキャスト ルーティング プロトコルは、マルチキャストおよびユニキャスト BGP データベースの両方を使用して、ルートの調達、リバース パス フォワーディング（RPF）によるマルチキャスト対応ソースの検索、およびマルチキャスト分散ツリー（MDT）の構築を実行します。マルチキャスト テーブルは、ルータのプライマリ ソースですが、マルチキャスト テーブルでルートが見つからない場合はユニキャスト テーブルが検索されます。マルチキャストはユニキャスト BGP で実行できますが、マルチキャスト BGP ルートには RPF に使用する代替トポロジが許可されています。

マルチプロトコル BGP ルートが BGP に再配布される、ユニキャストおよびマルチキャスト両方のネットワーク層到着可能性情報（NLRI）を交換する BGP ピアを設定できます。ただし、

マルチプロトコル拡張はマルチプロトコル BGP をサポートしていないピアのすべてにおいて無視されます。PIM によりユニキャスト BGP ネットワークを通過するマルチキャスト分散ツリーを構築する場合（ユニキャスト ネットワークを通過するルートが最も魅力的なため）、RPF チェックが失敗し、MDT が構築されない場合があります。マルチプロトコル BGP がユニキャスト ネットワークによって実行される場合、適切なマルチキャスト アドレス ファミリを使用してピアリングを設定できます。マルチキャスト アドレス ファミリ構成では、マルチプロトコル BGP によりマルチキャスト情報が伝送でき、RPF 検索が成功します。

下の図に、不一致のユニキャストおよびマルチキャスト トポロジの簡単な例を示します。これらのトポロジ間では、マルチプロトコル BGP を実装しない場合は情報を交換できません。自律システム 100、200、および 300 は、FDDI リングである 2 つの NAP にそれぞれ接続しています。1 つはユニキャスト ピアリング（ユニキャスト トラフィックの交換）に使用されます。Multicast Friendly Interconnect（MFI）リングは、マルチキャスト ピアリング（マルチキャスト トラフィックの交換）に使用されます。各ルータは、ユニキャストおよびマルチキャスト対応です。

図 *2:* 不一致のユニキャスト ルートおよびマルチキャスト ルート



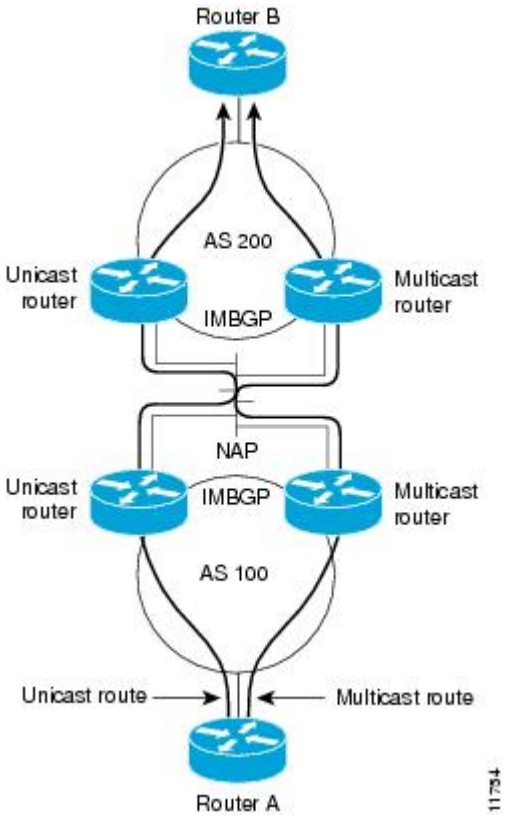
下の図は、ユニキャストだけに対応したルータおよびマルチキャストだけに対応したルータのトポロジです。左側にある 2 つのルータはユニキャストだけに対応しています（マルチキャスト ルーティングをサポートしていないか、マルチキャスト ルーティングを実行するよう設定されていない）。右側にある 2 つのルータはマルチキャストだけに対応したルータです。ルータ A および B は、ユニキャストおよびマルチキャスト ルーティングの両方をサポートしています。ユニキャストだけに対応したルータおよびマルチキャストだけに対応したルータは、1 つの NAP に接続されています。

下の図では、ユニキャスト トラフィックだけがルータ A からユニキャスト ルータを経由してルータ B との間を行き来できます。このパスでは、マルチキャスト トラフィックはフローされません。マルチキャスト ルーティングがユニキャスト ルータで設定されておらず、そのため BGP ルーティング テーブルにマルチキャスト ルートがまったく含まれていないためです。マルチキャスト ルータでは、マルチキャスト ルートが有効になり、マルチキャスト ルートを保持する個別のルーティング テーブルが BGP により構築されます。マルチキャスト トラフィッ

クは、ルータ A からマルチキャスト ルータを経由してルータ B との間を行き来するパスを使用します。

下の図に、ルータ A からルータ B へユニキャスト ルートおよびマルチキャスト ルートを別々に持つマルチプロトコル BGP 環境を示します。マルチプロトコル BGP では、これらのルートが不一致であることが許可されています。この図では、両方の自律システムに内部マルチプロトコル BGP（図中の IMBGP）が設定されている必要があります。

図 *3 :* マルチキャスト *BGP* 環境



IP マルチキャストの詳細については、「IP マルチキャストの設定」設定ライブラリを参照してください。

NLRI コンフィギュレーション CLI

BGP は、ユニキャストの IPv4 ルーティング情報だけを伝送するように設計されました。シスコ ソフトウェアの BGP 設定では、NLRI 形式の CLI が使用されました。NLRI 形式では、マルチキャスト ルーティング情報のサポートは限られており、複数のネットワーク層プロトコルはサポートされません。BGP 設定に NLRI 形式 CLI を使用することは推奨できません。

BGP ハイブリッド CLI 機能を使用すれば、アドレス ファミリ VPNv4 形式でコマンドを設定し、既存の NLRI でフォーマットされた構成を変更することなく、これらのコマンド コンフィギュレーションを保存できます。IPv4 ユニキャストまたはマルチキャストなどのその他のアド

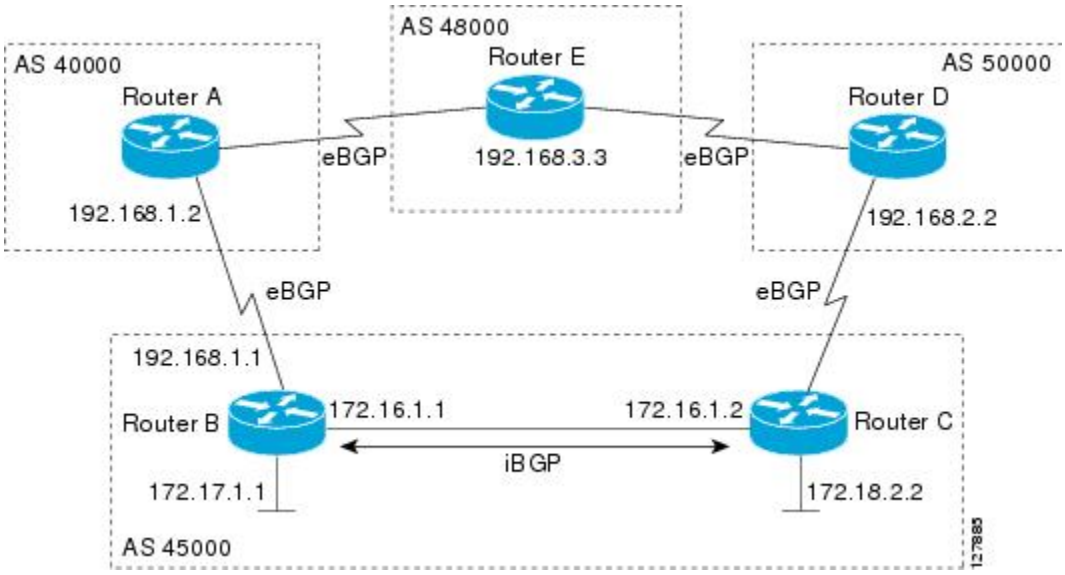
レス ファミリ コンフィギュレーションを使用する場合は、**bgp upgrade-cli** コマンドを使用して、設定をアップグレードする必要があります。

BGP ハイブリッド CLI コマンドの使用に関する詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。アドレス ファミリ設定形式、および NLRI CLI 形式の制限の詳細については、「マルチプロトコル BGP」および「Cisco BGP アドレス ファミリ モデル」の項を参照してください。

Cisco BGP アドレス ファミリ モデル

Cisco BGP の Address Family Identifier（AFI）モデルは、マルチプロトコル BGP と一緒に導入され、モジュラ式かつスケーラブルで、複数の AFI および Subsequent Address Family Identifier（SAFI）コンフィギュレーションをサポートするように設計されています。ネットワークの複雑性はさらに増しており、現在多くの企業では、多くの自律システムに接続する際に下図のネットワーク トポロジに示されているように BGP を使用しています。下の図に示されている個別の各自律システムでは、マルチプロトコル ラベル スイッチング（MPLS）および IPv6 などのいくつかのルーティング プロトコルが実行されている場合があり、ユニキャストおよびマルチキャスト両方のルートが BGP 経由で転送されることを必要とする場合があります。

図 *4:* 複数のアドレス ファミリ用の *BGP* ネットワーク トポロジ



Cisco BGP AFI モデルでは、新しい内部構造でサポートされた、新しいコマンドライン インターフェイス（CLI）コマンドが導入されています。マルチプロトコル BGP は、複数のネットワーク層プロトコルおよび IP マルチキャスト ルートに関するルーティング情報を伝送します。このルーティング情報は、AFI モデルではアペンドされた BGP 属性（マルチプロトコル拡張）として伝送されます。各アドレス ファミリでは別々の BGP データベースが保持されています。このため、BGP ポリシーをアドレス ファミリごとに設定できます。SAFI コンフィギュレーションは、親 AFI のサブセットです。SAFI は、BGP ポリシー コンフィギュレーションの再取得に使用できます。

AFI モデルは、NLRI 形式ではスケーラビリティに制限があるために作成されました。NLRI 形式で設定されたルータは、IPv4 ユニキャスト機能を備えていますが、マルチキャスト機能は限られています。NLRI 形式で設定されたネットワークには、次の制限事項があります。

- AFI および SAFI 設定情報がサポートされていない。多くの新しい BGP（および MPLS などのその他のプロトコル）機能は AFI および SAFI コンフィギュレーション モードだけでサポートされており、NLRI コンフィギュレーション モードでは設定できません。
- IPv6 がサポートされていない。NLRI 形式で設定されたルータは、IPv6 ネイバーとピアリングを構築できません。
- マルチキャスト ドメイン間ルーティングおよび不一致のマルチキャストおよびユニキャスト トポロジに対するサポートが限られている。NLRI 形式では、すべての設定オプションが使用可能というわけではなく、VPNv4 はサポートされていません。NLRI 形式コンフィギュレーションは、AFI モデルをサポートするコンフィギュレーションよりも複雑になる場合があります。インフラストラクチャ内のルータにマルチキャスト機能が備わっていない場合、またはマルチキャスト トラフィックがどのようにフローするかについての設定に関してポリシーが異なっている場合は、マルチキャスト ルーティングはサポートされません。

マルチプロトコル BGP における AFI モデルは、複数の AFI および SAFI、すべての NLRI に基づくコマンドおよびポリシー コンフィギュレーションをサポートしており、NLRI 形式だけをサポートするルータに対し下位互換性があります。AFI モデルを使用して設定されたルータには、次の機能が備わっています。

- AFI および SAFI 情報およびコンフィギュレーションがサポートされている。AFI モデルを使用して設定されたルータは、複数のネットワーク層プロトコル アドレス ファミリ（たとえば IPv4 および IPv6）のルーティング情報を伝送できます。
- AFI コンフィギュレーションはすべてのアドレス ファミリで同様であり、NLRI 形式構文よりも CLI 構文を使いやすくしている。
- すべての BGP ルーティング ポリシー機能およびコマンドがサポートされている。
- 不一致のマルチキャストおよびユニキャスト トポロジがサポートされているのと同様に、異なるポリシーを持つ一致するユニキャストおよびマルチキャスト トポロジ（BGP フィルタリング コンフィギュレーション）がサポートされている。
- CLNS がサポートされている。
- NLRI 形式だけをサポートするルータ間の相互運用がサポートされている（AFI に基づくネットワークは下位互換性）。これには、IPv4 ユニキャストおよびマルチキャスト NLRI ピアの両方が含まれています。
- バーチャル プライベート ネットワーク（VPN）および VPN ルーティング/転送（VRF）インスタンスがサポートされている。VRF のユニキャスト IPv4 は特定のアドレス ファミリ IPv4 VRF から設定できます。このコンフィギュレーション アップデートは BGP VPNv4 データベースに統合されています。

特定のアドレスファミリ コンフィギュレーション モードでは、疑問符（?）によるオンライン ヘルプ機能を使用して、サポートされているコマンドを表示できます。アドレス ファミリ コンフィギュレーション モードでサポートされている BGP コマンドとルータ コンフィギュレーション モードでサポートされている BGP コマンドでは同じ機能が設定されますが、ルータ コンフィギュレーション モードの BGP コマンドで設定されるのは IPv4 ユニキャスト アドレス プレフィックスの機能だけです。その他のアドレス ファミリ プレフィックス（たとえば、IPv4 マルチキャストまたは IPv6 ユニキャスト アドレス プレフィックス）の BGP コマンドおよび機能を設定するには、それらのアドレス プレフィックスのアドレス ファミリ コンフィギュレーション モードを開始する必要があります。

Cisco IOS ソフトウェアの BGP アドレス ファミリ モデルは、IPv4、IPv6、CLNS、および VPNv4 の 4 つのアドレス ファミリで構成されています。Cisco IOS Release 12.2(33)SRB 以降のリリースでは、L2VPN アドレス ファミリに対するサポートが追加されました。また、L2VPN アドレス ファミリ内でバーチャル プライベート LAN サービス（VPLS）SAFI がサポートされています。IPv4 および IPv6 アドレス ファミリには、マルチキャスト分散ツリー（MDT）、トンネル、および VRF などの SAFI が存在します。下の表に、Cisco IOS ソフトウェアでサポートされている SAFI のリストを示します。すべてのタイプの AFI および SAFI コンフィギュレーションを実行するネットワーク間における互換性を確保するには、マルチプロトコル BGP アドレス ファミリ モデルを使用して Cisco IOS デバイスに BGP を設定することを推奨します。

表 *4 : Cisco IOS* ソフトウェアでサポートされる *SAFI*

SAFI フィールド値	説明	参照先
1	ユニキャスト フォワーディングに使用される NLRI	RFC 2858
2	マルチキャスト フォワーディングに使用される NLRI	RFC 2858
3	ユニキャストおよびマルチキャスト フォワーディングの両方に使用される NLRI	RFC 2858
4	MPLS ラベル付き NLRI	RFC 3107
64	トンネル SAFI	draft-nalawade-kapoor-tunnel-safi -01.txt
65	バーチャル プライベート LAN サービス（VPLS）	-
66	BGP MDT SAFI	draft-nalawade-idr-mdt-safi-00.txt
128	MPLS ラベル付き VPN アドレス	RFC-ietf-l3vpn-rfc2547bis-03.txt

IPv4 アドレス ファミリ

IPv4 アドレス ファミリは、標準 IP バージョン 4 アドレス プレフィックスを使用する BGP などのプロトコルのルーティング セッションを識別する場合に使用されます。ユニキャストまたはマルチキャスト アドレス プレフィックスは、IPv4 アドレス ファミリ内で指定できます。デフォルトでは、アドレス ファミリ IPv4 ユニキャストのルーティング情報は、ユニキャスト IPv4 情報のアドバタイズメントが明示的にオフにされていない限り、BGP ピアが設定されたことときにアドバタイズされます。

VRF インスタンスも、IPv4 AFI コンフィギュレーション モード コマンドと関連付けできます。

Cisco IOS Release 12.0(28)S では、マルチポイント トンネリング IPv4 ルーティング セッションをサポートするためにトンネル SAFI が追加されました。トンネル SAFI は、トンネル タイプとトンネル機能を含む SAFI 固有属性およびトンネル エンドポイントをアドバタイズするために使用されます。トンネル アドレス ファミリが設定されたときに、トンネル エンドポイントが BGP IPv4 トンネル SAFI テーブルへ自動的に再配布されます。ただし、トンネル情報がセッションで交換されるようにするには、トンネル アドレス ファミリでピアをアクティブ化する必要があります。

Cisco IOS Release 12.0(29)S では、マルチキャスト VPN アーキテクチャをサポートするためにマルチキャスト分散ツリー（MDT）SAFI が追加されました。MDT SAFI はマルチキャスト対応の推移的なコネクタ属性で、BGP では IPv4 アドレス ファミリとして定義されています。MDT アドレス ファミリ セッションは、IPv4 マルチキャスト アドレス ファミリで SAFI として動作し、プロバイダー エッジ（PE）ルータで設定されて AS 間マルチキャスト VPN ピアリング セッションをサポートする カスタマーエッジ（CE）ルータと VPN ピアリング セッションを確立します。

IPv6 アドレス ファミリ

IPv6 アドレス ファミリは、標準 IPv6 アドレス プレフィックスを使用する BGP などのプロトコルのルーティング セッションを識別する場合に使用されます。ユニキャストまたはマルチキャスト アドレス プレフィックスは、IPv6 アドレス ファミリ内で指定できます。

（注） デフォルトでは、アドレス ファミリ IPv4 ユニキャストのルーティング情報は、ユニキャスト IPv4 情報のアドバタイズメントを明示的にオフにしない限り、BGP ピアを設定したときにアドバタイズされます。

CLNS アドレス ファミリ

CLNS アドレス ファミリは、標準ネットワーク サービス アクセス ポイント（NSAP）アドレス プレフィックスを使用する BGP などのプロトコルのルーティング セッションを識別する場合に使用されます。NSAP アドレス プレフィックスが設定されたとき、ユニキャスト アドレス プレフィックスがデフォルトとなります。

CLNS ルートは、CLNS アドレスが設定されたネットワークで使用されます。これはテレコミュニケーション データ通信ネットワーク（DCN）の典型です。ピアリングは IP アドレスを使用して確立されますが、アップデート メッセージには CLNS ルートが含まれます。

CLNS ネットワークのスケーリング機能を提供する、CLNS に対する BGP サポートの設定の詳細については、「CLNS に対するマルチプロトコル BGP（MP-BGP）サポートの設定」モジュールを参照してください。

VPNv4 アドレス ファミリ

VPNv4 マルチキャスト アドレス ファミリは、標準 VPN バージョン 4 アドレス プレフィックスを使用する BGP などのプロトコルのルーティング セッションを識別する場合に使用されます。VPNv4 アドレス プレフィックスが設定されたとき、ユニキャスト アドレス プレフィックスがデフォルトとなります。VPNv4 ルートは IPv4 ルートと同様ですが、VPNv4 ルートにはプレフィックスのレプリケーションを許可するルート ディスクリプタ（RD）がプリペンドされています。異なる各 RD を異なる VPN に関連付けることが可能です。各 VPN には、独自のプレフィックス セットが必要です。

企業は、アプリケーションおよびデータ ホスティング、ネットワーク商取引、電話サービスといったビジネス カスタマーへの付加価値サービスを展開および管理する基盤として IP VPN を使用します。

プライベート LAN では、IP をベースとしたイントラネットにより、企業のビジネス実践のあり方が根本的に変化しました。企業は、イントラネットのビジネス アプリケーションを WAN で拡大することに移行しつつあります。また、企業はエクストラネット（複数のビジネスを包含するイントラネット）を使用してカスタマー、サプライヤ、およびパートナーのニーズに取り組んでいます。エクストラネットにより、企業はサプライチェーンの自動化、電子データ交換（EDI）、およびその他のネットワーク商取引の形態を簡易化することで、ビジネスプロセスのコストを削減します。このビジネス チャンスを活かすには、サービス プロバイダーはパブリック インフラストラクチャを通じてビジネスにプライベート ネットワーク サービスを提供する IP VPN インフラストラクチャを持つ必要があります。

MPLS とあわせて VPN を使用した場合、サービス プロバイダーのネットワークを通じて複数の拠点同士を透過的に相互接続することが可能になります。1 つのサービス プロバイダー ネットワークで、複数の異なる IP VPN のサポートが可能です。これらはそれぞれ、そのユーザにとってはその他すべてのネットワークとは隔離されたプライベート ネットワークとして現れます。1 つの VPN 内では、各拠点は同一 VPN 内のいずれの拠点にも IP パケットを送信できます。各 VPN は 1 つ以上の VPN VRF に関連付けられます。VPNv4 ルートは、すべての VRF のルートのスーパーセットであり、特定の VRF アドレス ファミリにおいて VRF ごとにルート挿入が行われます。ルータは、各 VRF に対し別々のルーティングおよび Cisco Express Forwarding（CEF）テーブルを保持します。これにより、情報が VPN 外に送信されることが回避でき、重複 IP アドレスの問題を起こすことなく同一のサブネットが複数の VPN で使用可能になります。BGP を使用しているルータは、BGP 拡張コミュニティを使用して VPN のルーティング情報を配布します。

VPN アドレス空間は、設計によりグローバル アドレス空間から隔離されます。ある VPN へのルートはその VPN のその他のメンバだけが学習できるように、VPN-IPv4 プレフィックスの到

着可能性情報はBGPによりVPNv4マルチプロトコル拡張を使用して各VPNに配布されます。これにより VPN のメンバが相互に通信できるようになります。

RFC 3107 に、SAFI を使用してマルチプロトコル BGP アドレス ファミリにラベル情報を追加する方法が指定されています。Cisco IOS 実装の MPLS では、IPv4 ルートをラベルと一緒に送信するサポートの提供に RFC 3107 が使用されています。VPNv4 には、暗黙的に各ルートに関連付けられたラベルが備わっています。

L2VPN アドレス ファミリ

L2VPN は、IP セキュリティ（IPsec）または総称ルーティング カプセル化（GRE）などの暗号化テクノロジーを使用して、セキュアでないネットワーク内で運用されるセキュアなネットワークと定義されています。L2VPNアドレス ファミリはBGPルーティング コンフィギュレーション モードで設定され、L2VPN アドレス ファミリ内では VPLS Subsequent Address Family Identifier（SAFI）がサポートされています。

L2VPN アドレス ファミリに対する BGP サポートでは、L2VPN エンドポイント プロビジョニング情報を配布するBGPをベースとしたオートディスカバリ メカニズムが導入されています。BGP では、エンドポイント プロビジョニング情報を保存する際に個別の L2VPN ルーティング情報ベース（RIB）が使用されます。これは、レイヤ 2 Virtual Forwarding Instance（VFI）が設定されたときに毎回アップデートされます。プレフィックスおよびパス情報は L2VPN データベースに保存され、ベスト パスが BGP により決定されるようになります。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、エンドポイント情報を使用して Pseudowire メッシュがセットアップされます。

BGP オートディスカバリ メカニズムにより、Cisco IOS Virtual Private LAN Service（VPLS）機能に必要不可欠な L2VPN サービスのセットアップが簡易化されます。VPLS は、高速イーサネットを使用した堅牢でスケーラブルな IP MPLS ネットワークによる大規模な LAN として、地理的に分散した拠点間を接続することで柔軟なサービスの展開を実現します。VPLS の詳細については、「VPLS Autodiscovery: BGP Based」機能を参照してください。

L2VPN アドレス ファミリでは、次の BGP コマンドライン インターフェイス（CLI）コマンドがサポートされています。

- **bgp scan-time**
- **bgp nexthop**
- **neighbor activate**
- **neighbor advertisement-interval**
- **neighbor allowas-in**
- **neighbor capability**
- **neighbor inherit**
- **neighbor peer-group**
- **neighbor maximum-prefix**

- **neighbor next-hop-self**
- **neighbor next-hop-unchanged**
- **neighbor remove-private-as**
- **neighbor route-map**
- **neighbor route-reflector-client**
- **neighbor send-community**
- **neighbor soft-reconfiguration**
- **neighbor soo**
- **neighbor weight**

（注） L2VPN を使用したルート リフレクタでは、**neighbor next-hop-self** コマンドおよび **neighbor next-hop-unchanged** コマンドはサポートされていません。

L2VPN アドレス ファミリ コンフィギュレーションで使用された場合、BGP 内で使用されるルートマップでは、プレフィックス処理、タグ処理、および自動タグ処理に関連するすべてのコマンドは無視されます。その他すべてのルート マップ コマンドはサポートされています。

L2VPN アドレス ファミリでは、BGP マルチパスおよびコンフェデレーションはサポートされていません。

L2VPN アドレス ファミリでの BGP 設定の詳細については、「L2VPN アドレス ファミリに対する BGP サポート」モジュールを参照してください。

BGP CLI 削除の考慮事項

小規模な BGP ネットワークであっても、BGP CLI コンフィギュレーションは非常に複雑になることがあります。すべての CLI コンフィギュレーションを削除する必要がある場合は、CLI を削除することで生じるあらゆる影響を考慮する必要があります。現在の実行コンフィギュレーションを分析し、現在の BGP ネイバー関係、アドレス ファミリの考慮事項、その他の設定済みルーティング プロトコルを判断します。BGP CLI コマンドの多くは、CLI コンフィギュレーションのその他の部分に影響を与えています。たとえば次のコンフィギュレーションでは、ルート マップは BGP 自律システム番号の一致に使用され、その後一致したルートを拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）のその他の自律システム番号にセットする際に使用されます。

```
route-map bgp-to-eigrp permit 10
 match tag 50000
 set tag 65000
```

3 つの異なる自律システムにある BGP ネイバーが設定およびアクティブ化されます。

```
router bgp 45000
```

```
bgp log-neighbor-changes
address-family ipv4
 neighbor 172.16.1.2 remote-as 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 172.16.1.2 activate
 neighbor 192.168.1.2 activate
 neighbor 192.168.3.2 activate
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

その後、EIGRP ルーティング プロセスが設定され、ルート マップによりルートがフィルタ処理されて BGP ルートが EIGRP に再配布されます。

```
router eigrp 100
 redistribute bgp 45000 metric 10000 100 255 1 1500 route-map bgp-to-eigrp
 no auto-summary
 exit
```

後でルート マップを削除する場合は、**route-map** コマンドの **no** 形式を使用します。ほぼすべてのコンフィギュレーション コマンドには **no** 形式があります。通常、**no** 形式は機能を無効にします。しかし、このコンフィギュレーションの例では、ルートマップを無効にしただけではルート再配布は停止しません。ルートマップからのフィルタ処理または照合が行われなくなるだけです。ルートマップを使用しないで再配布を行うと、ご使用のネットワークで予期しない動作が生じるおそれがあります。アクセス リストまたはルート マップを削除する場合は、そのアクセス リストまたはルート マップを参照しているコマンドを確認して、意図した動作が得られるかどうかを検討する必要もあります。

次のコンフィギュレーションでは、ルート マップおよび再配布の両方が削除されます。

```
configure terminal
 no route-map bgp-to-eigrp
 router eigrp 100
  no redistribute bgp 45000
  end
```

BGP CLI コンフィギュレーションを削除する設定の詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準

標準	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB のリンク
CISCO-BGP4-MIB	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

RFC

RFC	タイトル
RFC 1700	『*Assigned Numbers*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4893	『*BGP Support for Four-Octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous System (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

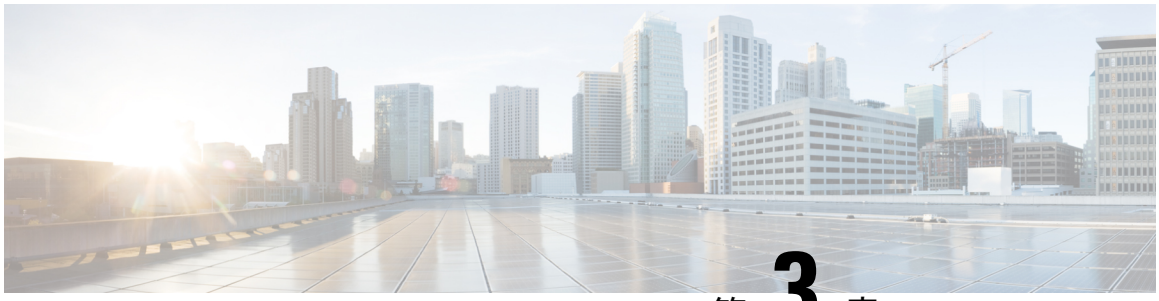
Cisco BGP 概要の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *5 : Cisco BGP* 概要の機能情報

機能名	リリース	機能情報
マルチプロトコル BGP	Cisco IOS XE 3.1.0SG	Cisco IOS ソフトウェアは、RFC 2858『*Multiprotocol Extensions for BGP-4*』で定義されているマルチプロトコル BGP 拡張をサポートしています。この RFC で導入された拡張により、BGP は CLNS、IPv4、IPv6、および VPNv4 を含む複数のネットワーク層プロトコルのルーティング情報を伝送できるようになりました。これらの拡張は下位互換性となっており、マルチプロトコル拡張をサポートしていないルータが、マルチプロトコル拡張をサポートしているルータと通信できるようになっています。マルチプロトコル BGP は、複数のネットワーク層プロトコルおよび IP マルチキャスト ルートに関するルーティング情報を伝送します。



第 3 章

BGP 4

BGP は、独自のルーティング ポリシー（自律システム）を持つ異なるルーティング ドメイン間に、ループのないルーティングを行うように設計されたドメイン間ルーティング プロトコルです。

- 機能情報の確認 （25 ページ）
- BGP 4 に関する情報 （25 ページ）
- BGP 4 の設定方法 （33 ページ）
- BGP 4 の設定例 （70 ページ）
- その他の参考資料 （76 ページ）
- BGP 4 の機能情報 （77 ページ）

機能情報の確認

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

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

BGP 4 に関する情報

BGP バージョン 4 機能の概要

BGP は、組織間にループが発生しないルーティング リンクを実現することを目的としたドメイン間ルーティング プロトコルです。BGP は、信頼性の高いトランスポート プロトコル上で

実行できるように設計されています。伝送制御プロトコル（TCP）はコネクション型プロトコルのため、BGP は TCP（ポート 179）をトランスポート プロトコルとして使用します。宛先の TCP ポートは 179 が割り当てられ、ローカル ポートではランダムなポート番号が割り当てられます。シスコ ソフトウェアは、BGP バージョン 4 をサポートしています。このバージョンは、インターネット サービス プロバイダー（ISP）がインターネットを構築するために使用しています。RFC 1771 では、プロトコルをインターネット規模での使用に合わせるため、新機能の BGP への追加や検討が多数行われました。RFC 2858 により、IPv4、IPv6、CLNS を含む IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報を BGP で伝送できるようにする、マルチプロトコル拡張が導入されました。

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。外部組織への接続時に、外部 BGP（eBGP）ピアリング セッションが作成されます。BGP は外部ゲートウェイ プロトコル（EGP）と呼ばれますが、組織における多くのネットワークは非常に複雑になりつつあるため、BGP を組織内で使用されている内部ネットワークを簡素化する際にも使用できます。同じ組織内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

BGP は、パスベクタ ルーティング アルゴリズムを使用して他の BGP 対応ネットワーキング デバイスとネットワーク到着可能性情報を交換します。ネットワーク到着可能性情報は、ルーティング アップデートにより BGP ピア間で交換されます。ネットワーク到着可能性情報には、ネットワーク番号、パス固有の属性、および宛先ネットワークに到達するためにルートが通過する必要がある自律システムの番号リストが含まれます。このリストは、自律システム（AS）属性に含まれます。ルーティング アップデートにローカル自律システム番号が含まれている場合、ルートはその自律システムをすでに通過していることを意味しており、ループが発生する可能性があります。そのため、BGP はローカル自律システム番号を含むすべてのルーティング アップデートを拒否することで、ルーティング ループを回避します。BGP パスベクタ ルーティング アルゴリズムは、ディスタンス ベクタ ルーティング アルゴリズムと AS パス ループ検出を組み合わせたものです。

BGP はデフォルトで、宛先ホストまたはネットワークへのベストパスとして、1 つだけパスを選択します。ベストパス選択アルゴリズムによりパス属性が分析され、BGP ルーティング テーブル内でどのルートがベスト パスとしてインストールされているかが判断されます。各パスは、BGP ベストパス分析で使用される well-known mandatory、well-known discretionary、optional transitive の各属性を伝送します。シスコ ソフトウェアは、コマンドライン インターフェイス（CLI）を通してそのような属性を変更することで、BGP パス選択に影響を与えられるようになっています。BGP パス選択はまた、標準 BGP ポリシー設定によっても変化させることができます。BGP を使用してパス選択に影響を与えること、およびポリシーを設定してトラフィックをフィルタ処理することの詳細については、「BGP 4 プレフィックス フィルタおよびインバウンド ルート マップ」モジュールおよび「BGP プレフィックス ベース アウトバウンド ルート フィルタリング」モジュールを参照してください。

BGP では、ベスト パス選択アルゴリズムを使用して、全体的に良好なルートのセットを検索します。このようなルートは、潜在的なマルチパスです。Cisco IOS Release 12.2(33)SRD 以降のリリースでは、全体的に良好なマルチパスが、許可される最大数よりも多く存在する場合、最も古いパスがマルチパスとして選択されます。

内部ゲートウェイプロトコル（IGP）とインターフェイスすることで、BGPを複雑な内部ネットワークの管理に役立てることができます。内部 BGP は、ネットワークの効率を維持しながら既存のIGPをトラフィックの要件にあわせてスケーリングするといった問題に役立ちます。

（注） BGP は他のルーティング プロトコルよりも多くの設定を必要としますが、ユーザは設定変更の影響をよく理解しておく必要があります。設定が正しくないと、ルーティング ループが発生し、通常のネットワーク操作に悪影響を及ぼす可能性があります。

BGP ルータ ID

BGP では、ルータ ID を使用して、BGP スピーキング ピアを識別します。BGP ルータ ID は 32 ビット値であり、IPv4 アドレスで表すことがよくあります。デフォルトでは、シスコ ソフトウェアによって、ルータ ID がルータ上のループバック インターフェイスの IPv4 アドレスに設定されます。デバイス上でループバック インターフェイスが設定されていない場合は、BGP ルータ ID を表すためにデバイスの物理インターフェイスに設定されている最上位の IPv4 アドレスがソフトウェアによって選択されます。BGP ルータ ID は、ネットワーク内の BGP ピアごとに一意である必要があります。

BGP スピーカーとピア関係

BGP 対応デバイスは、別の BGP 対応デバイスを自動的には検出しません。ネットワーク管理者は、通常、BGP 対応デバイス間の関係を手動で設定します。ピア デバイスとは、別の BGP 対応デバイスへのアクティブな TCP 接続を持つ BGP 対応デバイスです。この BGP デバイス間の関係がネイバーと呼ばれることはよくありますが、これは BGP デバイスは直接接続されていて、その間に他のデバイスははさまっていないということを暗示することがあるため、このマニュアルではネイバーという語の使用は極力避けています。BGP スピーカーはローカル デバイスのことで、その他の BGP 対応ネットワーク デバイスはすべてピアです。

ピアとピアの間に TCP 接続が確立されると、最初、個々の BGP ピアはもう 1 つのピアと、そのルート（完成したBGPルーティングテーブル）をすべて交換します。この交換の後は、ネットワークでトポロジの変更が行われたとき、あるいはルーティング ポリシーが実装または変更されたときに差分更新が送信されるだけです。更新と更新の間の非アクティブ期間には、ピアは「キープアライブ」と呼ばれる特別なメッセージを交換します。

BGP 自律システムは、単一のアドミニストレーション エンティティにより制御されるネットワークです。ピア デバイスは、異なる自律システムに存在する場合は外部ピア、同一の自律システムに存在する場合は内部ピアと呼ばれます。通常、外部ピアは隣接し、サブネットを共有していますが、内部ピアは同じ自律システムのどのような場所にあってもかまいません。

BGP ピア セッションの確立

BGP ルーティング プロセスがピアとピアリング セッションを確立するとき、ステートは次のように変化します。

- Idle：ルーティング プロセスが有効になったとき、またはデバイスがリセットされたときの BGP ルーティング プロセスの初期ステート。このステートでは、デバイスはリモート ピアとのピアリング設定など、開始イベントを待ちます。リモート ピアから TCP 接続要求を受信すると、デバイスはリモート ピアへの TCP 接続を開始する前に、タイマーを待機するための開始イベントを新たに開始します。デバイスがリセットされ、ピアがリセットされると、BGP ルーティング プロセスは Idle ステートに戻ります。
- Connect：ローカル BGP スピーカーとの TCP セッションを確立しようとしていることを BGP ルーティング プロセスが検知します。
- Active：このステートでは、BGP ルーティング プロセスは、ConnectRetry タイマーを使用して、ピア デバイスとの TCP セッションを確立しようとします。BGP ルーティング プロセスが Active ステートの間、開始イベントは無視されます。BGP ルーティング プロセスが再構成された場合、またはエラーが発生した場合、BGP ルーティング プロセスはシステム リソースを解放し、Idle ステートに戻ります。
- OpenSent：TCP 接続が確立され、BGP ルーティング プロセスはリモート ピアに OPEN メッセージを送信し、OpenSent ステートに移行します。このステートでは、BGP ルーティング プロセスはその他の OPEN メッセージを受信できます。接続に失敗した場合、BGP ルーティング プロセスは Active ステートに移行します。
- OpenReceive：BGP ルーティング プロセスはリモート ピアから OPEN メッセージを受信し、リモート ピアからの最初のキープアライブ メッセージを待ちます。キープアライブ メッセージを受信すると、BGP ルーティング プロセスは Established ステートに移行します。通知メッセージを受信した場合は、BGP ルーティング プロセスは Idle ステートに移行します。ピアリング セッションに影響を与えるエラー、または設定変更が発生した場合、BGP ルーティング プロセスは、有限状態マシン（FSM）エラー コードが入った通知メッセージを送信してから、Idle ステートに移行します。
- Established：リモート ピアから最初のキープアライブが受信されます。これにより、リモート ネイバーとのピアリングが確立され、BGP ルーティング プロセスは、リモート ピアとのアップデート メッセージの交換を開始します。アップデート メッセージ、またはキープアライブ メッセージが受信されると、ホールド タイマーが再起動されます。エラー通知を受信した BGP プロセスは、Idle ステートに移行します。

BGP セッションのリセット

設定変更のためにルーティング ポリシーに変更が生じた場合は、必ず **clear ip bgp** コマンドを使用して、BGP ピアリング セッションをリセットする必要があります。シスコ ソフトウェアは、BGP ピアリング セッションのリセットとして、次の 3 つのメカニズムをサポートしています。

- ハード リセット：ハード リセットは、TCP 接続を含む指定されたピアリング セッションを終了し、指定されたピアから到着したルートを削除します。
- ソフト リセット：ソフト リセットは、保存されたプレフィックス情報を使用し、既存のピアリング セッションを廃棄せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アッ

プデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しいBGPポリシーを適用することができます。ソフト再構成は、インバウンドセッション、またはアウトバウンドセッションに対して設定できます。

- ダイナミック インバウンド ソフト リセット：これは RFC 2918 に定義されているルートリフレッシュ機能で、サポートしているピアへのルートリフレッシュ要求を交換することにより、ローカル デバイスがインバウンド ルーティング テーブルを動的にリセットできるようにするものです。ルートリフレッシュ機能は、中断を伴わないポリシー変更についてはアップデート情報をローカルに保存しません。その代わり、サポートしているピアとの動的な交換に依存します。ルートリフレッシュは、最初にピア間のBGP機能ネゴシエーションを通じてアドバタイズされる必要があります。すべての BGP デバイスが、ルートリフレッシュ機能をサポートしていなければなりません。BGP デバイスがこの機能をサポートしているかどうかを確認するには、**show ip bgp neighbors** コマンドを使用します。デバイスがルートリフレッシュ機能をサポートしている場合、次のメッセージが出力されます。

```
Received route refresh capability from peer.
```

bgp soft-reconfig-backup コマンドは、ルートリフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を実行するように BGP を設定するために導入されました。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。

BGP ルート集約

BGP ピアはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約を使用することにより、関係する情報の量が減ります。集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティングテーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。これにより、アドバタイズが必要なルートの数が少なくなります。

BGPでのルート集約の実装方法は2種類あります。集約されたルートをBGPに再配布するか、または条件付き集約の形を使用することができます。基本ルートの再配布では、集約ルートの作成後、このルートが BGP に再配布されます。条件付き集約では、集約ルートの作成後、アドバタイズするか、または Autonomous System Set Path（AS-SET）情報、もしくは要約情報に基づいて、特定ルートのアドバタイズを抑制します。

bgp suppress-inactive コマンドは、非アクティブのルートをどの BGP ピアにもアドバタイズしないように BGP を設定します。BGP ルーティング プロセスは、デフォルトで、ルーティング情報データベース（RIB）にインストールされていないルートをBGPピアにアドバタイズできます。RIBにインストールされていないルートは非アクティブなルートです。非アクティブなルートのアドバタイズメントは、たとえば、共通のルート集約を通じてルートがアドバタイズされた場合に行われます。非アクティブなルートのアドバタイズメントを抑制して、より整合性の取れたデータ フォワーディングを行うことができます。

BGP ルート集約の AS_SET 情報生成

AS_SET 情報は、**aggregate-address** コマンドを使用して、BGP ルートが集約されたときに生成されます。このようなルートについてアドバタイズされたパスは、コミュニティを含め、要約されているすべてのパスに含まれる、すべての要素から構成される AS_SET です。集約される AS_PATH が同じものである場合、AS_PATH だけがアドバタイズされます。**aggregate-address** コマンド用にデフォルトで設定されている ATOMIC-AGGREGATE 属性は、AS_SET には追加されません。

ルーティング ポリシーの変更管理

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブルの更新に影響する可能性のあるルート マップ、配布リスト、プレフィックス リスト、フィルタ リストなど、すべての要素に関するコンフィギュレーションが含まれています。ルーティング ポリシーを変更した場合、変更後のポリシーを有効にするには、必ず BGP セッションをソフト クリア、またはソフト リセットしてください。インバウンド リセットを実行すると、デバイスで設定されている新しいインバウンド ポリシーが有効になります。アウトバウンド リセットを実行すると、BGP セッションをリセットしなくても、デバイスで設定されている新しいローカル アウトバウンド ポリシーが有効になります。アウトバウンド ポリシーのリセット中に、新しい一連のアップデートが送信されると、ネイバーの新しいインバウンドポリシーも有効になります。つまり、インバウンド ポリシーの変更後は、ローカル デバイスでインバウンド リセットを実行するか、ピア デバイスでアウトバウンド リセットを実行する必要があります。アウトバウンド ポリシーを変更した場合は、ローカル デバイスでのアウトバウンド リセット、またはピア デバイスでのインバウンド リセットが必要になります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。下の表は、これらの利点と欠点をまとめたものです。

表 *6:* ハード リセットとソフト リセットの利点および欠点

リセット タイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが起こらない。	ネイバーにより提供される BGP、IP、および転送情報ベース（FIB）テーブル内のプレフィックスが失われる。ハード リセットは推奨されない。
発信ソフト リセット	設定が必要ない。ルーティング テーブル アップデートの保存が必要ない。	インバウンド ルーティング テーブル アップデートがリセットされない。

リセット タイプ	利点	欠点
ダイナミック インバウンド ソフト リセット	BGP セッションおよびキャッシュがクリアされない。 ルーティング テーブル アップデートの保存が必要ない。また、メモリのオーバーヘッドが発生しない。	両方のBGPデバイスがルート リフレッシュ機能をサポートしていなければならない。 （注） アウトバウンド ルーティング テーブル アップデートがリセットされない。
設定済みのインバウンド ソフト リセット（**neighbor soft-reconfiguration** ルータ コンフィギュレーション コマンドを使用）	どちらの BGP デバイスも自動ルート リフレッシュ機能をサポートしていない場合に使用可能。 **bgp soft-reconfig-backup** コマンドは、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を設定するために導入された。	再構成が必要である。 受信した（インバウンド）ルーティング ポリシー アップデートをすべてそのまま格納するため、メモリが大量に使用される。 どちらの BGP デバイスも自動ルート リフレッシュ機能をサポートしていない場合など、絶対に必要な場合だけ推奨される。 （注） アウトバウンド ルーティング テーブル アップデートがリセットされない。

BGP ネイバーになるように定義された 2 つのデバイスは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィギュレーションの変更を有効にするために、BGP 接続をリセットする必要があります。

ソフト リセットは、インバウンドおよびアウトバウンド ルーティング アップデートで使用されるルーティング テーブルをアップデートします。シスコ ソフトウェアでは、事前に設定を行わなくても、ソフト リセットを使用できます。このソフト リセットにより、BGP デバイスの間でルート リフレッシュ要求やルーティング情報をダイナミックに交換し、対応するアウトバウンド ルーティング テーブルをアドバタイズできるようになります。ソフト リセットには 2 種類があります。

- ソフトリセットを使用して、ネイバーからインバウンドアップデートを生成することを、ダイナミック インバウンド ソフト リセットと呼びます。
- ソフトリセットを使用して、ネイバーに新しい一連のアップデートを送信することを、アウトバウンド ソフト リセットと呼びます。

事前にコンフィギュレーションを行わずにソフト リセットを使用するためには、BGP ピアでソフトルートリフレッシュ機能がサポートされていなければなりません。これは、ピアがTCP セッションを確立したときに送信される OPEN メッセージでアドバタイズされます。

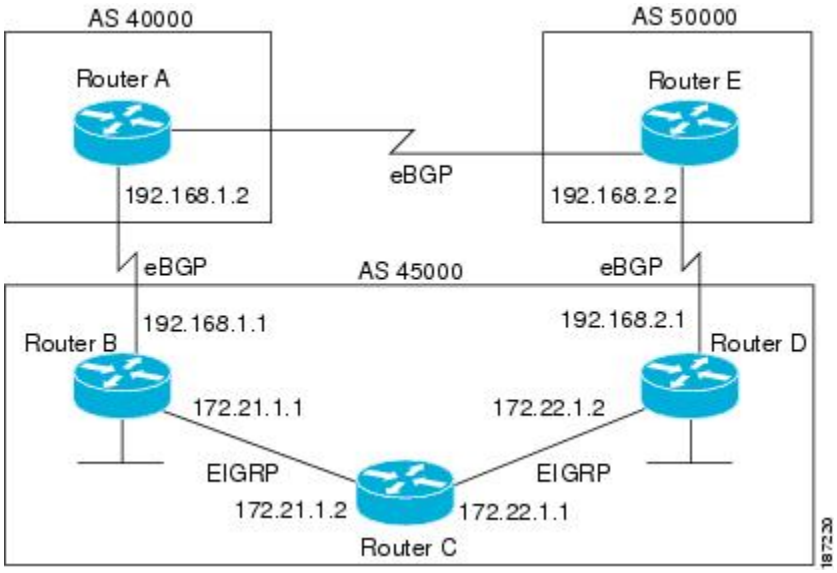
BGP ピア グループ

BGP ネットワークでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります. 同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、コンフィギュレーションのアップデートをより効率化するために、BGP ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

BGP バックドア ルート

さまざまな自律システムとの通信に eBGP を使用する境界デバイスを 2 つ使った BGP ネットワーク トポロジでは、2つの境界デバイス間の通信で、最も効果的なルーティング方法はeBGPを使用することではありません。下の図では、ルータ B はBGP スピーカーとして、eBGP を通るルータ D へのルートを受け取りますが、このルートは少なくとも 2 つの自律システムを横切っています。また、ルータ B とルータ D はEnhanced Interior Gateway Routing Protocol（EIGRP）ネットワーク（ここでは、すべてのIGPを使用可能）を通じて接続されていますが、これが最短ルートです。しかし、EIGRP ルートのデフォルト アドミニストレーティブ ディスタンスは 90 で、eBGP ルートのデフォルト アドミニストレーティブ ディスタンスは 20 であるため、BGP は eBGP ルートを選びます。アドミニストレーティブ ディスタンスを変更すると、ルーティングがループする可能性があるため、デフォルト アドミニストレーティブ ディスタンスの変更は推奨しません。BGP に EIGRP ルートを選択させるには、**network backdoor** コマンドを使用します。BGP は、**network backdoor** コマンドで指定されたネットワークをローカルに割り当てられたネットワークとして扱います。ただし、BGPアップデートで指定されたネットワークのアドバタイズは行いません。これは、 下の図では、ルータ B は長い eBGP ルートの代わりに、短い EIGRP を使ってルータ D と通信するという意味です。

図 *5: BGP* バックドア ルートのトポロジ



BGP 4 の設定方法

ベーシック BGP ネットワークの設定は、いくつかの必須作業と多数の任意の作業からなります。BGP ルーティング プロセスと BGP ピアは必ず設定する必要がありますが、このとき、できればアドレス ファミリ コンフィギュレーション モデルを使用してください。BGP ピアが VPN ネットワークの一部である場合、BGP ピアの設定には、IPv4 VRF アドレス ファミリ タスクを使用する必要があります。

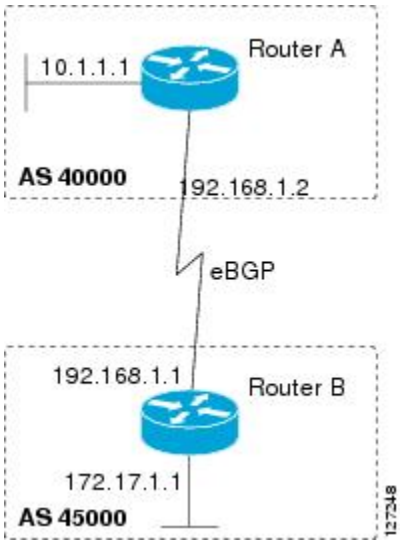
BGP ルーティング プロセスの設定

BGP ルーティング プロセスを設定するには、次の作業を実行します。BGP を有効にするには、必須の手順を少なくとも一度、実行する必要があります。ここで説明する任意の手順を実行すると、BGP ネットワークでその他の機能を設定できます。ネイバー リセットのロギングやリンクが停止したときのピアの即時リセットなど、一部の機能はデフォルトで有効にされていますが、BGP ネットワークの動作方法をよりよく理解できるようにするため、これらの機能についてはここで説明しています。

（注） シスコ ソフトウェアを実行するデバイスは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスおよび自律システムは、同時に使用する複数の BGP アドレス ファミリおよびサブアドレス ファミリ コンフィギュレーションをサポートできます。

下の図では、この作業のコンフィギュレーションはルータ A で行われますが、2 つのデバイスの間で BGP プロセスを完全に実現するには、たとえば、ルータ B で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。ここでは、BGP ルーティング プロセスに対して設定されるアドレス ファミリはないため、IPv4 ユニキャスト アドレス ファミリのルーティング情報はデフォルトでアドバタイズされます。

図 *6 : 2* つの自律システムを持つ *BGP* トポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
5. **bgp router-id** *ip-address*
6. **timers bgp** *keepalive holdtime*
7. **bgp fast-external-fallover**
8. **bgp log-neighbor-changes**
9. **end**
10. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 40000`	BGP ルーティング プロセスを設定し、指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • *autonomous-system-number* 引数を使用して、0 ～ 65534 の範囲の整数を 1 つ指定します。これは、その他の BGP スピーカーへのデバイスを表します。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router)# network 10.1.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 5	**bgp router-id** *ip-address* 例： `Device(config-router)# bgp router-id 10.1.1.99`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル デバイスの ID として設定します。 • *ip-address* 引数を使用して、ネットワーク内で固有のルータ ID を指定します。 （注） **bgp router-id** コマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションがすべてリセットされます。
ステップ 6	**timers bgp** *keepalive holdtime* 例： `Device(config-router)# timers bgp 70 120`	（任意）BGP ネットワーク タイマーを設定します。 • *keepalive* 引数を使用して、頻度を秒単位で指定します。ソフトウェアはこの間隔で、BGP ペアにキープアライブ メッセージを送信します。デフォルトでは、keepalive タイマーは 60 秒に設定されます。 • *holdtime* 引数を使用して、インターバルを秒単位で指定します。この時間を過ぎても、キープアライブ メッセージが届かなかった場合、BGP ピアはデッドであると宣言されます。デフォルトでは、holdtime タイマーは 180 秒に設定されます。

	コマンドまたはアクション	目的
ステップ 7	**bgp fast-external-fallover** 例： `Device(config-router)# bgp fast-external-fallover`	（任意）BGP セッションの自動リセットをイネーブルにします。 • デフォルトでは、直接隣接する外部ピアへのアクセスに使用されるリンクがダウンした場合、このピアの BGP セッションはリセットされます。
ステップ 8	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	（任意）BGP ネイバー ステータスの変更（アップまたはダウン）およびネイバーのリセットのロギングをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を上の図のルータ A で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。この自律システムに対してローカルなネットワーク 10.1.1.0 に対するエントリも表示されています。

```
BGP table version is 12, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性をチェックするには、**ping** コマンドを使用します。

BGP ピアの設定

2 つの IPv4 デバイス（ピア）の間に BGP を設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は上の図のルータ A で行われています。BGP ピアとなりうるネイバー デバイスすべてについて、必ず、この作業を実行してください。

始める前に

この作業を実行する前に、「BGP ルーティング プロセスの設定」の作業を実行します。

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **activate**
7. **end**
8. **show ip bgp** [*network*] [*network-mask*]
9. **show ip bgp neighbors** [*neighbor-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 7	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show ip bgp** [*network*] [*network-mask*] 例：	（任意）BGP ルーティング テーブル内のエントリを表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp`	（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 9	**show ip bgp neighbors** [*neighbor-address*] 例： `Device(config-router-af)# show ip bgp neighbors 192.168.2.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を上の図のルータ A およびルータ B で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。これで、自律システム 45000 でネットワーク 172.17.1.0 のエントリを確認できるようになります。

```
BGP table version is 13, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
*> 172.17.1.0/24    192.168.1.1              0             0 45000 i
```

次に、この作業を上の図のルータ A で設定した後で、ルータ A の BGP ネイバー 192.168.1.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例を示します。

```
BGP neighbor is 192.168.1.1,  remote AS 45000, external link
  BGP version 4, remote router ID 172.17.1.99
  BGP state = Established, up for 00:06:55
  Last read 00:00:15, last write 00:00:15, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            13         13
    Route Refresh:          0          0
    Total:                 15         16
  Default minimum time between advertisement runs is 30 seconds
```

```
 For address family: IPv4 Unicast
  BGP table version 13, neighbor version 13/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              1          1 (Consumes 52 bytes)
    Prefixes Total:                1          1
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          1
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    AS_PATH loop:                      n/a          1
    Bestpath from this peer:             1        n/a
    Total:                               1          1
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.1.2, Local port: 179
Foreign host: 192.168.1.1, Foreign port: 37725
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x12F4F2C):
Timer          Starts    Wakeups            Next
Retrans            14          0             0x0
TimeWait            0          0             0x0
AckHold            13          8             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss:  165379618  snduna:  165379963  sndnxt:  165379963     sndwnd:  16040
irs: 3127821601  rcvnxt: 3127821993  rcvwnd:      15993  delrcvwnd:    391
SRTT: 254 ms, RTTO: 619 ms, RTV: 365 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 20 (out of order: 0), with data: 15, total data bytes: 391
Sent: 22 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 04
```

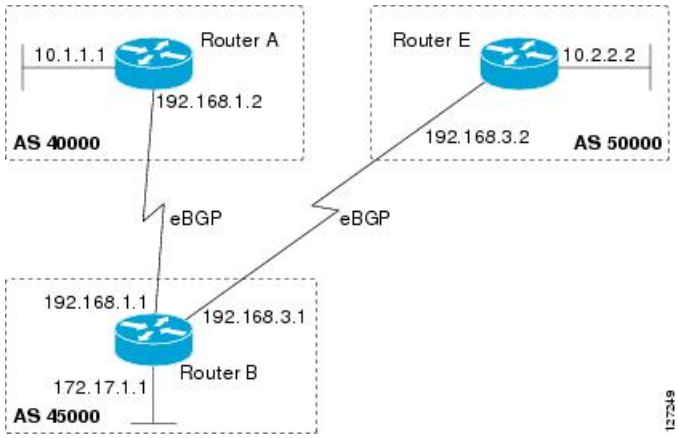
トラブルシューティングのヒント

BGPデバイス間の基本的なネットワーク接続性を確認するには、**ping**コマンドを使用します。

IPv4 VRF アドレス ファミリ用に BGP ピアを設定

VPN 内に存在するため IPv4 VRF 情報を交換しなければならない 2 つの IPv4 デバイス（ピア）の間に BGP を設定するには、次の作業を任意で実行します。ここで設定するアドレス ファミリは IPv4 VRF アドレス ファミリで、設定は下の図のルータ B で自律システム 50000 のルータ E にあるネイバー 192.168.3.2 を使って行われています。BGP IPv4 VRF アドレス ファミリ ピアとなりうるネイバー デバイスすべてについて、必ず、この作業を実行してください。

図 *7 : IPv4 VRF* アドレス ファミリ用 *BGP* トポロジ



始める前に

この作業を実行する前に、「BGP ルーティング プロセスの設定」の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
6. **exit**
7. **ip vrf** *vrf-name*
8. **rd** *route-distinguisher*
9. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
10. **exit**
11. **router bgp** *autonomous-system-number*
12. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
15. **neighbor** *ip-address* **activate**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	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：	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	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding vpn1`	VPN VRF インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 5	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.3.1 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • VRF に割り当てる名前を指定するには、*vrf-name* 引数を使用します。
ステップ 8	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 45000:5`	ルーティング テーブル、およびフォワーディング テーブルを作成し、VPN 用のデフォルト ルート識別子を指定します。 • 一意の VPN IPv4 プレフィックスを作成するために、IPv4 プレフィックスに 8 バイト値を追加するには、*route-distinguisher* 引数を使用します。
ステップ 9	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target both 45000:100`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。

	コマンドまたはアクション	目的
		• ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • インポートおよびエクスポート ルーティング情報の両方をターゲット VPN 拡張コミュニティにインポートするには、**both** キーワードを使用します。 • ルート ターゲット拡張コミュニティ属性を VRF のインポート、エクスポート、または両方（インポートとエクスポート）のルート ターゲット拡張コミュニティ リストに追加するには、*route-target-ext-community* 引数を使用します。
ステップ 10	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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 11	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 12	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**] 例： `Device(config-router-af)# neighbor 192.168.3.2 maximum-prefix 10000 warning-only`	ネイバーから受信できるプレフィックスの数を制御します。 • 特定のネイバーから受信できるプレフィックス数の最大値を指定するには、*maximum* 引数を使用します。設定可能なプレフィックス数は、デバイス上の使用可能なシステム リソースのみによって制限されます。 • プレフィックスの上限をパーセント単位で表した整数を指定するには、*threshold* 引数を使用します。この上限に達すると、デバイスは警告メッセージの生成を開始します。 • プレフィックスの上限を超えた場合に、ピアリングセッションを終了する代わりに、ログメッセージを生成するようにデバイスを設定するには、**warning-only** キーワードを使用します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.3.2 activate`	ネイバーが IPv4 VRF アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 16	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

トラブルシューティングのヒント

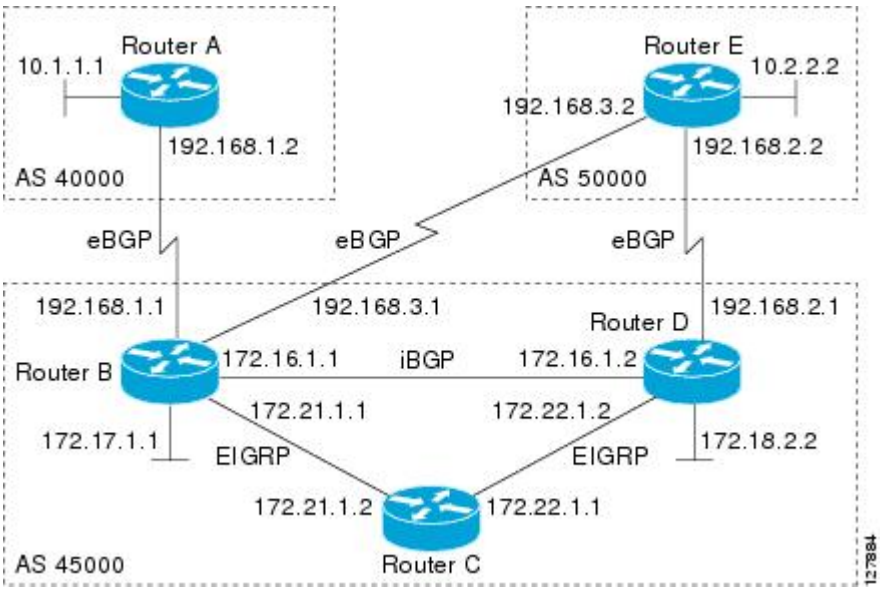
BGPデバイス間の基本的なネットワーク接続を検証するには**ping vrf**コマンドを使用します。また、VRFインスタンスが作成されたことを確認するには**show ip vrf**コマンドを使用します。

BGP ピアのカスタマイズ

BGP ピアをカスタマイズするには、次の作業を実行します。この作業の手順の多くは任意ですが、ネイバーとアドレス ファミリ コンフィギュレーション コマンドの関係がどのように機能しているかを示しています。IPv4 マルチキャスト アドレス ファミリの例を使用すると、IPv4 マルチキャスト アドレス ファミリを設定する前に、ネイバー アドレス ファミリに依存しないコマンドが設定されます。その後、アドレス ファミリに依存するコマンドが設定され、**exit address-family** コマンドが表示されます。任意の手順は、ネイバーを無効にする方法を示しています。

下の図では、この作業のコンフィギュレーションがルータ B で行われます。2 つのデバイスの間で BGP プロセスを完全に実現するには、たとえば、ルータ E で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。

図 *8 : BGP* ピア トポロジ



（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**

5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*
11. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]
12. **exit-address-family**
13. **neighbor** {*ip-address* | *peer-group-name*} **shutdown**
14. **end**
15. **show ip bgp ipv4 multicast** [*command*]
16. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received prefix-filter**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text* 例： `Device(config-router)# neighbor 192.168.3.2 description finance`	（任意）テキストによる説明を指定されたネイバーと関連付けます。
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 multicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャストアドレスファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 8	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.3.2 activate`	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds* 例： `Device(config-router-af)# neighbor 192.168.3.2 advertisement-interval 25`	（任意）BGP ルーティング アップデートの最小送信間隔を設定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] 例： `Device(config-router-af)# neighbor 192.168.3.2 default-originate`	（任意）デフォルトルートとして使用するために、BGP スピーカー（ローカル デバイス）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。
ステップ 12	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **shutdown** 例： `Device(config-router)# neighbor 192.168.3.2 shutdown`	（任意）BGP ピア、またはピア グループを無効にします。 （注） この手順を実行すると、ネイバーが無効化されるため、この後の **show** コマンドを使った手順をいずれも実行できなくなります。
ステップ 14	**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。
ステップ 15	**show ip bgp ipv4 multicast** [*command*] 例： `Device# show ip bgp ipv4 multicast`	（任意）IPv4 マルチキャスト データベース関連情報を表示します。 • サポートされているマルチプロトコル BGP コマンドがあれば、*command* 引数を使用して指定します。サポートされているコマンドを表示するには、CLI で ? プロンプトを使用します。
ステップ 16	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received prefix-filter**] 例： `Device# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。

例

次に、この作業を上の図のルータ B およびルータ E で設定した後で、ルータ B の BGP IPv4 マルチキャスト情報を表示する **show ip bgp ipv4 multicast** コマンドの出力例を示します。IPv4 マルチキャストアドレスファミリで設定された各デバイスに対してローカルなネットワークは、出力テーブルに表示されます。

```
BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

次は、ネイバー 192.168.3.2 に対する **show ip bgp neighbors** コマンドからの出力例の一部分ですが、これにはこのネイバーに関する一般的な BGP 情報と、具体的な BGP IPv4 マルチキャスト アドレス ファミリ情報が表示されます。このコマンドは、上の図のルータ B とルータ E でこの作業を設定した後、ルータ B で入力されたものです。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Description: finance
  BGP version 4, remote router ID 10.2.2.99
  BGP state = Established, up for 01:48:27
  Last read 00:00:26, last write 00:00:26, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised
    Address family IPv4 Multicast: advertised and received
!
 For address family: IPv4 Multicast
  BGP table version 3, neighbor version 3/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
    Uses NEXT_HOP attribute for MBGP NLRIs
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              1          1 (Consumes 48 bytes)
    Prefixes Total:                1          1
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          1
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from this peer:              1        n/a
    Total:                                1          0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 25 seconds
  Connections established 8; dropped 7
  Last reset 01:48:54, due to User reset
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.3.1, Local port: 13172
Foreign host: 192.168.3.2, Foreign port: 179
!
```

再配布を使用した BGP コンフィギュレーション コマンドの削除

小規模な BGP ネットワークであっても、BGP CLI コンフィギュレーションは非常に複雑になることがあります。すべての CLI コンフィギュレーションを削除する必要がある場合は、CLI を削除することで生じるあらゆる影響を考慮する必要があります。現在の実行コンフィギュレーションを分析し、現在の BGP ネイバー関係、アドレス ファミリの考慮事項、その他の設定済みルーティング プロトコルを判断します。BGP CLI コマンドの多くは、CLI コンフィギュレーションのその他の部分に影響を与えています。

EIGRP への BGP ルートの再配布で使用されている BGP コンフィギュレーション コマンドをすべて削除するには、この作業を実行します。ルート マップをパラメータのマッチングや設定、再配布ルートのフィルタに使用して、これらのルートが EIGRP によりアドバタイズされるときに、ルーティング ループが発生しないようにすることができます。BGP コンフィギュレーション コマンドを削除する場合は、必ず、関連するコマンドをすべて削除、または無効にしてください。この例では、**route-map** コマンドを省略しても、再配布は行われ、ルート マップのフィルタリングが取り除かれているために、予期しない結果となる可能性があります。**redistribute** コマンドだけを省略すると、ルート マップは適用されませんが、実行コンフィギュレーションに未使用コマンドが残ります。

BGP CLI の削除の詳細については、「Cisco BGP 概要」モジュールの「BGP CLI 削除の考慮事項」の概念を参照してください。

CLI を削除する前と後の再配布コンフィギュレーションの表示については、「例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no route-map** *map-name*
4. **router eigrp** *autonomous-system-number*
5. **no redistribute** *protocol* [*as-number*]
6. **end**
7. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**no route-map** *map-name* 例： `Device(config)# no route-map bgp-to-eigrp`	実行コンフィギュレーションからルートマップを削除します。 • この例では、bgp-to-eigrp というルート マップがコンフィギュレーションから削除されています。
ステップ 4	**router eigrp** *autonomous-system-number* 例： `Device(config)# router eigrp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 5	**no redistribute** *protocol* [*as-number*] 例： `Device(config-router)# no redistribute bgp 45000`	あるルーティング ドメインから別のルーティング ドメインへのルートの再配布をディセーブルにします。 • この例では、EIGRP ルーティング プロセスへの BGP ルートの再配布のコンフィギュレーションが、実行コンフィギュレーションから削除されています。 （注） オリジナルの **redistribute** コマンド コンフィギュレーションにルート マップが含まれていた場合は、この作業例の手順 3 にあるとおり、**route-map** コマンド コンフィギュレーションを必ず削除してください。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
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 モードを開始します。
ステップ 7	**show running-config** 例： `Device# show running-config`	（任意）ルータの現在の実行コンフィギュレーションを表示します。 • このコマンドは、ルータ コンフィギュレーションから、**redistribute** および **route-map** コマンドが削除されたことを確認するために使用します。

基本的な BGP のモニタリングとメンテナンス

ここでは、基本的な BGP プロセスとピア関係についての情報のリセットおよび表示に関する作業を説明します。BGP ネイバーになるように定義された 2 つのデバイスは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィギュレーションの変更を有効にするために、BGP 接続のリセットが必要になることがあります。

ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定

ルート リフレッシュ機能をサポートしていない BGP ピアに対して、**bgp soft-reconfig-backup** コマンドを使用してインバウンド ソフト再構成を設定するには、この作業を実行します。このコマンドを設定しても、ルート リフレッシュ機能をサポートしている BGP ピアは影響されません。インバウンド更新情報を格納するためのメモリ要件は非常に大きくなる可能性があることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **bgp soft-reconfig-backup**
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 を繰り返します。
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **set ip next-hop** *ip-address*
13. **end**
14. **show ip bgp neighbors** [*neighbor-address*]
15. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングを有効にします。
ステップ 5	**bgp soft-reconfig-backup** 例： `Device(config-router)# bgp soft-reconfig-backup`	ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定します。 • このコマンドは、ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定するために使用します。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**] 例： `Device(config-router)# neighbor 192.168.1.2 soft-reconfiguration inbound`	アップデートの格納を開始するように、シスコ ソフトウェアを設定します。 • このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。着信ソフト再設定が後で行われるときは、格納されている情報を使用して新しい着信アップデートのセットが生成されます。

	コマンドまたはアクション	目的
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router)# neighbor 192.168.1.2 route-map LOCAL in`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、LOCAL という名前のルート マップが着信ルートに適用されます。
ステップ 9	インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 を繰り返します。	-
ステップ 10	**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 11	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map LOCAL permit 10`	ルート マップを設定し、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。 • この例では、LOCAL という名前のルート マップが作成されます。
ステップ 12	**set ip next-hop** *ip-address* 例： `Device(config-route-map)# set ip next-hop 192.168.1.144`	ポリシー ルーティング用のルート マップの match 句を満たしたパケットの送出先を指定します。 • この例では、IP アドレスは 192.168.1.144 に設定されています。
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show ip bgp neighbors** [*neighbor-address*] 例： `Device# show ip bgp neighbors 192.168.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 15	**show ip bgp** [*network*] [*network-mask*] 例：	（任意）BGP ルーティング テーブル内のエントリを表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp`	（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、BGP ネイバー 192.168.2.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされています。

```
BGP neighbor is 192.168.1.2,  remote AS 40000, external link
 Neighbor capabilities:
   Route refresh: advertised and received(new)
```

次に、BGP ネイバー 192.168.3.2 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされておらず、インバウンドポリシーアップデートを更新する方法が他にはないため、BGP ピア 192.168.3.2 の soft-reconfig inbound パスが保存されます。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Neighbor capabilities:
   Route refresh: advertised
```

次の **show ip bgp** コマンドの出力例には、ネットワーク 172.17.1.0 のエントリがあります。BGP ピアは両方とも 172.17.1.0/24 をアドバタイズしていますが、192.168.3.2 については、received-only パスだけが格納されます。

```
BGP routing table entry for 172.17.1.0/24, version 11
Paths: (3 available, best #3, table Default-IP-Routing-Table, RIB-failure(4))
Flag: 0x820
 Advertised to update-groups:
    1
 50000
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external
 50000, (received-only)
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 100, valid, external
 40000
   192.168.1.2 from 192.168.1.2 (172.16.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external, best
```

基本 BGP 情報のリセットと表示

基本 BGP プロセスとピア関係に関する情報をリセットおよび表示するには、この作業を実行します。

手順の概要

1. **enable**
2. **clear ip bgp** {***** | *autonomous-system-number* | *neighbor-address*} [**soft** [**in** | **out**]]
3. **show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]
4. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]
5. **show ip bgp paths**
6. **show ip bgp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip bgp** {*****	*autonomous-system-number*	*neighbor-address*} [**soft** [**in**	**out**]] 例： `Device# clear ip bgp *`	BGP ネイバーセッションをクリアし、リセットします。 • この例では、BGP ネイバーセッションはすべてクリアされ、リセットされます。
ステップ 3	**show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name*	**route-map** *route-map-name*] [**shorter prefixes** *mask-length*] 例： `Device# show ip bgp 10.1.1.0 255.255.255.0`	BGP ルーティング テーブル内のすべてのエントリを表示します。 • この例では、10.1.1.0 ネットワークの BGP ルーティング テーブル情報が表示されます。
ステップ 4	**show ip bgp neighbors** [*neighbor-address*] [**received-routes**	**routes**	**advertised-routes**	**paths** *regexp*	**dampened-routes**	**received** *prefix-filter*] 例： `Device# show ip bgp neighbors 192.168.3.2 advertised-routes`	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。 • この例では、デバイスから他のデバイスの BGP ネイバー 192.168.3.2 にアドバタイズされたルートが表示されます。
ステップ 5	**show ip bgp paths** 例： `Device# show ip bgp paths`	データベース内のすべての BGP パスに関する情報を表示します。
ステップ 6	**show ip bgp summary** 例：	すべての BGP 接続のステータスに関する情報を表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp summary`	

BGP を使用したルート プレフィックスの集約

BGP ピアは、ローカル ネットワークに関する情報を交換しますが、このために、BGP ルーティング テーブルはすぐに巨大になります。CIDR は、ルーティング テーブルのサイズを最小限に抑えるため、集約ルート（スーパーネット）の作成を可能にします。BGP ルーティング テーブルが小さければ小さいほど、ネットワークのコンバージェンス時間が短縮され、ネットワークのパフォーマンスが高まります。集約されたルートは、BGP を使用して、設定およびアドバタイズできます。集約の中には、サマリー ルートだけをアドバタイズするものもありますが、別の方法を使ってルートを集約すると、より具体的なルートが転送できるようになります。集約は、BGP ルーティング テーブルに存在するルートだけに適用されます。集約されたルートは、BGP ルーティング テーブルに具体的な集約ルートが少なくともあと 1 つ存在する場合に転送されます。BGP 内でルートを集約するには、次の作業のいずれかを行います。

BGP へのスタティック集約ルートの再配布

スタティック集約ルートを BPG に再配布するには、この作業を使用します。スタティック集約ルートは設定後、BGP ルーティング テーブルに再配布されます。スタティック ルートは、インターフェイス ヌル 0 をポイントするように設定する必要があります。また、プレフィックスは、既知の BGP ルートのスーパーセットでなければなりません。BGP パケットを受信したデバイスは、より具体的な BGP ルートを使用します。BGP ルーティング テーブルにルートがない場合、パケットはヌル 0 に転送され、廃棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
4. **router bgp** *autonomous-system-number*
5. **redistribute static**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	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 route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*] 例： `Device(config)# ip route 172.0.0.0 255.0.0.0 null 0`	スタティック ルートを作成します。
ステップ 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute static** 例： `Device(config-router)# redistribute static`	BGP ルーティング テーブルにルートを再配布します。
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。

BGP を使用した条件付き集約ルートの設定

少なくとも 1 つのルートが指定された範囲に含まれる場合、この作業を使用して、BGP ルーティング テーブルに集約ルート エントリを作成します。集約ルートは、このユーザの自律システムから始まるものとしてアドバタイズされます。詳細については、「BGP ルート集約の AS_SET 情報生成」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **aggregate-address** *address mask* [**as-set**]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**aggregate-address** *address mask* [**as-set**] 例： `Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 as-set`	BGP ルーティング テーブルに集約エントリを作成します。 • 指定されたルートは、BGP テーブル内に存在する必要があります。 • 指定された範囲に含まれる、より詳しい BGP ルートがある場合は、キーワードを指定せずに **aggregate-address** コマンドを使用して、集約エントリを作成します。 • このルートについてアドバタイズされるパスが AS_SET であることを指定するには、**as-set** キーワードを使用します。このルートは、集約されたルートの到達可能性情報が変更されるたびに取り消され、アップデートされるため、多数のパスを集約するときには、**as-set** キーワードは使用しないでください。 （注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 5	**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。

BGP を使用した集約ルートのアドバタイズメントの抑制および抑制解除

集約ルートを作成し、BGP を使用してルートのアドバタイズメントを抑制して、その後、ルートのアドバタイズの抑制を解除するには、この作業を使用します。抑制されているルートはいかなるネイバーにもアドバタイズされませんが、特定のネイバーに対してすでに抑制されているルートの抑制を解除することはできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. 次のいずれかを実行します。
   - **aggregate-address** *address mask* [**summary-only**]
   - **aggregate-address** *address mask* [**suppress-map** *map-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカルデバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	次のいずれかを実行します。	集約ルートを作成します。

	コマンドまたはアクション	目的

	• **aggregate-address** *address mask* [**summary-only**]
	• **aggregate-address** *address mask* [**suppress-map** *map-name*]
	例：
	`Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 summary-only`
	例：
	`Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1`
		• 集約ルート（たとえば、10.*.*.*）を作成し、すべてのネイバーに対するより具体的なルートのアドバタイズメントを抑制するには、オプションの **summary-only** キーワードを使用します。
		• 集約ルートを作成するが、指定されたルートのアドバタイズメントを抑制するには、オプションの **suppress-map** キーワードを使用します。抑制されたルートは、いかなるネイバーにもアドバタイズされません。ルートマップの **match** 句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートを抑制しないでおくことができます。IP アクセス リストと自律システム パス アクセス リストの **match** 句がサポートされています。
		（注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name* 例： `Device(config-router)# neighbor 192.168.1.2 unsuppress map1`	（任意）**aggregate-address** コマンドにより、すでに抑制されているルートを選択的にアドバタイズします。 • この例では、ステップ 5 ですでに抑制されているルートが、ネイバー 192.168.1.2 にアドバタイズされます。
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 モードを開始します。

BGP ルートの条件付きアドバタイズ

選択した BGP ルートを条件付きでアドバタイズするには、この作業を実行します。条件付きでアドバタイズされるルートまたはプレフィックスは、アドバタイズマップと存在マップまたは非存在マップの 2 つのルートマップで定義されます。存在マップまたは不在マップと関連付けられているルート マップは、BGP スピーカーが追跡するプレフィックスを指定します。アドバタイズ マップと関連付けられているルート マップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィックスを指定します。

- プレフィックスが存在マップにあることが BGP スピーカーにより判明した場合、アドバタイズ マップで指定されたプレフィックスがアドバタイズされます。

- プレフィックスが非存在マップにないことが BGP スピーカーにより判明した場合、アドバタイズ マップで指定されたプレフィックスがアドバタイズされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティング テーブルに存在する必要があります。これらのルートは、アクセス リストから、または IP プレフィックス リストから参照されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
8. **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...*]}
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
11. **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...*]}
12. **exit**
13. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
14. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
15. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 45000`	
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} 例： `Device(config-router)# neighbor 192.168.1.2 advertise-map map1 exist-map map2`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、存在マップ（map2 という名前付きルート マップ）の ACL と一致するプレフィックス（192.168.50.0）がローカル BGP テーブルにある場合に限り、アドバタイズマップ（map1 という名前付きルート マップ）の ACL と一致するプレフィックス（172.17.0.0）がネイバーにアドバタイズされます。
ステップ 6	**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 7	**route-map** *map-tag* [**permit** | **deny**] [**sequence-number**] 例： `Device(config)# route-map map1 permit 10`	ルート マップを設定し、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。 • この例では、map1 という名前のルート マップが作成されます。
ステップ 8	**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...*]} 例： `Device(config-route-map)# match ip address 1`	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 リストにより許可されているプレフィックスと一致するルート マップを作成します。 • この例では、ルート マップは、アクセス リスト 1 で許可されているプレフィックスとマッチングされます。
ステップ 9	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map map2 permit 10`	ルート マップを設定し、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。 • この例では、map2 という名前のルート マップが作成されます。
ステップ 11	**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...*]} 例： `Device(config-route-map)# match ip address 2`	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 リストにより許可されているプレフィックスと一致するルート マップを作成します。 • この例では、ルート マップは、アクセス リスト 2 で許可されているプレフィックスとマッチングされます。
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 モードを終了して、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 13	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 1 permit 172.17.0.0`	標準アクセス リストを設定します。 • この例では、アクセス リスト 1 で、**neighbor advertise-map** コマンドによって設定された他の条件に応じて、172.17.0.0 プレフィックスのアドバタイズが許可されます。
ステップ 14	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 2 permit 192.168.50.0`	標準アクセス リストを設定します。 • この例では、192.168.50.0 が exist-map のプレフィックスになるように、アクセス リスト 2 が認可を与えます。
ステップ 15	**exit** 例： `Device(config)# exit`	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。

BGP ルートの開始

ルート集約は BGP テーブルのサイズを最小化するには便利ですが、BGP テーブルに特定のプレフィックスを追加する必要が生じることがあります。ルート集約では、特定のプレフィックスをさらに非表示にすることができます。「BGP ルーティング プロセスの設定」の項で示さ

れている **network** コマンドを使用して、ルートを開始し、次のオプション作業によってさまざまな状況に対応した BGP テーブルへの BGP ルートを開始します。

BGP を使用したデフォルト ルートのアドバタイジング

BGP ピアへのデフォルト ルートをアドバタイズするには、次の作業を実行します。デフォルト ルートはローカルに開始されます。デフォルト ルートは、コンフィギュレーションを簡素化する場合やデバイスでシステム リソースが過剰に使用されないようにする場合に便利です。デバイスがインターネット サービス プロバイダー（ISP）のピアである場合、ISP は完全なルーティング テーブルを持っているため、ISP ネットワークへのデフォルト ルートを設定しておくと、ローカル デバイスのリソースが節約されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length* | **permit** *network / length*} [**ge** *ge-value*] [**le** *le-value*]
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **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...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*	**permit** *network / length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list DEFAULT permit 10.1.1.0/24`	IP プレフィックス リストを設定します。 • この例では、プレフィックス リスト DEFAULT は、**match ip address** コマンドによって設定されたマッチングに応じて、10.1.1.0/24 プレフィックスのアドバタイズを許可します。

	コマンドまたはアクション	目的
ステップ 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map ROUTE`	ルートマップを設定し、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。 • この例では、ROUTE という名前のルート マップが作成されます。
ステップ 5	**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...*]} 例： `Device(config-route-map)# match ip address prefix-list DEFAULT`	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により許可されているプレフィックスと一致するルートマップを作成します。 • この例では、ルートマップは、プレフィックス リスト DEFAULT で許可されているプレフィックスとマッチングされます。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 7	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] 例： `Device(config-router)# neighbor 192.168.3.2 default-originate`	（任意）デフォルト ルートとして使用するために、BGP スピーカー（ローカルデバイス）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードを開始します。

バックドア ルートを使用した BGP ルートの開始

バックドア ルートを使用して到達可能なネットワークを示すには、この作業を実行します。バックドア ネットワークはローカル ネットワークと同様に扱われますが、アドバタイズされません。詳細については、「BGP バックドア ルート」の項を参照してください。

始める前に

この作業は、BGP ピアに対して、IGP（この例ではEIGRP）がすでに設定されていることを前提にしています。この設定は「BGPバックドア ルート」の項にあるのルータ B で行われます。また、BGP ピアはルータ D です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **network** *ip-address* **backdoor**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 172.22.1.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスのマルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ピアに指定されている自律システム番号はステップ 3 で指定された番号と同じであるため、このピアは内部ピアです。
ステップ 5	**network** *ip-address* **backdoor** 例： `Device(config-router)# network 172.21.1.0 backdoor`	バックドア ルートを通じて到達可能なネットワークを示します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-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。

BGP ピア グループの設定

この作業では、BGP ピア グループの設定方法を説明します。BGP スピーカーでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります。同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、アップデートをより効率化するために、ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

次の作業で説明されている、BGP ピア グループを設定するための 3 つの手順は次のとおりです。

- ピア グループを作成する
- ピア グループへオプションに割り当てる
- ピア グループのメンバをネイバーにする

neighbor shutdown ルータ コンフィギュレーション コマンドを使用して、コンフィギュレーション情報を削除せずに、BGP ピア、またはピア グループを削除することができます。

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **peer-group** *peer-group-name*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **neighbor** *peer-group-name* **activate**
9. **neighbor** *ip-address* **peer-group** *peer-group-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router)# neighbor fingroup peer-group`	BGP ピア グループを作成します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスのマルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 multicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。これがデフォルトです。 • キーワード **multicast** は、IPv4 マルチキャスト アドレス プレフィックスが交換されることを表します。

	コマンドまたはアクション	目的
		• **vrf** キーワードおよび *vrf-name* 引数は、IPv4 VRF インスタンス情報が交換されることを示します。
ステップ 8	**neighbor** *peer-group-name* **activate** 例： `Device(config-router-af)# neighbor fingroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。 （注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、ユニキャストアドレスプレフィックスだけを交換します。この例で設定しているマルチキャストなど、その他のアドレスプレフィックス タイプを BGP が交換できるようにするには、**neighbor activate** コマンドを使用してネイバーをアクティブ化することも必要です。
ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP 4 の設定例

例：BGP プロセスの設定とピアのカスタマイズ

次の例は、上の（「BGP ピアのカスタマイズ」の項）に示されている異なる自律システムにある 2 つのネイバー ピア（ルータ A のピアとルータ E のピア）を使って BGP プロセスが設定されているルータ B のコンフィギュレーションを示しています。IPv4 ユニキャスト ルートは両方のピアと交換され、IPv4 マルチキャスト ルートはルータ E の BGP ピアと交換されます。

ルータ B

```
router bgp 45000
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
```

```
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 !
 address-family ipv4 multicast
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 advertisement-interval 25
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除

次の例は、ルート マップを使用して EIGRP への BGP ルートの再配布を有効にする CLI コンフィギュレーションと、再配布とルート マップを削除する CLI コンフィギュレーションを示しています。BGP コンフィギュレーション コマンドの中には、他の CLI コマンドに影響を与えるものもありますが、この例は、あるコマンドの削除が他のコマンドにどのような影響を与えるかを示しています。

1つ目のコンフィギュレーション例では、ルートマップは、自律システム番号をマッチングおよび設定するように設定されています。3つの異なる自律システムにあるBGPネイバーが設定およびアクティブ化されます。EIGRP ルーティング プロセスが開始され、ルート マップを使用して、EIGRP への BGP ルートの再配布が設定されます。

EIGRP への BGP ルート再配布を有効にする CLI

```
route-map bgp-to-eigrp permit 10
 match tag 50000
 set tag 65000
 exit
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4
  neighbor 172.16.1.2 remote-as 45000
  neighbor 172.21.1.2 remote-as 45000
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.3.2 remote-as 50000
  neighbor 172.16.1.2 activate
  neighbor 172.21.1.2 activate
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 exit
```

```
router eigrp 100
 redistribute bgp 45000 metric 10000 100 255 1 1500 route-map bgp-to-eigrp
 no auto-summary
 exit
```

2 つ目のコンフィギュレーション例では、**route-map** コマンドと **redistribute** コマンドの両方が無効になっています。route-map コマンドだけを削除した場合、再配布が自動的に無効になることはありません。再配布は行われますが、マッチングやフィルタリングは行われません。再配布コンフィギュレーションを削除するには、**redistribute** コマンドも無効にする必要があります。

EIGRP への BGP ルート再配布を削除する CLI

```
configure terminal
 no route-map bgp-to-eigrp
 router eigrp 100
  no redistribute bgp 45000
  end
```

例：BGP ソフト リセット

次の例は、BGP ピア 192.168.1.1 の接続をリセットする 2 通りの方法を示しています。

例：ダイナミック インバウンド ソフト リセット

次に、BGP ピア 192.168.1.1 でダイナミック ソフト再構成を開始するコマンドの例を示します。このコマンドを使用するには、ピアでルート リフレッシュ機能がサポートされている必要があります。

```
clear ip bgp 192.168.1.1 soft in
```

例：格納された情報を使用したインバウンド ソフト リセット

次の例では、ネイバー 192.168.1.1 に対してインバウンド ソフト再構成を有効にする方法を示しています。このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。インバウンド ソフトウェア再構成を後で行う場合、格納された情報を使用して、新たに一連のインバウンド アップデートが生成されます。

```
router bgp 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 soft-reconfiguration inbound
```

次の例では、ネイバー 192.168.1.1 のセッションがクリアされます。

```
clear ip bgp 192.168.1.1 soft in
```

例：基本 BGP 情報のリセットおよび表示

次に、基本 BGP 情報をリセットおよび表示する例を示します。

clear ip bgp * コマンドは BGP ネイバー セッションをすべてクリアし、リセットします。特定のネイバーをクリアするには *neighbor-address* 引数、自律システムにあるすべてのピアをクリアするには *autonomous-system-number* 引数を使用します。引数が指定されていない場合、このコマンドは BGP ネイバー セッションをすべてクリアし、リセットします。

（注） また、**clear ip bgp *** コマンドは内部 BGP 構造をすべてクリアするため、トラブルシューティング ツールとして便利です。

```
Device# clear ip bgp *
```

show ip bgp コマンドは、BGP ルーティング テーブルのすべてのエントリを表示するために使用します。次に、10.1.1.0 ネットワークの BGP ルーティング テーブル情報を表示する例を示します。

```
Device# show ip bgp 10.1.1.0 255.255.255.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1
  40000
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

show ip bgp neighbors コマンドは、TCP および BGP 接続に関する情報をネイバーに表示するために使用します。次の例は、上の図（「IPv4 VRF アドレス ファミリ用に BGP ピアを設定」の項）のルータ B から、ルータ E にある BGP ネイバー 192.168.3.2 にアドバタイズされるルートを示しています。

```
Device# show ip bgp neighbors 192.168.3.2 advertised-routes

BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
Total number of prefixes 2
```

show ip bgp paths コマンドは、データベース内のすべての BGP パスを表示するために使用します。次に、上の図（「BGP ピアのカスタマイズ」の項）のルータ B に対する BGP パス情報を表示する例を示します。

```
Device# show ip bgp paths

Address    Hash Refcount Metric Path
0x2FB5DB0     0        5      0 i
0x2FB5C90     1        4      0 i
0x2FB5C00  1361        2      0 50000 i
0x2FB5D20  2625        2      0 40000 i
```

show ip bgp summary コマンドは、すべての BGP 接続のステータスを表示するために使用します。次に、上の図（「BGP ピアのカスタマイズ」の項）のルータ B に対する BGP ルーティング テーブル情報を表示する例を示します。

```
Device# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 45000
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 882 total bytes of memory
BGP activity 14/10 prefixes, 16/12 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.2     4 40000     667     672        3    0    0 00:03:49        1
192.168.3.2     4 50000     468     467        0    0    0 00:03:49 (NoNeg)
```

例：BGP を使用したプレフィックスの集約

次の例は、集約ルートを BGP に再配布するか、または BGP 条件付き集約ルーティング機能を使用することにより、BGP で集約ルートを使用する方法を示します。

次の例では、**redistribute static** ルータ コンフィギュレーション コマンドを使用して、集約ルート 10.0.0.0 が再配布されます。

```
ip route 10.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

次のコンフィギュレーションは、少なくとも 1 つのルートが指定された範囲に含まれる場合に、BGP ルーティング テーブルに集約エントリを作成する方法を示します。自律システムから受け取られるに従って、集約ルートはアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、atomic aggregate 属性が設定されています（デフォルトでは、**aggregate-address** ルータ コンフィギュレーション コマンドで **as-set** キーワードを使用しない限り、atomic aggregate は設定されています）。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0
```

次の例は、直前の例と同じルールを使用して集約エントリを作成する方法を示していますが、このルートでアドバタイズされるパスは、要約されているパスすべてに含まれるすべての要素から構成される AS_SET です。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 as-set
```

次の例は、10.0.0.0 に対する集約ルートを作成しながら、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する方法を示します。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

次の例は、非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# bgp suppress-inactive
Device(config-router-af)# end
```

次の例は、RED という名前の VRF でルートの上限を設定し、RED という名前の VRF 経由で非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Device(config)# ip vrf RED
Device(config-vrf)# rd 50000:10
Device(config-vrf)# maximum routes 1000 10
Device(config-vrf)# exit
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 vrf RED
Device(config-router-af)# bgp suppress-inactive
Device(config-router-af)# end
```

例：BGP ピア グループの設定

次の例は、アドレス ファミリを使用して、ピア グループのすべてのメンバがユニキャストとマルチキャストの両方に対応できるようにピア グループを設定する方法を示しています。

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 unicast
  neighbor mygroup peer-group
  neighbor 192.168.1.2 peer-group mygroup
  neighbor 192.168.3.2 peer-group mygroup
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 multicast
  neighbor mygroup peer-group
  neighbor 192.168.1.2 peer-group mygroup
  neighbor 192.168.3.2 peer-group mygroup
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
```

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration on an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』

MIB

MIB	MIB のリンク
CISCO-BGP4-MIB	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

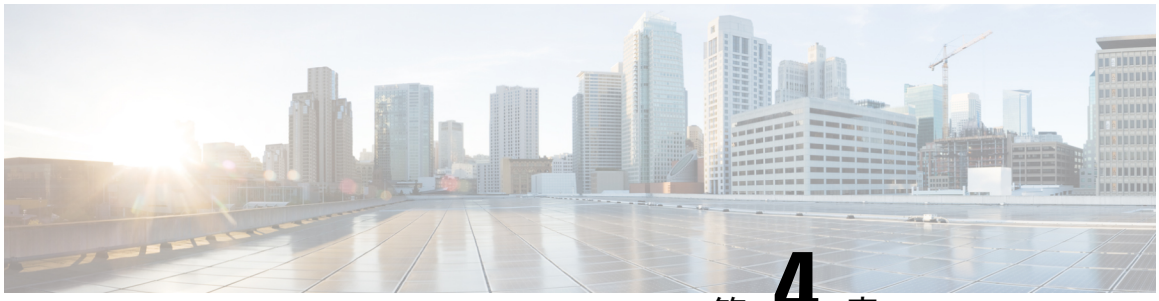
BGP 4 の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *7: BGP 4* の機能情報

機能名	リリース	機能情報
BGP 4		BGP は、独自のルーティング ポリシー（自律システム）を持つ異なるルーティング ドメイン間に、ループのないルーティングを行うように設計されたドメイン間ルーティング プロトコルです。BGP バージョン 4 のシスコ ソフトウェア実装では、マルチプロトコル拡張がサポートされており、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、バーチャル プライベート ネットワーク バージョン 4（VPNv4）、コネクションレス型ネットワーク サービス（CLNS）を含むインターネット プロトコル（IP）マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報が BGP により伝送されるようになっています。



第 4 章

基本 BGP ネットワークの設定

このモジュールでは、基本的なボーダー ゲートウェイ プロトコル（BGP）ネットワークを設定するための基本的な作業について説明します。BGP は、組織間にループのないルーティングを提供するために設計されたドメイン間ルーティング プロトコルです。ここでは、ネイバーおよびアドレス ファミリ コマンドの Cisco IOS 実装について説明します。また、このモジュールには BGP ピアの設定およびカスタマイズ、BGP ルート集約の実装、BGP ルート オリジネーションの設定、および BGP バックドア ルートの定義を行うための作業も含まれます。BGP ピア グループを定義し、ピア セッション テンプレートについて紹介するとともに、グループのアップデートについて説明します。

- 機能情報の確認 （79 ページ）
- 基本 BGP ネットワーク設定の前提条件 （80 ページ）
- 基本 BGP ネットワーク設定の制約事項 （80 ページ）
- 基本 BGP ネットワーク設定の概要 （80 ページ）
- 基本 BGP ネットワークの設定方法 （99 ページ）
- 基本 BGP ネットワークの設定例 （166 ページ）
- 次の作業 （181 ページ）
- その他の参考資料 （182 ページ）
- 基本 BGP ネットワーク設定の機能情報 （184 ページ）

機能情報の確認

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

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

基本 BGP ネットワーク設定の前提条件

基本BGPネットワークを設定する前に、「CiscoBGP概要」モジュールを理解しておく必要があります。

基本 BGP ネットワーク設定の制約事項

シスコ ソフトウェアを実行するデバイスは、1つのBGPルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスと自律システムでは、複数のアドレス ファミリ設定をサポートできます。

基本 BGP ネットワーク設定の概要

BGP バージョン 4

ボーダー ゲートウェイ プロトコル（BGP）は、独立したルーティング ポリシーを持つルーティング ドメイン（自律システム）の間に、ループのないルーティングを提供するように設計されたドメイン間ルーティング プロトコルです。BGP バージョン 4 のシスコ ソフトウェア実装では、マルチプロトコル拡張がサポートされており、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、バーチャル プライベート ネットワーク バージョン 4（VPNv4）を含むインターネット プロトコル（IP）マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報が BGP により伝送されるようになっています。

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。外部組織への接続時に、外部 BGP（eBGP）ピアリング セッションが作成されます。BGP は外部ゲートウェイ プロトコル（EGP）と呼ばれますが、組織における多くのネットワークは非常に複雑になりつつあるため、BGPを組織内で使用されている内部ネットワークを簡素化する際にも使用できます。同じ組織内のBGPピアは、内部BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

（注） BGP は他のルーティング プロトコルよりも多くの設定を必要としますが、ユーザは設定変更の影響をよく理解しておく必要があります。設定が正しくないと、ルーティング ループが発生し、通常のネットワーク操作に悪影響を及ぼす可能性があります。

BGP ルータ ID

BGP では、ルータ ID を使用して、BGP スピーキング ピアを識別します。BGP ルータ ID は 32 ビット値であり、IPv4 アドレスで表すことがよくあります。デフォルトでは、シスコ ソフト

ウェアによって、ルータ ID がルータ上のループバック インターフェイスの IPv4 アドレスに設定されます。デバイス上でループバック インターフェイスが設定されていない場合は、BGP ルータ ID を表すためにデバイスの物理インターフェイスに設定されている最上位の IPv4 アドレスがソフトウェアによって選択されます。BGP ルータ ID は、ネットワーク内の BGP ピアごとに一意である必要があります。

BGP スピーカーとピア関係

BGP 対応デバイスは、別の BGP 対応デバイスを自動的には検出しません。ネットワーク管理者は、通常、BGP 対応デバイス間の関係を手動で設定します。ピア デバイスとは、別の BGP 対応デバイスへのアクティブな TCP 接続を持つ BGP 対応デバイスです。この BGP デバイス間の関係がネイバーと呼ばれることはよくありますが、これは BGP デバイスは直接接続されていて、その間に他のデバイスははさまっていないということを暗示することがあるため、このマニュアルではネイバーという語の使用は極力避けています。BGP スピーカーはローカル デバイスのことで、その他の BGP 対応ネットワーク デバイスはすべてピアです。

ピアとピアの間に TCP 接続が確立されると、最初、個々の BGP ピアはもう 1 つのピアと、そのルート（完成した BGP ルーティング テーブル）をすべて交換します。この交換の後は、ネットワークでトポロジの変更が行われたとき、あるいはルーティング ポリシーが実装または変更されたときに差分更新が送信されるだけです。更新と更新の間の非アクティブ期間には、ピアは「キープアライブ」と呼ばれる特別なメッセージを交換します。

BGP 自律システムは、単一のアドミニストレーション エンティティにより制御されるネットワークです。ピア デバイスは、異なる自律システムに存在する場合は外部ピア、同一の自律システムに存在する場合は内部ピアと呼ばれます。通常、外部ピアは隣接し、サブネットを共有していますが、内部ピアは同じ自律システムのどのような場所にあってもかまいません。

BGP 自律システム番号の形式

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

asdot だけを使用する自律システム番号形式

Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースでは、4 オクテット（4 バイト）の自律システム番号は asdot 表記法だけで入力および表示されます。たとえば、1.10 または 45000.64000 です。4 バイト自律システム番号のマッチングに正規表現を使用する場合、asdot 形式には正規表現で特殊文字となるピリオドが含まれていることに注意します。正規表現でのマッチングに失敗しないよう、（1\.14 のように）ピリオドの前にバックスラッシュを入力する必要があります。次の表は、asdot 形式だけが使用できる Cisco IOS イメージで、2 バイトおよび 4 バイト自律システム番号の設定、正規表現とのマッチング、および **show** コマンド出力での表示に使用される形式をまとめたものです。

表 *8 : asdot* だけを使用する *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

asplain をデフォルトとする自律システム番号形式

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコ実装の 4 バイト自律システム番号で asplain がデフォルトの自律システム番号表示形式として使用されていますが、4 バイト自律システム番号は asplain および asdot 形式のどちらにも設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力を変更して、4 バイトの自律システム番号を asdot 形式で表示する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式が有効にされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。**show** コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト自律システム番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドを有効にした後、**clear ip bgp *** コマンドを入力してすべての BGP セッションに対してハード リセットを開始する必要があります。

（注） 4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

表 *9 : asplain* をデフォルトとする *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295

表 *10 : asdot* を使用する *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

予約済みおよびプライベートの自律システム番号

Cisco IOS Release 12.0(32)S12、12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、12.4(24)T、およびそれ以降のリリースでは、RFC 4893 がシスコの BGP 実装でサポートされています。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。新しい予約済み（プライベート）自律システム番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を自律システム番号として設定できません。

RFC 5398『*Autonomous System (AS) Number Reservation for Documentation Use*』では、文書化を目的として新たに予約された自律システム番号について説明されています。予約済み番号を使用することで、設定例を正確に文書化しつつ、その設定がそのままコピーされた場合でも製品ネットワークに競合が発生することを防止できます。予約済み番号は IANA 自律システム番号レジストリに記載されています。予約済み 2 バイト自律システム番号は 64496 ～ 64511 の連続したブロック、予約済み 4 バイト自律システム番号は 65536 ～ 65551 をその範囲としています。

64512 ～ 65534 を範囲とするプライベートの 2 バイト自律システム番号は依然有効で、65535 は特殊な目的のために予約されています。プライベート自律システム番号は内部ルーティングドメインで使用できますが、インターネットにルーティングされるトラフィックについては変換が必要です。プライベート自律システム番号を外部ネットワークへアドバタイズするように BGP を設定しないでください。Cisco IOS ソフトウェアは、デフォルトではルーティング アップデートからプライベート自律システム番号を削除しません。ISP がプライベート自律システム番号をフィルタリングすることを推奨します。

（注） パブリック ネットワークおよびプライベート ネットワークに対する自律システム番号の割り当ては、IANA が管理しています。予約済み番号の割り当てや自律システム番号の登録申込など、自律システム番号についての情報については、http://www.iana.org/ を参照してください。

シスコが採用している 4 バイト自律システム番号

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、15.1(1)SG、およびそれ以降のリリースでは、シスコが採用している 4 バイト自律システム番号は、AS 番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用しています。ただし、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。

4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドの後に **clear ip bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

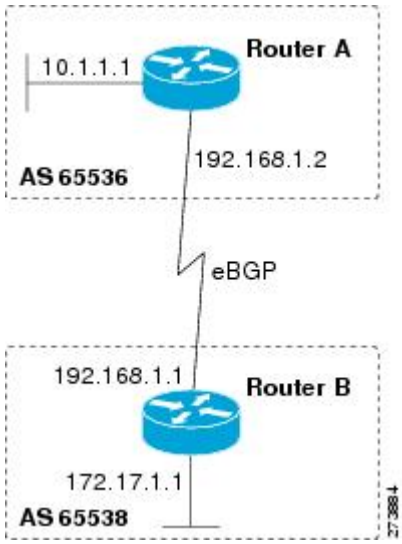
Cisco IOS Release 12.0(32)S12、および 12.4(24)T では、シスコが採用している 4 バイト自律システム番号は、設定形式、正規表現とのマッチング、および出力表示として、asdot（たとえば、1.2）だけを使用しています。asplain はサポートしていません。

4 バイト番号を使用する 2 つの自律システム内の BGP ピアの例については、下の図を参照してください。asdot 表記法を使用して設定された、異なる 4 バイトの自律システムにある 3 つのネイバー ピアの間での設定例については、「例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定」を参照してください。

シスコは、BGP が 2 バイト自律システム番号から 4 バイト自律システム番号へ段階的に移行できるように開発された RFC 4893 もサポートしています。スムーズな移行を確実に行うには、4 バイト自律システム番号を使用して識別される自律システム内の BGP スピーカーをすべて、4 バイト自律システム番号をサポートするようにアップグレードすることを推奨します。

（注） 新しいプライベート自律システム番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を自律システム番号として設定できません。

図 *9 : 4* バイト番号を使用する *2* つの自律システム内の *BGP* ピア



BGP ピア セッションの確立

BGP ルーティング プロセスがピアとピアリング セッションを確立するとき、ステートは次のように変化します。

- Idle：ルーティング プロセスが有効になったとき、またはデバイスがリセットされたときの BGP ルーティング プロセスの初期ステート。このステートでは、デバイスはリモート ピアとのピアリング設定など、開始イベントを待ちます。リモート ピアから TCP 接続要求を受信すると、デバイスはリモート ピアへの TCP 接続を開始する前に、タイマーを待機するための開始イベントを新たに開始します。デバイスがリセットされ、ピアがリセットされると、BGP ルーティング プロセスは Idle ステートに戻ります。
- Connect：ローカル BGP スピーカーとの TCP セッションを確立しようとしていることを BGP ルーティング プロセスが検知します。
- Active：このステートでは、BGP ルーティング プロセスは、ConnectRetry タイマーを使用して、ピア デバイスとの TCP セッションを確立しようとします。BGP ルーティング プロセスが Active ステートの間、開始イベントは無視されます。BGP ルーティング プロセスが再構成された場合、またはエラーが発生した場合、BGP ルーティング プロセスはシステム リソースを解放し、Idle ステートに戻ります。
- OpenSent：TCP 接続が確立され、BGP ルーティング プロセスはリモート ピアに OPEN メッセージを送信し、OpenSent ステートに移行します。このステートでは、BGP ルーティング プロセスはその他の OPEN メッセージを受信できます。接続に失敗した場合、BGP ルーティング プロセスは Active ステートに移行します。
- OpenReceive：BGP ルーティング プロセスはリモート ピアから OPEN メッセージを受信し、リモート ピアからの最初のキープアライブ メッセージを待ちます。キープアライブ メッセージを受信すると、BGP ルーティング プロセスは Established ステートに移行します。通知メッセージを受信した場合は、BGP ルーティング プロセスは Idle ステートに移

行します。ピアリング セッションに影響を与えるエラー、または設定変更が発生した場合、BGP ルーティング プロセスは、有限状態マシン（FSM）エラー コードが入った通知メッセージを送信してから、Idle ステートに移行します。

- Established：リモート ピアから最初のキープアライブが受信されます。これにより、リモート ネイバーとのピアリングが確立され、BGP ルーティング プロセスは、リモート ピアとのアップデート メッセージの交換を開始します。アップデート メッセージ、またはキープアライブ メッセージが受信されると、ホールドタイマーが再起動されます。エラー通知を受信した BGP プロセスは、Idle ステートに移行します。

シスコが採用している BGP グローバル コマンドとアドレス ファミリ コンフィギュレーション コマンド

BGP を設定するためのアドレス ファミリ モデルでは、基本的にアドレス ファミリごとに設定が分割されます。設定の最初に、アドレス ファミリとは関係のない（非依存の）コマンドがすべてグループ化され（最上位レベル）、これに各アドレス ファミリに固有のコマンドで使用される個々のサブモードが続きます（ただし、IPv4 ユニキャストに関係するコマンドは例外で、これらは設定の先頭に入力することができます）。ネットワーク オペレータが BGP を設定した場合の BGP 設定カテゴリのフローは、次の箇条書きの順に表されます。

- グローバル コンフィギュレーション：特定のネイバーではなく、BGP に全般的に適用される設定。**network**、**redistribute**、**bgp bestpath** コマンドなどです。
- アドレス ファミリ依存コンフィギュレーション：個々のネイバーのポリシーなど、特定のアドレス ファミリに適用されるコンフィギュレーション。

BGP グローバルおよび BGP アドレス ファミリ依存設定のカテゴリを下の表に示します。

表 *11 : BGP* コンフィギュレーション カテゴリの関係

BGP コンフィギュレーション カテゴリ	**カテゴリ内のコンフィギュレーション セット**
グローバル アドレス ファミリ非依存	グローバル アドレス ファミリ非依存コンフィギュレーション 1 セット
アドレス ファミリ依存	1 アドレス ファミリにつき、グローバル アドレス ファミリ依存コンフィギュレーション 1 セット

（注） アドレス ファミリ コンフィギュレーションは、それが適用されるアドレス ファミリ サブモードで入力する必要があります。

次の BGP コンフィギュレーション文の例は、グループ分けされたグローバル アドレス ファミリ非依存コマンドと、アドレス ファミリ依存コマンドを示しています。

```
router bgp <AS>
 ! AF independent part
 neighbor <ip-address> <command> ! Session config; AF independent
 address-family ipv4 unicast
  ! AF dependant part
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
 address-family ipv4 multicast
  ! AF dependant part
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
 address-family ipv4 unicast vrf <vrf-name>
  ! VRF specific AS independent commands
  ! VRF specific AS dependant commands
  neighbor <ip-address> <command> ! Session config; AF independent
  neighbor <ip-address> <command> ! Policy config; AF dependant
  exit-address-family
```

次の例は、前の例で、BGP コンフィギュレーション文と一致する、実際の BGP コマンドを示しています。

```
router bgp 45000
 router-id 172.17.1.99
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 unicast
  neighbor 192.168.1.2 activate
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 address-family ipv4 multicast
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 advertisement-interval 25
  network 172.16.1.0 mask 255.255.255.0
  exit-address-family
 address-family ipv4 vrf vpn1
  neighbor 192.168.3.2 activate
  network 172.21.1.0 mask 255.255.255.0
  exit-address-family
```

bgp upgrade-cli コマンドは、BGP ネットワークと既存のコンフィギュレーションのネットワーク層到達可能性情報（NLRI）形式からアドレス ファミリ形式への移行を簡素化します。ネットワーク オペレータは、Address Family Identifier（AFI）形式でコマンドを設定し、この設定を既存の NLRI 形式の設定に保存できます。NLRI 形式の制限のため、BGP ハイブリッド コマンドライン インターフェイス（CLI）は、AFI および NLRI の統合を完全にはサポートしていません。AFI コマンドおよび機能をすべてサポートするためには、**bgp upgrade-cli** コマンドを使用して、既存の NLRI コンフィギュレーションをアップグレードすることを推奨します。NLRI 形式からアドレス ファミリ形式への BGP コンフィギュレーションの移行例については、このモジュールの「例：NLRI から AFI へのコンフィギュレーション」の項を参照してください。

BGP セッションのリセット

設定変更のためにルーティング ポリシーに変更が生じた場合は、必ず **clear ip bgp** コマンドを使用して、BGP ピアリング セッションをリセットする必要があります。シスコ ソフトウェア

は、BGP ピアリング セッションのリセットとして、次の 3 つのメカニズムをサポートしています。

- ハード リセット：ハード リセットは、TCP 接続を含む指定されたピアリング セッションを終了し、指定されたピアから到着したルートを削除します。
- ソフト リセット：ソフト リセットは、保存されたプレフィックス情報を使用し、既存のピアリング セッションを廃棄せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しいBGPポリシーを適用することができます。ソフト再構成は、インバウンドセッション、またはアウトバウンド セッションに対して設定できます。
- ダイナミック インバウンド ソフト リセット：これは RFC 2918 に定義されているルート リフレッシュ機能で、サポートしているピアへのルート リフレッシュ要求を交換することにより、ローカル デバイスがインバウンド ルーティング テーブルを動的にリセットできるようにするものです。ルート リフレッシュ機能は、中断を伴わないポリシー変更についてはアップデート情報をローカルに保存しません。その代わり、サポートしているピアとの動的な交換に依存します。ルート リフレッシュは、最初にピア間のBGP機能ネゴシエーションを通じてアドバタイズされる必要があります。すべての BGP デバイスが、ルート リフレッシュ機能をサポートしていなければなりません。BGP デバイスがこの機能をサポートしているかどうかを確認するには、**show ip bgp neighbors** コマンドを使用します。デバイスがルート リフレッシュ機能をサポートしている場合、次のメッセージが出力されます。

```
Received route refresh capability from peer.
```

bgp soft-reconfig-backup コマンドは、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を実行するように BGP を設定するために導入されました。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。

BGP ルート集約

BGP ピアはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約を使用することにより、関係する情報の量が減ります。集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティングテーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。これにより、アドバタイズが必要なルートの数が少なくなります。

BGP でのルート集約の実装方法は 2 種類あります。集約されたルートを BGP に再配布するか、または条件付き集約の形を使用することができます。基本ルートの再配布では、集約ルートの作成後、このルートが BGP に再配布されます。条件付き集約では、集約ルートの作成後、ア

ドバタイズするか、または Autonomous System Set Path（AS-SET）情報、もしくは要約情報に基づいて、特定ルートのアドバタイズを抑制します。

bgp suppress-inactive コマンドは、非アクティブのルートをどの BGP ピアにもアドバタイズしないように BGP を設定します。BGP ルーティング プロセスは、デフォルトで、ルーティング情報データベース（RIB）にインストールされていないルートを BGP ピアにアドバタイズできます。RIB にインストールされていないルートは非アクティブなルートです。非アクティブなルートのアドバタイズメントは、たとえば、共通のルート集約を通じてルートがアドバタイズされた場合に行われます。非アクティブなルートのアドバタイズメントを抑制して、より整合性の取れたデータ フォワーディングを行うことができます。

BGP 集約ルートの AS_SET 情報生成

AS_SET 情報は、**aggregate-address** コマンドを使用して、BGP ルートが集約されたときに生成されます。このようなルートについてアドバタイズされたパスは、コミュニティを含め、要約されているすべてのパスに含まれる、すべての要素から構成される AS_SET です。集約される AS_PATH が同じものである場合、AS_PATH だけがアドバタイズされます。**aggregate-address** コマンド用にデフォルトで設定されている ATOMIC_AGGREGATE 属性は、AS_SET には追加されません。

ルーティング ポリシーの変更管理

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブルの更新に影響する可能性のあるルート マップ、配布リスト、プレフィックス リスト、フィルタ リストなど、すべての要素に関するコンフィギュレーションが含まれています。ルーティング ポリシーの変更があるたびに、ポリシーの変更がピアに自動的に更新されます。インバウンド リセットを実行すると、ルータで設定されている新しいインバウンド ポリシーが有効になります。アウトバウンド リセットを実行すると、BGP セッションをリセットしなくても、ルータで設定されている新しいローカル アウトバウンド ポリシーが有効になります。アウトバウンドポリシーのリセット中に、新しい一連のアップデートが送信されると、ネイバーの新しいインバウンド ポリシーも有効になります。つまり、インバウンド ポリシーの変更後は、ローカル ルータでインバウンド リセットを実行するか、ピア ルータでアウトバウンド リセットを実行する必要があります。アウトバウンド ポリシーを変更した場合は、ローカル ルータでのアウトバウンド リセット、またはピア ルータでのインバウンド リセットが必要になります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。下の表は、これらの利点と欠点をまとめたものです。

表 *12 :* ハード リセットとソフト リセットの利点および欠点

リセット タイプ	利点	欠点
ハード リセット	メモリ オーバーヘッドが起こらない。	ネイバーにより提供されるBGP、IP、および転送情報ベース（FIB）テーブル内のプレフィックスが失われる。非推奨
発信ソフト リセット	設定が必要ない。ルーティング テーブル アップデートの保存が必要ない。	インバウンド ルーティング テーブル アップデートがリセットされない。
ダイナミック インバウンド ソフト リセット	BGP セッションおよびキャッシュがクリアされない。 ルーティング テーブル アップデートの保存が必要ない。また、メモリのオーバーヘッドが発生しない。	両方の BGP ルータでルート リフレッシュ機能（Cisco IOS Release 12.1 以降）がサポートされている必要がある。 （注） アウトバウンド ルーティング テーブル アップデートがリセットされない。
設定済みのインバウンド ソフト リセット（**neighbor soft-reconfiguration** ルータ コンフィギュレーション コマンドを使用）	どちらの BGP ルータも自動ルート リフレッシュ機能をサポートしていない場合に使用可能。 Cisco IOS Release 12.3(14)T では、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を設定するための **bgp soft-reconfig-backup** コマンドが導入されている。	再構成が必要である。 受信した（インバウンド）ルーティング ポリシー アップデートをすべてそのまま格納するため、メモリが大量に使用される。 どちらの BGP ルータも自動ルート リフレッシュ機能をサポートしていない場合など、絶対に必要な場合だけ推奨される。 （注） アウトバウンド ルーティング テーブル アップデートがリセットされない。

BGP ネイバーになるように定義された 2 つのルータは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィギュレーションの変更を有効にするために、BGP 接続をリセットする必要があります。

ソフト リセットは、インバウンドおよびアウトバウンド ルーティング アップデートで使用されるルーティング テーブルをアップデートします。Cisco IOS Release 12.1 以降では、事前設定を必要としないソフト リセットがサポートされています。このソフト リセットにより、BGP ルータの間でルート リフレッシュ要求やルーティング情報をダイナミックに交換し、対応するアウトバウンド ルーティング テーブルをアドバタイズできるようになります。ソフト リセットには 2 種類があります。

- ソフトリセットを使用して、ネイバーからインバウンドアップデートを生成することを、ダイナミック インバウンド ソフト リセットと呼びます。
- ソフトリセットを使用して、ネイバーに新しい一連のアップデートを送信することを、アウトバウンド ソフト リセットと呼びます。

事前にコンフィギュレーションを行わずにソフト リセットを使用するためには、BGP ピアでソフトルートリフレッシュ機能がサポートされていなければなりません。これは、ピアがTCPセッションを確立したときに送信されるOPENメッセージでアドバタイズされます。リリース12.1 以前の Cisco IOS リリースが実行されているルータでは、ルート リフレッシュ機能はサポートされていないため、**neighbor soft-reconfiguration** ルータ コンフィギュレーション コマンドを使用して、BGP セッションをクリアする必要があります。この方法で BGP セッションをクリアすると、ネットワークの動作が悪い影響を受けるため、これは最後の手段として使用してください。

条件付き BGP ルートの挿入

BGP を通じてアドバタイズされるルートは、通常、使用されるルートの数が最小化され、グローバル ルーティング テーブルのサイズが小さくなるように集約されます。しかし、共通のルート集約では、より具体的なルーティング情報（より正確であるが、パケットを宛先に転送するために必要なわけではない）がわかりにくくなってしまいます。ルーティングの精度は、共通のルート集約により低下します。これは、トポロジ的に大きな領域に広がる複数のアドレスやホストを表すプレフィックスを 1 つのルートに正確に反映させることはできないからです。シスコ ソフトウェアには、プレフィックスを BGP 由来とする方法がいくつか用意されています。BGP 条件付きルート インジェクション機能の導入以前は、既存の方法として、再配布や **network** または **aggregate-address** コマンドが使用されていました。ただし、これらの方法は、より具体的なルーティング情報（開始されるルートと一致するもの）がルーティング テーブルまたは BGP テーブルのいずれかに存在することを前提にしています。

BGP の条件付きルートの挿入により、一致するものがなくても、プレフィックスを BGP ルーティング テーブルにすることができます。この機能を使って、管理ポリシーやトラフィック エンジニアリング情報に基づいて、より具体的なルートを生成することができます。これにより、設定された条件が満たされた場合にだけ BGP ルーティング テーブルに挿入される、より具体的なルートへのパケットの転送をさらに厳密に制御できるようになります。この機能をイネーブルにすると、条件に応じて、あまり具体的ではないプレフィックスにより具体的なプレフィックスを挿入または置き換えることにより、共通のルート集約の精度を高めることができるようになります。元のプレフィックスと同じ、またはより具体的なプレフィックスだけが挿入されます。BGP条件付きルートインジェクションを有効にするには、**bgp inject-map exist-map** コマンドを使用します。また、BGP条件付きルートインジェクションでは、2つのルートマップ（挿入マップと存在マップ）を使用して、1 つ（または複数）のより具体的なプレフィックスが BGP ルーティング テーブルに挿入されます。存在マップは、BGP スピーカーが追跡するプレフィックスを指定します。inject map は、ローカル BGP テーブルで作成され、このテーブルにインストールされるプレフィックスを定義します。

（注） 挿入マップおよび存在マップで一致となるプレフィックスはルートマップ句ごとに1つだけです。さらにプレフィックスを挿入するには、ルート マップ句を追加で設定する必要があります。複数のプレフィックスが使用されている場合は、一致する最初のプレフィックスが使用されます。

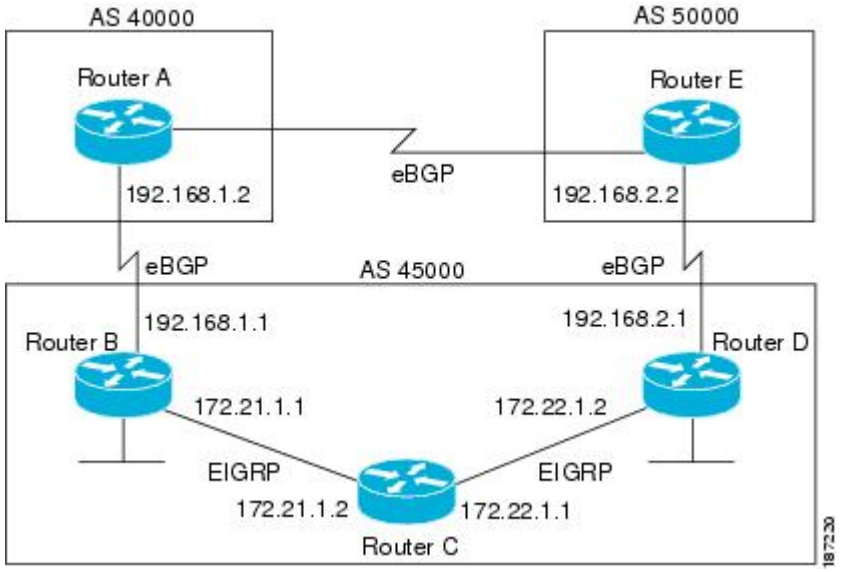
BGP ピア グループ

BGP ネットワークでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります. 同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、コンフィギュレーションのアップデートをより効率化するために、BGP ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

BGP バックドア ルート

さまざまな自律システムとの通信に eBGP を使用する境界デバイスを 2 つ使った BGP ネットワーク トポロジでは、2つの境界デバイス間の通信で、最も効果的なルーティング方法はeBGPを使用することではありません。下の図では、ルータ B はBGP スピーカーとして、eBGP を通るルータ D へのルートを受け取りますが、このルートは少なくとも 2 つの自律システムを横切っています。また、ルータ B とルータ D は Enhanced Interior Gateway Routing Protocol（EIGRP）ネットワーク（ここでは、すべての IGP を使用可能）を通じて接続されていますが、これが最短ルートです。しかし、EIGRP ルートのデフォルト アドミニストレーティブ ディスタンスは 90 で、eBGP ルートのデフォルト アドミニストレーティブ ディスタンスは 20 であるため、BGP は eBGP ルートを選びます。アドミニストレーティブ ディスタンスを変更すると、ルーティングがループする可能性があるため、デフォルト アドミニストレーティブ ディスタンスの変更は推奨しません。BGP に EIGRP ルートを選択させるには、**network backdoor** コマンドを使用します。BGP は、**network backdoor** コマンドで指定されたネットワークをローカルに割り当てられたネットワークとして扱います。ただし、BGPアップデートで指定されたネットワークのアドバタイズは行いません。これは、 下の図では、ルータ B は長い eBGP ルートの代わりに、短い EIGRP を使ってルータ D と通信するという意味です。

図 *10 : BGP* バックドア ルートのトポロジ



ピア グループおよび BGP アップデート メッセージ

リリース 12.0(24)S、12.2(18)S、または 12.3(4)T 以前の Cisco IOS ソフトウェア リリースでは、BGP アップデート メッセージは、ピア グループのコンフィギュレーションに基づいてグループ化されていました。BGP アップデート メッセージ生成において、ネイバーをグループ化するこの方法により、ルーティングテーブルのスキャンに必要なシステム処理リソースの量が削減されました。しかし、この方法には、次のような制約がありました。

- ピア グループ コンフィギュレーションを共有するネイバーはすべて、アウトバウンドルーティング ポリシーも共有する必要がある。
- すべてのネイバーは同じピア グループとアドレス ファミリに属している必要がある。別のアドレス ファミリで設定されているネイバーは異なるピアグループに属することはできません。

このような制約は、ピア グループ コンフィギュレーションに対して、最適なアップデート生成とレプリケーションのバランスをとるためのものでした。これらの制約により、ネットワーク オペレータは小さめのピア グループを設定するようになるため、アップデート メッセージの生成効率が下がり、ネイバー コンフィギュレーションのスケーラビリティが限定されていました。

BGP アップデート グループ

BGP（ダイナミック）アップデート グループの導入により、既存の BGP ピア グループから異なるタイプの BGP ピア グループ分けが可能になります。既存のピア グループは影響を受けませんが、現在のピア グループのメンバではない、同一のアウトバウンド ポリシーを持つ設定済みピアをアップデート グループに入れることができます。このアップデート グループのメ

ンバは同一のアップデート生成エンジンを使用します。BGP アップデート グループを設定すると、アウトバウンド ポリシーに基づいて、BGP アップデート グループ メンバーシップがダイナミックに計算されます。最適な BGP アップデート メッセージの生成は、単独で自動的に行われます。BGP ネイバー コンフィギュレーションはアウトバウンド ルーティング ポリシーによる制約を受けなくなり、アップデート グループは異なるアドレス ファミリに属すことができるようになります。

BGP ダイナミック アップデート グループのコンフィギュレーション

Cisco IOS Release 12.0(24)S、12.2(18)S、12.3(4)T、12.2(27)SBC、およびそれ以降のリリースには、同一のアウトバウンド ポリシーを共有し、同一のアップデート メッセージを共有するネイバーのアップデート グループをダイナミックに計算および最適化できる新しいアルゴリズムが導入されました。BGP ダイナミック アップデート グループをイネーブルにするための設定は必要ありません。アルゴリズムは自動的に実行されます。アウトバウンドポリシーが変更された場合、ルータは、1 分間のタイマー期限が切れた後で、アウトバウンド ソフト リセットをトリガーすることにより、自動的にアップデート グループ メンバーシップを再計算し、変更を適用します。この動作は、ネットワーク オペレータがミスを犯した場合に、コンフィギュレーションを変更する時間を与えるように設計されています。タイマー期限が切れる前に、アウトバウンド ソフト リセットを手動で有効にするには、**clear ip bgp** *ip-address* **soft out** コマンドを入力します。

（注） Cisco IOS Release 12.0(22)S、12.2(14)S、12.3(2)T およびそれ以前のリリースでは、アップデート グループの再計算遅延タイマーは 3 分間に設定されています。

BGP アップデート グループの生成を最適化するには、ネットワーク オペレータは、類似するアウトバウンド ポリシーを持つネイバーのアウトバウンド ルーティング ポリシーを同じものにしておくことを推奨します。

BGP Peer テンプレート

構成管理など、ピア グループの制約の一部に対応するため、BGP アップデート グループ コンフィギュレーションをサポートする BGP ピア テンプレートが導入されました。

ピア テンプレートは、ポリシーを共有するネイバーに適用可能なコンフィギュレーション パターンです。ピア テンプレートは再利用が可能で、継承がサポートされているため、ネットワーク オペレータはピア テンプレートを使用して、ポリシーを共有している BGP ネイバーに対して異なるネイバー コンフィギュレーションをグループ化し適用できます。また、ネットワーク オペレータは、別のピア テンプレートからコンフィギュレーションを継承できるというピア テンプレートの機能を使用して、非常に複雑なコンフィギュレーション パターンを定義できるようになります。

ピア テンプレートには 2 種類あります。

- ピア セッション テンプレート。アドレス ファミリ モードおよびNLRI コンフィギュレーション モードすべてに共通する一般的なセッション コマンドのコンフィギュレーションをグループ化し、適用するために使用されます。
- ピア ポリシー テンプレート。特定のアドレス ファミリおよびNLRI コンフィギュレーション モードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。

ピア テンプレートにより、柔軟性が高まり、ネイバー コンフィギュレーションの機能が強化されます。また、ピア テンプレートはピア グループ コンフィギュレーションに代わるものを提供し、ピア グループの制約の一部を解決します。ピア テンプレートを使用した BGP ピア ルータも、自動アップデート グループ コンフィギュレーションの恩恵を受けています。BGP ピア テンプレートが設定され、BGP ダイナミック アップデート ピア グループがサポートされたことにより、ネットワーク オペレータは BGP でピア グループを設定する必要がなくなります。また、ネットワークはコンフィギュレーションの柔軟性が高まり、コンバージェンスが高速化されたことによる恩恵を受けます。

（注） BGP ネイバーを、ピア グループとピア テンプレートの両方と連動するようには設定できません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートからポリシーを継承するように設定します。

ピア ポリシー テンプレートには、次の制約事項が適用されます。

- ピア ポリシー テンプレートは、直接的、または間接的に、最高 8 個のピア ポリシー テンプレートを継承できます。
- BGP ネイバーを、ピア グループとピア テンプレートの両方と連動するようには設定できません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートだけからポリシーを継承するように設定できます。

ピア テンプレートでの継承

継承機能は、ピア テンプレート操作の重要なコンポーネントです。ピア テンプレートでの継承は、たとえば、ファイルとディレクトリ ツリーなど、一般的なコンピューティングで見られるノードとツリーの構造に似ています。ピア テンプレートは、別のピア テンプレートから直接、または間接的にコンフィギュレーションを継承することができます。直接継承されたピア テンプレートは、構造体のツリーを表します。間接的に継承されたピア テンプレートはツリーのノードを表します。個々のノードも継承をサポートしているため、チェーン内で間接的に継承されたピア テンプレートすべてのコンフィギュレーションを、直接継承されたピア テンプレート、またはツリーのソースに適用するブランチも作成できます。

この構造により、ネイバーのグループに通常、再適用されるコンフィギュレーション文を繰り返す必要がなくなります。これは、共通のコンフィギュレーション文を一度適用しておくと、その後は共通のコンフィギュレーションを持つネイバー グループに適用されるピア グループにより間接的に継承されるからです。ノードとツリーの内部で別々に複製されたコンフィギュ

レーション文は、直接継承したテンプレートにより、ツリーのソースでフィルタ処理されます。直接継承されたテンプレートは、直接継承されたテンプレートで複製された、間接的に継承された文をすべて上書きします。

継承によりネイバー コンフィギュレーションのスケーラビリティと柔軟性がさらに広がり、複数のピアテンプレート コンフィギュレーションをチェーンして、共通のコンフィギュレーション文を継承する単純なコンフィギュレーションを作成したり、共通に継承されるコンフィギュレーションとともに非常に限定的なコンフィギュレーション文を適用する複雑なコンフィギュレーションを作成したりできるようになります。ピア セッション テンプレートおよびピア ポリシーテンプレートでの継承の設定についての詳細は、これ以降のセクションで説明します。

BGP ネイバーが継承したピア テンプレートを使用する場合、特定のテンプレートに関連付けられているポリシーを判断するのが難しいことがあります。**show ip bgptemplate peer-policy** コマンドに、特定のテンプレートに関連付けられているローカルポリシーおよび継承されたポリシーの詳しいコンフィギュレーションを表示するためのキーワード **detail** が追加されました。

ピア セッション テンプレート

ピア セッション テンプレートは、一般的なセッション コマンドのコンフィギュレーションをグループ化し、セッション コンフィギュレーション要素を共有するネイバーのグループに適用するために使用されます。異なるアドレス ファミリで設定されているネイバーに共通する一般的なセッション コマンドは、同じピア セッション テンプレートに設定できます。ピア セッション テンプレートの作成と設定は、ピア セッション コンフィギュレーション モードで行います。ピア セッション テンプレートで設定できるのは、一般的なセッション コマンドだけです。次の一般的なセッション コマンドは、ピア セッション テンプレートでサポートされています。

- **description**
- **disable-connected-check**
- **ebgp-multihop**
- **exit peer-session**
- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

一般的なセッション コマンドをピア セッションで一度設定しておくと、ピア セッション テンプレートの直接適用、またはピア セッション テンプレートの間接継承によって、多数のネイバーに適用できます。ピア セッション テンプレートのコンフィギュレーションにより、自律システム内のすべてのネイバーに共通に適用される一般的なセッション コマンドのコンフィギュレーションが簡素化されます。

ピア セッション テンプレートは、直接継承と間接継承をサポートします。一度にピアの設定に使用できるピア セッション テンプレートは 1 つだけです。また、このピア セッション テンプレートは、間接継承されたピア セッション テンプレートを 1 つだけ含むことができます。

（注） 1 つのピア セッション テンプレートを使って、複数の継承文を設定しようとすると、エラー メッセージが表示されます。

この動作により、BGP ネイバーは 1 つのセッション テンプレートだけを直接継承し、最高 7 個のピア セッション テンプレートを間接継承できます。したがって、1 つのネイバーに最高 8 個のピア セッション コンフィギュレーション（直接継承されたピア セッション テンプレートのコンフィギュレーションと最高 7 個の間接継承されたピア セッション テンプレートのコンフィギュレーション）を適用できます。継承されたピア セッション コンフィギュレーションが最初に評価され、ブランチの最後のノードから、ツリーのソースで直接適用されたピア セッション テンプレートまで適用されます。直接適用されたピア セッション テンプレートは、継承されたピア セッション テンプレート コンフィギュレーションよりも優先されます。継承されたピア セッション テンプレートで複製されたコンフィギュレーション文はすべて、直接適用されたピア セッション テンプレートにより上書きされます。したがって、基本セッション コマンドが異なる値で再び適用される場合は、後の値が優先され、間接的に継承されたテンプレートに設定されていた前の値は上書きされます。次に、この機能を使用した例を示します。

次の例では、一般セッション コマンド **remote-as 1** がピア セッション テンプレート SESSION-TEMPLATE-ONE に適用されます。

```
template peer-session SESSION-TEMPLATE-ONE
 remote-as 1
 exit peer-session
```

ピア セッション テンプレートは、一般的なセッション コマンドだけをサポートします。特定のアドレス ファミリ、または NLRI コンフィギュレーション モードだけのために設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

ピア ポリシー テンプレート

ピア ポリシー テンプレートは、特定のアドレス ファミリおよび NLRI コンフィギュレーション モードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。ピア ポリシー テンプレートの作成と設定は、ピア ポリシー コンフィギュレーション モードで行います。特定のアドレス ファミリ専用に設定される BGP ポリシー コマンドは、ピア ポリシー テンプレートで設定されます。ピア ポリシー テンプレートでは、次の BGP ポリシー コマンドがサポートされています。

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**
- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

ピア ポリシー テンプレートは、特定のアドレス ファミリに属するネイバーに設定される BGP ポリシー コマンドの設定に使用されます。ピア セッション テンプレートと同様、ピア ポリシーテンプレートを一度設定しておくと、直接適用、または継承を通じて、多数のネイバーにピア ポリシー テンプレートを適用することができます。ピア ポリシー テンプレートの設定により、自律システム内のすべてのネイバーに適用される BGP ポリシー コマンドの設定が簡略化されます。

ピア セッション テンプレートと同様、ピア ポリシー テンプレートは継承をサポートしています。しかし、多少の違いはあります。直接適用されたピア ポリシー テンプレートは、最大 7 つのピア ポリシーテンプレートから設定を直接的または間接的に継承できます。したがって、合計 8 つのピア ポリシー テンプレートをネイバーまたはネイバー グループに適用できます。ルート マップと同じように、継承されたピア ポリシー テンプレートにはシーケンス番号が設定されます。また、ルート マップと同じように、継承されたピア ポリシー テンプレートは、最も低いシーケンス番号を持つ **inherit peer-policy** 文が最初に評価され、最も高いシーケンス

番号のものが最後に評価されます。ただし、ピア ポリシー テンプレートはルート マップのように折りたたむことはできません。シーケンスはすべて評価されます。異なる値を使って、BGP ポリシー コマンドが再適用された場合は、シーケンス番号の小さいものから順に、前の値がすべて上書きされます。

直接適用されたピア ポリシーテンプレートと、シーケンス番号が最も大きい **inherit peer-policy** 文のプライオリティは常に最も高く、最後に適用されます。これ以降のピアテンプレートに再適用されるコマンドは、必ず、前の値を上書きします。この動作は、個々のポリシーコンフィギュレーション コマンドを重複させることなく、共通のポリシー コンフィギュレーションは大規模なネイバー グループに適用し、特定のポリシー コンフィギュレーションは特定のネイバーやネイバー グループだけに適用できるように設計されています。

ピア ポリシー テンプレートは、ポリシー コンフィギュレーション コマンドだけをサポートします。特定のアドレス ファミリ用に設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

ピア ポリシー テンプレートの設定により、BGP 設定が簡略化され、柔軟性が向上します。特定のポリシーを 1 回設定すれば、何回も参照できます。ピア ポリシーは最大 8 レベルの継承をサポートするため、非常に具体的で複雑な BGP ポリシーも作成できます。

IPv4 アドレス ファミリの下での BGP IPv6 ネイバーのアクティブ化

Cisco IOS Release 12.2(33)SRE4 よりも前のリリースでは、デフォルトで IPv6 と IPv4 の両方の機能は、IPv6 アドレスを持つ BGP ピアと交換されます。IPv6 ピアを設定すると、そのネイバーは、IPv4 ユニ キャスト アドレス ファミリの下で自動的にアクティブになります。

Cisco IOS Release 12.2(33)SRE4 以降では、新しい IPv6 ネイバーが設定されると、IPv4 アドレス ファミリの下では自動的にアクティブ化されません。たとえば、デュアル スタック環境があり、IPv6 と IPv4 プレフィックスを送信しようとする場合、IPv4 アドレス ファミリの下で手動で IPv6 ネイバーをアクティブにできます。

既存の IPv6 ピアを IPv4 アドレス ファミリの下でアクティブにしない場合、**no neighbor activate** コマンドでピアを手動で非アクティブにできます。それまでは、IPv4 ユニキャスト アドレス ファミリの下で IPv6 ネイバーをアクティブにする既存のコンフィギュレーションはセッションの確立を試行し続けます。

基本 BGP ネットワークの設定方法

ベーシック BGP ネットワークの設定は、いくつかの必須作業と多数の任意の作業からなります。BGP ルーティング プロセスと BGP ピアは必ず設定する必要がありますが、このとき、できればアドレス ファミリ コンフィギュレーション モデルを使用してください。BGP ピアが VPN ネットワークの一部である場合、BGP ピアの設定には、IPv4 VRF アドレス ファミリ タスクを使用する必要があります。次にあげるその他の作業は任意です。

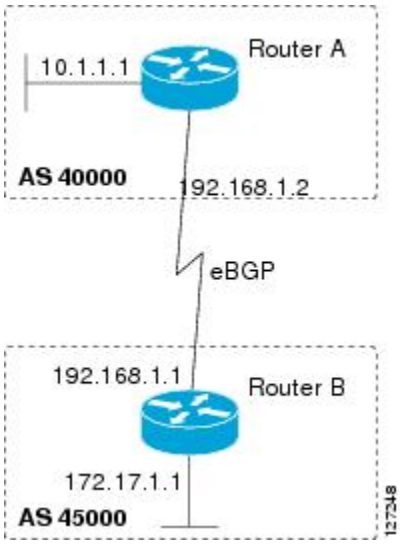
BGP ルーティング プロセスの設定

BGPルーティングプロセスを設定するには、次の作業を実行します。BGPを有効にするには、必須の手順を少なくとも一度、実行する必要があります。ここで説明する任意の手順を実行すると、BGP ネットワークでその他の機能を設定できます。ネイバー リセットのロギングやリンクが停止したときのピアの即時リセットなど、一部の機能はデフォルトで有効にされていますが、BGPネットワークの動作方法をよりよく理解できるようにするため、これらの機能についてはここで説明しています。

（注） シスコ ソフトウェアを実行するデバイスは、1つのBGPルーティングプロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスおよび自律システムは、同時に使用する複数の BGP アドレス ファミリおよびサブアドレス ファミリ コンフィギュレーションをサポートできます。

下の図では、この作業のコンフィギュレーションはルータ A で行われますが、2 つのデバイスの間で BGP プロセスを完全に実現するには、たとえば、ルータ B で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。ここでは、BGP ルーティング プロセスに対して設定されるアドレス ファミリはないため、IPv4 ユニキャスト アドレス ファミリのルーティング情報はデフォルトでアドバタイズされます。

図 *11 : 2* つの自律システムを持つ *BGP* トポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
5. **bgp router-id** *ip-address*

6. **timers bgp** *keepalive holdtime*
7. **bgp fast-external-fallover**
8. **bgp log-neighbor-changes**
9. **end**
10. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	BGP ルーティング プロセスを設定し、指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • *autonomous-system-number* 引数を使用して、0 ～ 65534 の範囲の整数を 1 つ指定します。これは、その他の BGP スピーカーへのデバイスを表します。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router)# network 10.1.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 5	**bgp router-id** *ip-address* 例： `Device(config-router)# bgp router-id 10.1.1.99`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル デバイスの ID として設定します。 • *ip-address* 引数を使用して、ネットワーク内で固有のルータ ID を指定します。 （注） **bgp router-id** コマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションがすべてリセットされます。

	コマンドまたはアクション	目的
ステップ 6	**timers bgp** *keepalive holdtime* 例： `Device(config-router)# timers bgp 70 120`	（任意）BGP ネットワーク タイマーを設定します。 • *keepalive* 引数を使用して、頻度を秒単位で指定します。ソフトウェアはこの間隔で、BGP ピアにキープアライブ メッセージを送信します。デフォルトでは、keepalive タイマーは 60 秒に設定されます。 • *holdtime* 引数を使用して、インターバルを秒単位で指定します。この時間を過ぎても、キープアライブ メッセージが届かなかった場合、BGP ピアはデッドであると宣言されます。デフォルトでは、holdtime タイマーは 180 秒に設定されます。
ステップ 7	**bgp fast-external-fallover** 例： `Device(config-router)# bgp fast-external-fallover`	（任意）BGP セッションの自動リセットをイネーブルにします。 • デフォルトでは、直接隣接する外部ピアへのアクセスに使用されるリンクがダウンした場合、このピアの BGP セッションはリセットされます。
ステップ 8	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	（任意）BGP ネイバー ステータスの変更（アップまたはダウン）およびネイバーのリセットのロギングをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp** [*network*] [*network-mask*] 例：	（任意）BGP ルーティング テーブル内のエントリを表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp`	（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を上の図のルータ A で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。この自律システムに対してローカルなネットワーク 10.1.1.0 に対するエントリも表示されています。

```
BGP table version is 12, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性をチェックするには、**ping** コマンドを使用します。

BGP ピアの設定

2 つの IPv4 ルータ（ピア）の間に BGP を設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は上の図のルータ A で行われています。BGP ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

始める前に

この作業を実行する前に、前項に示されている「BGP ルーティング プロセスの設定」の作業を実行します。

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **activate**
7. **end**
8. **show ip bgp** [*network*] [*network-mask*]
9. **show ip bgp neighbors** [*neighbor-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。

	コマンドまたはアクション	目的
		• **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 192.168.1.1 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。
ステップ 7	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 8	**show ip bgp** [*network*] [*network-mask*] 例： `Router# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 9	**show ip bgp neighbors** [*neighbor-address*] 例： `Router(config-router-af)# show ip bgp neighbors 192.168.2.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を上の図のルータ A およびルータ B で設定した後で、ルータ A の BGP ルーティング テーブルを表示する **show ip bgp** コマンドの出力例を示します。これで、自律システム 45000 でネットワーク 172.17.1.0 のエントリを確認できるようになります。

```
BGP table version is 13, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
             r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
*> 172.17.1.0/24    192.168.1.1              0             0 45000 i
```

次に、この作業を上の図のルータ A で設定した後で、ルータ A の BGP ネイバー 192.168.1.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例を示します。

```
BGP neighbor is 192.168.1.1,  remote AS 45000, external link
  BGP version 4, remote router ID 172.17.1.99
  BGP state = Established, up for 00:06:55
  Last read 00:00:15, last write 00:00:15, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            13         13
    Route Refresh:          0          0
    Total:                 15         16
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 13, neighbor version 13/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             1          1 (Consumes 52 bytes)
    Prefixes Total:               1          1
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          1
    Used as multipath:          n/a          0
                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    AS_PATH loop:                    n/a          1
    Bestpath from this peer:           1        n/a
    Total:                             1          1
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.1.2, Local port: 179
Foreign host: 192.168.1.1, Foreign port: 37725
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x12F4F2C):
Timer          Starts    Wakeups            Next
Retrans            14          0             0x0
TimeWait            0          0             0x0
AckHold            13          8             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
```

```
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss:  165379618  snduna:  165379963  sndnxt:  165379963     sndwnd:  16040
irs: 3127821601  rcvnxt: 3127821993  rcvwnd:      15993  delrcvwnd:    391
SRTT: 254 ms, RTTO: 619 ms, RTV: 365 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 20 (out of order: 0), with data: 15, total data bytes: 391
Sent: 22 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 04
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性を確認するには、**ping** コマンドを使用します。

次の作業

VPN で BGP ピアを使用している場合は、IPv4 VRF アドレス ファミリ用に BGP ピアを設定 （114 ページ）に進みます。VPN で BGP ピアを使用していない場合は、BGP ピアのカスタマイズ （45 ページ）に進みます。

BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定

4 バイト自律システム（AS）番号を使用する AS にボーダー ゲートウェイ プロトコル（BGP）ピアが配置されているときに、BGP ルーティング プロセスおよび BGP ピアを設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は上の図（「シスコが採用している 4 バイト自律システム番号」の項）のルータ A で行われています。この作業にある 4 バイト AS 番号は、デフォルトの asplain（10 進数値）形式にフォーマットされています。たとえば、上の図にあるルータ B の AS 番号は 65538 です。BGP ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

始める前に

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. 必要に応じて、手順 4 を繰り返し、その他の BGP ネイバーを定義します。
6. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
7. **neighbor** *ip-address* **activate**
8. 必要に応じて、手順 7 を繰り返し、その他の BGP ネイバーをアクティブ化します。
9. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
10. **end**
11. **show ip bgp** [*network*] [*network-mask*]
12. **show ip bgp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 65538`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 65536`	指定された AS のネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、4 バイト AS 番号 65536 は asplain 表記法で定義されています。
ステップ 5	必要に応じて、手順 4 を繰り返し、その他の BGP ネイバーを定義します。	--
ステップ 6	**address-family ipv4** [**unicast**	**multicast**	**vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4

	コマンドまたはアクション	目的
		ユニキャストアドレスファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.2 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 8	必要に応じて、手順 7 を繰り返し、その他の BGP ネイバーをアクティブ化します。	--
ステップ 9	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この AS にローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp 10.1.1.0`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 12	**show ip bgp summary** 例：	（任意）BGP 接続すべての状況を表示します。

	コマンドまたはアクション	目的
	Device# show ip bgp summary	

例

次の例は、上の図のルータ B で実行された **show ip bgp** コマンドの出力ですが、ここにはルータ A で 192.168.1.2 にある BGP ネイバーから学習されたネットワーク 10.1.1.0 に対する BGP ルーティング テーブル エントリと、デフォルトの asplain 形式で表した 4 バイト AS 番号 65536 が表示されています。

```
RouterB# show ip bgp 10.1.1.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1)
  Advertised to update-groups:
     2
  65536
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

次の例は、**show ip bgp summary** コマンドの出力ですが、ここには、上の図のルータ B でこの作業を設定した後で、ルータ A にある BGP ネイバー 192.168.1.2 の 4 バイト AS 番号が 65536 であることが表示されています。

```
RouterB# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
3/2 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 806 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  Stated
192.168.1.2     4       65536       6       6        3    0    0 00:01:33       1
```

トラブルシューティングのヒント

BGP ルータ間の基本的なネットワーク接続性を確認するには、**ping** コマンドを使用します。

4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更

4 バイト自律システム（AS）番号のデフォルト出力形式を asplain 形式から asdot 表記法形式に変更するには、この作業を実行します。4 バイト AS 番号の出力形式の変化を表示するには、**show ip bgp summary** コマンドを使用します。

手順の概要

1. **enable**
2. **show ip bgp summary**
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **bgp asnotation dot**
6. **end**
7. **clear ip bgp ***
8. **show ip bgp summary**
9. **show ip bgp regexp** *regexp*
10. **configure terminal**
11. **router bgp** *autonomous-system-number*
12. **no bgp asnotation dot**
13. **end**
14. **clear ip bgp ***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp summary** 例： `Device# show ip bgp summary`	すべてのボーダーゲートウェイ プロトコル（BGP）接続のステータスを表示します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65538`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 5	**bgp asnotation dot** 例： `Device(config-router)# bgp asnotation dot`	BGP 4 バイト AS 番号のデフォルト出力形式を asplain（10 進数値）からドット表記法に変更します。

	コマンドまたはアクション	目的
		（注） 4 バイト AS 番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 6	**end** 例： `Device(config-router)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**clear ip bgp *** 例： `Device# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト AS 番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**show ip bgp summary** 例： `Device# show ip bgp summary`	BGP 接続すべての状況を表示します。
ステップ 9	**show ip bgp regexp** *regexp* 例： `Device# show ip bgp regexp ^1\.0$`	AS パスの正規表現と一致するルートを表示します。 • この例では、4 バイトの AS パスをマッチングする正規表現は、asdot 形式で設定されています。
ステップ 10	**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 11	**router bgp** *autonomous-system-number* 例：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 65538`	• この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 12	**no bgp asnotation dot** 例： `Device(config-router)# no bgp asnotation dot`	BGP 4 バイト AS 番号のデフォルト出力形式を asplain（10 進数値）にリセットします。 （注） 4 バイト AS 番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 13	**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 14	**clear ip bgp *** 例： `Device# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト AS 番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp summary** コマンドの出力は、4 バイト AS 番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト AS 番号 65536 および 65550 に注意してください。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハードリセットする **clear ip bgp *** コマンドが続きます）、出力は、次の **show ip bgp summary** コマンドの出力に示すように、asdot 表記法の形式に変換されます。asdot 形式で表された 4 バイト AS 番号 1.0 および 1.14 に注意してください。これらは AS 番号 65536 と 65550 を asdot 変換したものです。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24      0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハードリセットする **clear ip bgp *** コマンドが続きます）、4 バイトの AS パスで使用される正規表現とのマッチング形式は asdot 表記法の形式に変更されます。4 バイト AS 番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト AS 番号だけがマッチングされます。下の先頭の例では、**show ip bgp regexp** コマンドは、asplain 形式で表された 4 バイト AS 番号を使って設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの AS パスに関する情報が asdot 表記法を使って表示されます。

（注） この asdot 表記法で使用されているピリオドは、シスコの正規表現では特殊文字です。特殊な意味を取り除くには、ピリオドの前にバックスラッシュをつけます。

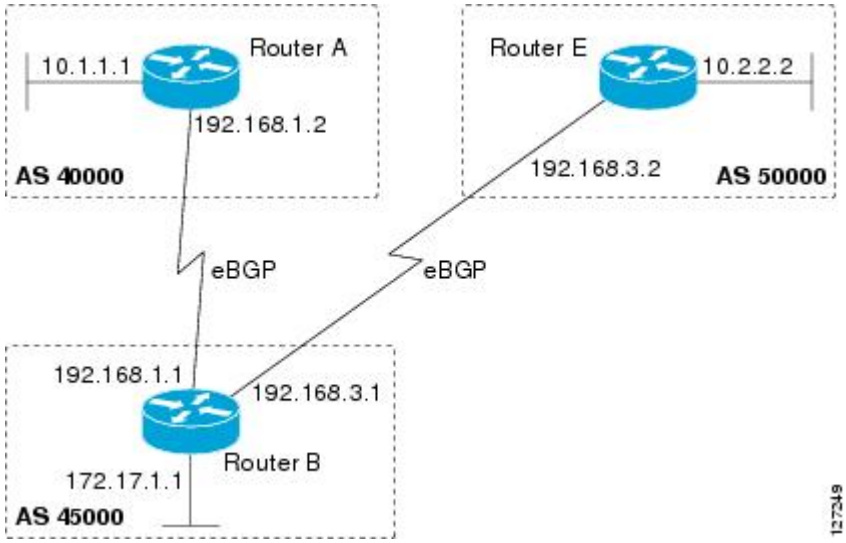
```
Router# show ip bgp regexp ^65536$

Router# show ip bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

IPv4 VRF アドレス ファミリ用に BGP ピアを設定

VPN 内に存在するため IPv4 VRF 情報を交換しなければならない 2 つの IPv4 ルータ（ピア）の間に BGP を設定するには、次の作業を任意で実行します。ここで設定するアドレス ファミリは IPv4 VRF アドレス ファミリで、設定は下の図のルータ B で自律システム 50000 のルータ E にあるネイバー 192.168.3.2 を使って行われています。BGP IPv4 VRF アドレス ファミリ ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

この作業は、VPNルーティングに必要な設定をすべて示しているわけではありません。完全な設定サンプル、および4バイト自律システム番号を使用する、ルートターゲットを使ったVRFの作成方法を示した設定サンプルについては、を参照してください。

図 *12 : IPv4 VRF* アドレス ファミリ用 *BGP* トポロジ



始める前に

この作業を実行する前に、BGP ルーティング プロセスの設定 （33 ページ）の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
9. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
10. **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
11. **neighbor** *ip-address* **activate**
12. **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf vpn1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • VRF に割り当てる名前を指定するには、*vrf-name* 引数を使用します。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 45000:5`	ルーティング テーブル、およびフォワーディング テーブルを作成し、VPN 用のデフォルト ルート識別子を指定します。 • 一意の VPN IPv4 プレフィックスを作成するために、IPv4 プレフィックスに 8 バイト値を追加するには、*route-distinguisher* 引数を使用します。
ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target both 45000:100`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲットVPN拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。 • ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • インポートおよびエクスポート ルーティング情報の両方をターゲットVPN拡張コミュニティにインポートするには、**both** キーワードを使用します。 • ルートターゲット拡張コミュニティ属性をVRFのインポート、エクスポート、または両方（インポートとエクスポート）のルート ターゲッ

	コマンドまたはアクション	目的
		ト拡張コミュニティ リストに追加するには、*route-target-ext-community* 引数を使用します。
ステップ 6	**exit** 例： `Router(config-vrf)# exit`	VRF 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 モードを開始します。
ステップ 7	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 8	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーションモードになります。 • IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 9	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.3.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**] 例： `Router(config-router-af)# neighbor 192.168.3.2 maximum-prefix 10000 warning-only`	ネイバーから受信できるプレフィックスの数を制御します。 • 特定のネイバーから受信できるプレフィックス数の最大値を指定するには、*maximum* 引数を使用します。設定可能なプレフィックス数は、ルータ上の使用可能なシステム リソースのみによって制限されます。

	コマンドまたはアクション	目的
		• プレフィックスの上限をパーセント単位で表した整数を指定するには、*threshold* 引数を使用します。この上限に達すると、ルータは警告メッセージの生成を開始します。 • プレフィックスの上限を超えた場合に、ピアリングセッションを終了する代わりに、ログメッセージを生成するようにルータを設定するには、**warning-only** キーワードを使用します。
ステップ 11	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 192.168.3.2 activate`	このネイバーをイネーブルにして、IPv4 VRF アドレス ファミリのプレフィックスをローカル ルータと交換します。
ステップ 12	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

トラブルシューティングのヒント

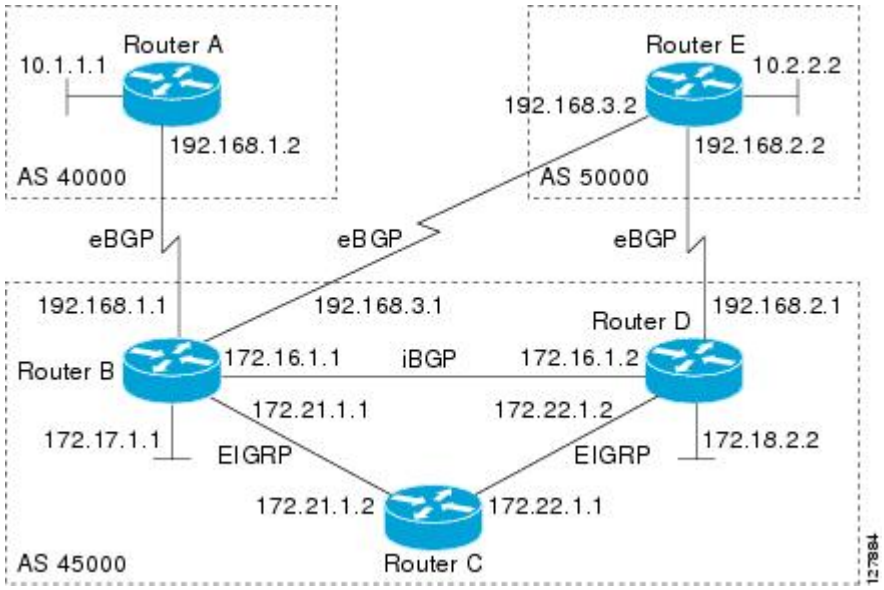
BGP ルータ間の基本的なネットワーク接続を検証するには **ping** コマンドを使用します。また、VRF インスタンスが作成されたことを確認するには **show ip vrf** コマンドを使用します。

BGP ピアのカスタマイズ

BGP ピアをカスタマイズするには、次の作業を実行します。この作業の手順の多くは任意ですが、ネイバーとアドレス ファミリ コンフィギュレーション コマンドの関係がどのように機能しているかを示しています。IPv4 マルチキャスト アドレス ファミリの例を使用すると、IPv4 マルチキャスト アドレス ファミリを設定する前に、ネイバー アドレス ファミリに依存しないコマンドが設定されます。その後、アドレス ファミリに依存するコマンドが設定され、**exit address-family** コマンドが表示されます。任意の手順は、ネイバーを無効にする方法を示しています。

下の図では、この作業のコンフィギュレーションがルータ B で行われます。2 つのデバイスの間で BGP プロセスを完全に実現するには、たとえば、ルータ E で IP アドレスを適宜、変更してこのコンフィギュレーションを繰り返す必要があります。

図 *13 : BGP* ピア トポロジ



（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*
11. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]
12. **exit-address-family**
13. **neighbor** {*ip-address* | *peer-group-name*} **shutdown**
14. **end**
15. **show ip bgp ipv4 multicast** [*command*]
16. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received prefix-filter**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **description** *text* 例： `Device(config-router)# neighbor 192.168.3.2 description finance`	（任意）テキストによる説明を指定されたネイバーと関連付けます。

	コマンドまたはアクション	目的
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 multicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャストアドレスファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 8	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.3.2 activate`	BGP ネイバーとの情報交換を有効にします。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds* 例： `Device(config-router-af)# neighbor 192.168.3.2 advertisement-interval 25`	（任意）BGP ルーティング アップデートの最小送信間隔を設定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] 例： `Device(config-router-af)# neighbor 192.168.3.2 default-originate`	（任意）デフォルトルートとして使用するために、BGP スピーカー（ローカル デバイス）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。

	コマンドまたはアクション	目的
ステップ 12	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 13	**neighbor** {*ip-address* | *peer-group-name*} **shutdown** 例： `Device(config-router)# neighbor 192.168.3.2 shutdown`	（任意）BGP ピア、またはピア グループを無効にします。 （注） この手順を実行すると、ネイバーが無効化されるため、この後の **show** コマンドを使った手順をいずれも実行できなくなります。
ステップ 14	**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。
ステップ 15	**show ip bgp ipv4 multicast** [*command*] 例： `Device# show ip bgp ipv4 multicast`	（任意）IPv4 マルチキャスト データベース関連情報を表示します。 • サポートされているマルチプロトコル BGP コマンドがあれば、*command* 引数を使用して指定します。サポートされているコマンドを表示するには、CLI で ? プロンプトを使用します。
ステップ 16	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received prefix-filter**] 例： `Device# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。

例

次に、この作業を上の図のルータ B およびルータ E で設定した後で、ルータ B の BGP IPv4 マルチキャスト情報を表示する **show ip bgp ipv4 multicast** コマンドの出力例を示します。IPv4 マルチキャスト アドレス ファミリで設定された各デバイスに対してローカルなネットワークは、出力テーブルに表示されます。

```
BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
```

```
*> 10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

次は、ネイバー 192.168.3.2 に対する **show ip bgp neighbors** コマンドからの出力例の一部分ですが、これにはこのネイバーに関する一般的な BGP 情報と、具体的な BGP IPv4 マルチキャスト アドレス ファミリ情報が表示されます。このコマンドは、上の図のルータ B とルータ E でこの作業を設定した後、ルータ B で入力されたものです。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Description: finance
  BGP version 4, remote router ID 10.2.2.99
  BGP state = Established, up for 01:48:27
  Last read 00:00:26, last write 00:00:26, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised
    Address family IPv4 Multicast: advertised and received
!
 For address family: IPv4 Multicast
  BGP table version 3, neighbor version 3/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
    Uses NEXT_HOP attribute for MBGP NLRIs
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              1          1 (Consumes 48 bytes)
    Prefixes Total:                1          1
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          1
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from this peer:              1        n/a
    Total:                                1          0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 25 seconds
  Connections established 8; dropped 7
  Last reset 01:48:54, due to User reset
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.3.1, Local port: 13172
Foreign host: 192.168.3.2, Foreign port: 179
!
```

再配布を使用した BGP コンフィギュレーション コマンドの削除

小規模な BGP ネットワークであっても、BGP CLI コンフィギュレーションは非常に複雑になることがあります。すべての CLI コンフィギュレーションを削除する必要がある場合は、CLI を削除することで生じるあらゆる影響を考慮する必要があります。現在の実行コンフィギュレーションを分析し、現在の BGP ネイバー関係、アドレス ファミリの考慮事項、その他の設定済みルーティング プロトコルを判断します。BGP CLI コマンドの多くは、CLI コンフィギュレーションのその他の部分に影響を与えています。

EIGRP への BGP ルートの再配布で使用されている BGP コンフィギュレーション コマンドをすべて削除するには、この作業を実行します。ルート マップをパラメータのマッチングや設定、再配布ルートのフィルタに使用して、これらのルートが EIGRP によりアドバタイズされるときに、ルーティング ループが発生しないようにすることができます。BGP コンフィギュレーション コマンドを削除する場合は、必ず、関連するコマンドをすべて削除、または無効にしてください。この例では、**route-map** コマンドを省略しても、再配布は行われ、ルート マップのフィルタリングが取り除かれているために、予期しない結果となる可能性があります。**redistribute** コマンドだけを省略すると、ルート マップは適用されませんが、実行コンフィギュレーションに未使用コマンドが残ります。

BGP CLI の削除の詳細については、「Cisco BGP 概要」モジュールの「BGP CLI 削除の考慮事項」の概念を参照してください。

CLI を削除する前と後の再配布コンフィギュレーションの表示については、「例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no route-map** *map-name*
4. **router eigrp** *autonomous-system-number*
5. **no redistribute** *protocol* [*as-number*]
6. **end**
7. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**no route-map** *map-name* 例： `Device(config)# no route-map bgp-to-eigrp`	実行コンフィギュレーションからルート マップを削除します。 • この例では、bgp-to-eigrp というルート マップがコンフィギュレーションから削除されています。

	コマンドまたはアクション	目的
ステップ 4	**router eigrp** *autonomous-system-number* 例： `Device(config)# router eigrp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 5	**no redistribute** *protocol* [*as-number*] 例： `Device(config-router)# no redistribute bgp 45000`	あるルーティング ドメインから別のルーティング ドメインへのルートの再配布をディセーブルにします。 • この例では、EIGRP ルーティング プロセスへの BGP ルートの再配布のコンフィギュレーションが、実行コンフィギュレーションから削除されています。 （注） オリジナルの **redistribute** コマンド コンフィギュレーションにルート マップが含まれていた場合は、この作業例の手順 3 にあるとおり、**route-map** コマンド コンフィギュレーションを必ず削除してください。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
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 モードを開始します。
ステップ 7	**show running-config** 例： `Device# show running-config`	（任意）ルータの現在の実行コンフィギュレーションを表示します。 • このコマンドは、ルータ コンフィギュレーションから、**redistribute** および **route-map** コマンドが削除されたことを確認するために使用します。

基本的な BGP のモニタリングとメンテナンス

ここでは、基本的な BGP プロセスとピア関係についての情報のリセットおよび表示に関する作業を説明します。BGP ネイバーになるように定義された 2 つのルータは、BGP 接続を形成し、ルーティング情報を交換します。その後、BGP フィルタ、重み、距離、バージョン、タイマーなどを変更したり、何らかのコンフィギュレーション変更を行ったりした場合、コンフィ

ギュレーションの変更を有効にするために、BGP 接続のリセットが必要になることがあります。

ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定

ルート リフレッシュ機能をサポートしていない BGP ピアに対して、**bgp soft-reconfig-backup** コマンドを使用してインバウンド ソフト再構成を設定するには、この作業を実行します。このコマンドを設定しても、ルート リフレッシュ機能をサポートしている BGP ピアは影響されません。インバウンド更新情報を格納するためのメモリ要件は非常に大きくなる可能性があることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **bgp soft-reconfig-backup**
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 を繰り返します。
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **set ip next-hop** *ip-address*
13. **end**
14. **show ip bgp neighbors** [*neighbor-address*]
15. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 45000`	
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングを有効にします。
ステップ 5	**bgp soft-reconfig-backup** 例： `Device(config-router)# bgp soft-reconfig-backup`	ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定します。 • このコマンドは、ルート リフレッシュ機能をサポートしていないピアに対して、インバウンドソフトウェア再構成を実行するように、BGP スピーカーを設定するために使用します。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**] 例： `Device(config-router)# neighbor 192.168.1.2 soft-reconfiguration inbound`	アップデートの格納を開始するように、シスコ ソフトウェアを設定します。 • このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。着信ソフト再設定が後で行われるときは、格納されている情報を使用して新しい着信アップデートのセットが生成されます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router)# neighbor 192.168.1.2 route-map LOCAL in`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、LOCAL という名前のルートマップが着信ルートに適用されます。
ステップ 9	インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 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 10	**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 11	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map LOCAL permit 10`	ルート マップを設定し、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。 • この例では、LOCAL という名前のルート マップが作成されます。
ステップ 12	**set ip next-hop** *ip-address* 例： `Device(config-route-map)# set ip next-hop 192.168.1.144`	ポリシー ルーティング用のルート マップの match 句を満たしたパケットの送出先を指定します。 • この例では、IP アドレスは 192.168.1.144 に設定されています。
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show ip bgp neighbors** [*neighbor-address*] 例： `Device# show ip bgp neighbors 192.168.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 15	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、BGP ネイバー 192.168.2.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされています。

```
BGP neighbor is 192.168.1.2,  remote AS 40000, external link
 Neighbor capabilities:
   Route refresh: advertised and received(new)
```

次に、BGP ネイバー 192.168.3.2 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされておらず、インバウンドポリシーアップデートを更新する方法が他にはないため、BGP ピア 192.168.3.2 の soft-reconfig inbound パスが保存されます。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Neighbor capabilities:
   Route refresh: advertised
```

次の **show ip bgp** コマンドの出力例には、ネットワーク 172.17.1.0 のエントリがあります。BGP ピアは両方とも 172.17.1.0/24 をアドバタイズしていますが、192.168.3.2 については、received-only パスだけが格納されます。

```
BGP routing table entry for 172.17.1.0/24, version 11
Paths: (3 available, best #3, table Default-IP-Routing-Table, RIB-failure(4))
Flag: 0x820
 Advertised to update-groups:
    1
 50000
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external
 50000, (received-only)
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 100, valid, external
 40000
   192.168.1.2 from 192.168.1.2 (172.16.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external, best
```

基本 BGP 情報のリセットと表示

基本 BGP プロセスとピア関係に関する情報をリセットおよび表示するには、この作業を実行します。

手順の概要

1. **enable**
2. **clear ip bgp** {***** | *autonomous-system-number* | *neighbor-address*} [**soft** [**in** | **out**]]
3. **show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]
4. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]
5. **show ip bgp paths**
6. **show ip bgp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip bgp** {* | *autonomous-system-number* | *neighbor-address*} [**soft** [**in** | **out**]] 例： `Device# clear ip bgp *`	BGP ネイバーセッションをクリアし、リセットします。 • この例では、BGP ネイバーセッションはすべてクリアされ、リセットされます。
ステップ 3	**show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*] 例： `Device# show ip bgp 10.1.1.0 255.255.255.0`	BGP ルーティング テーブル内のすべてのエントリを表示します。 • この例では、10.1.1.0 ネットワークの BGP ルーティング テーブル情報が表示されます。
ステップ 4	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*] 例： `Device# show ip bgp neighbors 192.168.3.2 advertised-routes`	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。 • この例では、デバイスから他のデバイスの BGP ネイバー 192.168.3.2 にアドバタイズされたルートが表示されます。
ステップ 5	**show ip bgp paths** 例： `Device# show ip bgp paths`	データベース内のすべての BGP パスに関する情報を表示します。
ステップ 6	**show ip bgp summary** 例： `Device# show ip bgp summary`	すべての BGP 接続のステータスに関する情報を表示します。

BGP を使用したルート プレフィックスの集約

BGP ピアは、ローカル ネットワークに関する情報を交換しますが、このために、BGP ルーティング テーブルはすぐに巨大になります。CIDR は、ルーティング テーブルのサイズを最小限に抑えるため、集約ルート（スーパーネット）の作成を可能にします。BGP ルーティング テーブルが小さければ小さいほど、ネットワークのコンバージェンス時間が短縮され、ネットワークのパフォーマンスが高まります。集約されたルートは、BGP を使用して、設定およびアドバ

タイズできます。集約の中には、サマリールートだけをアドバタイズするものもありますが、別の方法を使ってルートを集約すると、より具体的なルートが転送できるようになります。集約は、BGP ルーティング テーブルに存在するルートだけに適用されます。集約されたルートは、BGP ルーティング テーブルに具体的な集約ルートが少なくともあと 1 つ存在する場合に転送されます。BGP 内でルートを集約するには、次の作業のいずれかを行います。

BGP へのスタティック集約ルートの再配布

スタティック集約ルートを BPG に再配布するには、この作業を使用します。スタティック集約ルートは設定後、BGP ルーティング テーブルに再配布されます。スタティック ルートは、インターフェイス ヌル0 をポイントするように設定する必要があります。また、プレフィックスは、既知の BGP ルートのスーパーセットでなければなりません。BGP パケットを受信したデバイスは、より具体的な BGP ルートを使用します。BGP ルーティング テーブルにルートがない場合、パケットはヌル 0 に転送され、廃棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
4. **router bgp** *autonomous-system-number*
5. **redistribute static**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*] 例： `Device(config)# ip route 172.0.0.0 255.0.0.0 null 0`	スタティック ルートを作成します。

	コマンドまたはアクション	目的
ステップ 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute static** 例： `Device(config-router)# redistribute static`	BGP ルーティング テーブルにルートを再配布します。
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。

BGP を使用した条件付き集約ルートの設定

少なくとも 1 つのルートが指定された範囲に含まれる場合、この作業を使用して、BGP ルーティング テーブルに集約ルート エントリを作成します。集約ルートは、このユーザの自律システムから始まるものとしてアドバタイズされます。詳細については、「BGP ルート集約の AS_SET 情報生成」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **aggregate-address** *address mask* [**as-set**]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**aggregate-address** *address mask* [**as-set**] 例： `Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 as-set`	BGP ルーティング テーブルに集約エントリを作成します。 • 指定されたルートは、BGP テーブル内に存在する必要があります。 • 指定された範囲に含まれる、より詳しい BGP ルートがある場合は、キーワードを指定せずに **aggregate-address** コマンドを使用して、集約エントリを作成します。 • このルートについてアドバタイズされるパスが AS_SET であることを指定するには、**as-set** キーワードを使用します。このルートは、集約されたルートの到達可能性情報が変更されるたびに取り消され、アップデートされるため、多数のパスを集約するときには、**as-set** キーワードは使用しないでください。 （注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 5	**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。

BGP を使用した集約ルートのアドバタイズメントの抑制および抑制解除

集約ルートを作成し、BGP を使用してルートのアドバタイズメントを抑制して、その後、ルートのアドバタイズの抑制を解除するには、この作業を使用します。抑制されているルートはいかなるネイバーにもアドバタイズされませんが、特定のネイバーに対してすでに抑制されているルートの抑制を解除することはできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*

4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. 次のいずれかを実行します。
   - **aggregate-address** *address mask* [**summary-only**]
   - **aggregate-address** *address mask* [**suppress-map** *map-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。

ステップ 5	次のいずれかを実行します。
	• **aggregate-address** *address mask* [**summary-only**]
	• **aggregate-address** *address mask* [**suppress-map** *map-name*]
	例：
	`Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 summary-only`
	例：
	`Device(config-router)# aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1`
		集約ルートを作成します。
		• 集約ルート（たとえば、10.*.*.*）を作成し、すべてのネイバーに対するより具体的なルートのアドバタイズメントを抑制するには、オプションの **summary-only** キーワードを使用します。
		• 集約ルートを作成するが、指定されたルートのアドバタイズメントを抑制するには、オプションの **suppress-map** キーワードを使用します。抑制されたルートは、いかなるネイバーにもアドバタイズされません。ルートマップの **match** 句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートを抑制しないでおくことができます。IP アクセス リストと自律

	コマンドまたはアクション	目的
		システム パス アクセス リストの **match** 句がサポートされています。 （注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name* 例： `Device(config-router)# neighbor 192.168.1.2 unsuppress map1`	（任意）**aggregate-address** コマンドにより、すでに抑制されているルートを選択的にアドバタイズします。 • この例では、ステップ 5 ですでに抑制されているルートが、ネイバー 192.168.1.2 にアドバタイズされます。
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 モードを開始します。

BGP を使用した非アクティブなルート アドバタイズメントの抑制

BGPにより、非アクティブなルートのアドバタイズメントを抑制するには、この作業を実行します。Cisco IOS Release 12.2(25)S、12.2(33)SXH、および 15.0(1)M では、BGP ピアに非アクティブなルートをアドバタイズしないようにBGP を設定するための **bgp suppress-inactive** コマンドが導入されました。BGP ルーティング プロセスは、デフォルトで、RIB にインストールされていないルートを BGP ピアにアドバタイズできます。RIB にインストールされていないルートは非アクティブなルートです。非アクティブなルートのアドバタイズメントは、たとえば、共通のルート集約を通じてルートがアドバタイズされた場合に行われます。

非アクティブなルートのアドバタイズメントを抑制して、より整合性の取れたデータ フォワーディングを行うことができます。この機能は、IPv4 アドレス ファミリごとに設定できます。たとえば、**maximum routes** 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、VRF で設定できるルート数の最大値を指定するときに、この上限を超えた後、非アクティブなルートが VRF で使用されるのを防ぐために、このようなルートのアドバタイズメントを抑制することもできます。

始める前に

この作業は、BGP がイネーブルにされ、ピアリングが確立されていることを前提にしています。

（注） 非アクティブ ルートの抑制を設定できるのは、IPv4 アドレス ファミリ、またはデフォルトの IPv4 汎用セッションの下だけです。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **bgp suppress-inactive**
6. **end**
7. **show ip bgp rib-failure**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family** {**ipv4** [**mdt**	**multicast**	**unicast** [**vrf** *vrf-name*]	**vrf** *vrf-name*]	**vpnv4** [**unicast**]} 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ固有のコンフィギュレーションを使用するようにBGP ピアを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**bgp suppress-inactive** 例：	非アクティブなルートのBGPアドバタイジングを抑制します。

	コマンドまたはアクション	目的
	`Router(config-router-af)# bgp suppress-inactive`	• デフォルトの設定では、BGP は非アクティブなルートをアドバタイズします。 • 非アクティブルートのアドバタイズメントを再度有効にするには、このコマンドの **no** 形式を入力します。
ステップ 6	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 7	**show ip bgp rib-failure** 例： `Router# show ip bgp rib-failure`	（任意）RIB にインストールされていない BGP ルートを表示します。

例

次の例に示す **show ip bgp rib-failure** コマンドの出力には、RIB にインストールされていないルートが表示されています。この出力からは、表示されたルートがインストールされなかったのは、より都合のよいアドミニストレーティブ ディスタンスのルートがすでに RIB に存在していたからであることがわかります。

```
Router# show ip bgp rib-failure

Network           Next Hop                   RIB-failure   RIB-NH Matches
10.1.15.0/24      10.1.35.5          Higher admin distance             n/a
10.1.16.0/24      10.1.15.1          Higher admin distance             n/a
```

BGP ルートの条件付きアドバタイズ

選択した BGP ルートを条件付きでアドバタイズするには、この作業を実行します。条件付きでアドバタイズされるルートまたはプレフィックスは、アドバタイズマップと存在マップまたは非存在マップの 2 つのルート マップで定義されます。存在マップまたは不在マップと関連付けられているルート マップは、BGP スピーカーが追跡するプレフィックスを指定します。アドバタイズ マップと関連付けられているルート マップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィックスを指定します。

- プレフィックスが存在マップにあることが BGP スピーカーにより判明した場合、アドバタイズ マップで指定されたプレフィックスがアドバタイズされます。
- プレフィックスが非存在マップにないことが BGP スピーカーにより判明した場合、アドバタイズ マップで指定されたプレフィックスがアドバタイズされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティング テーブルに存在する必要があります。これらのルートは、アクセス リストから、または IP プレフィックス リストから参照されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
8. **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...*]}
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
11. **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...*]}
12. **exit**
13. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
14. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
15. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} 例： `Device(config-router)# neighbor 192.168.1.2 advertise-map map1 exist-map map2`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、存在マップ（map2 という名前付きルート マップ）の ACL と一致するプレフィックス（192.168.50.0）がローカル BGP テーブルにある場合に限り、アドバタイズマップ（map1 という名前付きルート マップ）の ACL と一致するプレフィックス（172.17.0.0）がネイバーにアドバタイズされます。
ステップ 6	**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 7	**route-map** *map-tag* [**permit** | **deny**] [**sequence-number**] 例： `Device(config)# route-map map1 permit 10`	ルート マップを設定し、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。 • この例では、map1 という名前のルート マップが作成されます。
ステップ 8	**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...*]} 例： `Device(config-route-map)# match ip address 1`	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 リストにより許可されているプレフィックスと一致するルート マップを作成します。 • この例では、ルート マップは、アクセス リスト 1 で許可されているプレフィックスとマッチングされます。
ステップ 9	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例：	ルート マップを設定し、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
	`Device(config)# route-map map2 permit 10`	• この例では、map2 という名前のルートマップが作成されます。
ステップ 11	**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...*]} 例： `Device(config-route-map)# match ip address 2`	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 リストにより許可されているプレフィックスと一致するルート マップを作成します。 • この例では、ルート マップは、アクセス リスト 2 で許可されているプレフィックスとマッチングされます。
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 モードを終了して、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 13	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 1 permit 172.17.0.0`	標準アクセス リストを設定します。 • この例では、アクセス リスト 1 で、**neighbor advertise-map** コマンドによって設定された他の条件に応じて、172.17.0.0 プレフィックスのアドバタイズが許可されます。
ステップ 14	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 2 permit 192.168.50.0`	標準アクセス リストを設定します。 • この例では、192.168.50.0 が exist-map のプレフィックスになるように、アクセス リスト 2 が認可を与えます。
ステップ 15	**exit** 例： `Device(config)# exit`	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。

BGP ルートの開始

ルート集約は BGP テーブルのサイズを最小化するには便利ですが、BGP テーブルに特定のプレフィックスを追加する必要が生じることがあります。ルート集約では、特定のプレフィックスをさらに非表示にすることができます。「BGP ルーティング プロセスの設定」の項で示されている **network** コマンドを使用して、ルートを開始し、次のオプション作業によってさまざまな状況に対応した BGP テーブルへの BGP ルートを開始します。

BGP を使用したデフォルト ルートのアドバタイジング

BGP ピアへのデフォルト ルートをアドバタイズするには、次の作業を実行します。デフォルト ルートはローカルに開始されます。デフォルト ルートは、コンフィギュレーションを簡素化する場合やデバイスでシステム リソースが過剰に使用されないようにする場合に便利です。デバイスがインターネット サービス プロバイダー（ISP）のピアである場合、ISP は完全なルーティング テーブルを持っているため、ISP ネットワークへのデフォルト ルートを設定しておくと、ローカル デバイスのリソースが節約されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length* | **permit** *network / length*} [**ge** *ge-value*] [**le** *le-value*]
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **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...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*	**permit** *network / length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list DEFAULT permit 10.1.1.0/24`	IP プレフィックス リストを設定します。 • この例では、プレフィックス リスト DEFAULT は、**match ip address** コマンドによって設定されたマッチングに応じて、10.1.1.0/24 プレフィックスのアドバタイズを許可します。
ステップ 4	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] 例：	ルート マップを設定し、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
	`Device(config)# route-map ROUTE`	• この例では、ROUTE という名前のルート マップが作成されます。
ステップ 5	**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...*]} 例： `Device(config-route-map)# match ip address prefix-list DEFAULT`	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により許可されているプレフィックスと一致するルートマップを作成します。 • この例では、ルートマップは、プレフィックス リスト DEFAULT で許可されているプレフィックスとマッチングされます。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 7	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] 例： `Device(config-router)# neighbor 192.168.3.2 default-originate`	（任意）デフォルト ルートとして使用するために、BGP スピーカー（ローカルデバイス）がデフォルト ルート 0.0.0.0 をピアに送信することを許可します。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードを開始します。

トラブルシューティングのヒント

デフォルト ルートが設定されていることを確認するには、ローカル ルータではなく受信側BGP ピアで **show ip route** コマンドを使用します。この出力で、次に類似した行にデフォルト ルート 0.0.0.0 が表示されていることを確認します。

```
B*   0.0.0.0/0 [20/0] via 192.168.1.2, 00:03:10
```

BGP ルートの条件付き挿入

標準のルート集約を通じて選択された具体性にかけるプレフィックスではなく、より具体的なプレフィックスを BGP ルーティング テーブルに挿入するには、この作業を実行します。より

具体的なプレフィックスを使用すると、集約されたルートを使う場合よりも、よりきめ細かなトラフィック エンジニアリングや管理制御を行うことができます。詳細については、「条件付き BGP ルートの挿入」の項を参照してください。

始める前に

この作業は、BGP ピアに対して、IGP がすでに設定されていることを前提にしています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**]
5. **exit**
6. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
7. **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...*]}
8. **match ip route-source** {*access-list-number* | *access-list-name*} [*access-list-number...*| *access-list-name...*]
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
11. **set 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...*]}
12. **set community** {*community-number* [**additive**] [*well-known-community*] | **none**}
13. **exit**
14. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
15. 作成される各プレフィックス リストについて、ステップ 14 を繰り返します。
16. **exit**
17. **show ip bgp injected-paths**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**] 例： `Router(config-router)# bgp inject-map ORIGINATE exist-map LEARNED_PATH`	条件付きルート挿入のために、挿入マップと存在マップを指定します。 • 挿入したルートが集約ルートの属性を継承することを指定するには、**copy-attributes** キーワードを使用します。
ステップ 5	**exit** 例： `Router(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 6	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map LEARNED_PATH permit 10`	ルート マップを設定し、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 7	**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...*]} 例： `Router(config-route-map)# match ip address prefix-list SOURCE`	より具体的なルートの挿入先となる集約ルートを指定します。 • この例では、ルートのソースの再配布に、プレフィックス リスト SOURCE が使用されています。
ステップ 8	**match ip route-source** {*access-list-number* | *access-list-name*} [*access-list-number...*| *access-list-name...*] 例： `Router(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE`	ルートのソースを再配布するための一致条件を指定します。 • この例では、ルートのソースの再配布に、プレフィックス リスト ROUTE_SOURCE が使用されています。 （注） ルート ソースは、**neighbor remote-as** コマンドで設定されたネイバー アドレスです。条件付きルート挿入が行われるようにするには、トラッキングされるプレフィックスはこのネイバーから来たものでなければなりません。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map ORIGINATE permit 10`	ルート マップを設定し、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 11	**set 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...*]} 例： `Router(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES`	挿入されるルートを指定します。 • この例では、ルートのソースの再配布に、プレフィックス リスト originated_routes が使用されています。
ステップ 12	**set community** {*community-number* [**additive**] [*well-known-community*] | **none**} 例： `Router(config-route-map)# set community 14616:555 additive`	挿入されたルートの BGP コミュニティ属性を設定します。
ステップ 13	**exit** 例： `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 14	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Router(config)# ip prefix-list SOURCE permit 10.1.1.0/24`	プレフィックス リストを設定します。 • この例では、プレフィックス リスト SOURCE は、ネットワーク 10.1.1.0/24 からのルートを許可するように設定されています。
ステップ 15	作成される各プレフィックス リストについて、ステップ 14 を繰り返します。	--
ステップ 16	**exit** 例： `Router(config)# exit`	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 17	**show ip bgp injected-paths** 例： `Router# show ip bgp injected-paths`	（任意）挿入されたパスに関する情報を表示します。

例

次の出力例は、**show ip bgp injected-paths** コマンドを入力したときに表示される出力に類似しています。

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                               0 ?
*> 172.17.0.0/16    10.0.0.2                               0 ?
```

トラブルシューティングのヒント

BGP 条件付きルート挿入は、あまり具体的ではないプレフィックスがある場合に行われる、BGP ルーティング テーブルへのより具体的なプレフィックスの挿入に基づいています。条件付きルート挿入が適切に行われない場合は、次の点を確認してください。

- 条件付きルート挿入は設定されているが、行われないという場合は、BGP ルーティング テーブルに集約プレフィックスが存在することを確認します。BGP ルーティング テーブルにトラッキングされたプレフィックスが存在するかしないかは、**show ip bgp** コマンドで確認できます。
- 集約プレフィックスは存在するが、条件付きルート挿入は行われないという場合は、集約プレフィックスが正しいネイバーから来ていること、およびこのネイバーを識別するプレフィックス リストが /32 一致であることを確認します。
- **show ip bgp injected-paths** コマンドを使用して、より具体的なプレフィックスが挿入されたかどうかを確認します。
- 挿入されるプレフィックスが、集約プレフィックスの範囲から外れていないことを確認します。
- 挿入ルート マップが、**match ip address** コマンドではなく、**set ip address** コマンドを使用して設定されていることを確認します。

バックドア ルートを使用した BGP ルートの開始

バックドア ルートを使用して到達可能なネットワークを示すには、この作業を実行します。バックドア ネットワークはローカル ネットワークと同様に扱われますが、アドバタイズされません。詳細については、「BGP バックドア ルート」の項を参照してください。

始める前に

この作業は、BGP ピアに対して、IGP（この例では EIGRP）がすでに設定されていることを前提にしています。この設定は「BGP バックドア ルート」の項にあるのルータ B で行われます。また、BGP ピアはルータ D です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **network** *ip-address* **backdoor**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 172.22.1.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスのマルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ピアに指定されている自律システム番号はステップ 3 で指定された番号と同じであるため、このピアは内部ピアです。

	コマンドまたはアクション	目的
ステップ 5	**network** *ip-address* **backdoor** 例： `Device(config-router)# network 172.21.1.0 backdoor`	バックドア ルートを通じて到達可能なネットワークを示します。
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。

BGP ピア グループの設定

この作業では、BGP ピア グループの設定方法を説明します。BGP スピーカーでは、多数のネイバーが同じアップデート ポリシー（つまり、同じアウトバウンド ルート マップ、配布リスト、フィルタ リスト、アップデート ソースなど）を使って設定されていることがよくあります。同じアップデート ポリシーを持つネイバーは、コンフィギュレーションを簡素化するため、またさらに重要なことには、アップデートをより効率化するために、ピア グループにグループ化されます。多数のピアがある場合、このアプローチを強く推奨します。

次の作業で説明されている、BGP ピア グループを設定するための 3 つの手順は次のとおりです。

- ピア グループを作成する
- ピア グループへオプションに割り当てる
- ピア グループのメンバをネイバーにする

neighbor shutdown ルータ コンフィギュレーション コマンドを使用して、コンフィギュレーション情報を削除せずに、BGP ピア、またはピア グループを削除することができます。

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*

6. **neighbor** *ip-address* **peer-group** *peer-group-name*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **neighbor** *peer-group-name* **activate**
9. **neighbor** *ip-address* **peer-group** *peer-group-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router)# neighbor fingroup peer-group`	BGP ピア グループを作成します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスのマルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 7	**address-family ipv4** [**unicast**	**multicast**	**vrf** *vrf-name*] 例：	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-router)# address-family ipv4 multicast`	• **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。これがデフォルトです。 • キーワード **multicast** は、IPv4 マルチキャスト アドレス プレフィックスが交換されることを表します。 • **vrf** キーワードおよび *vrf-name* 引数は、IPv4 VRF インスタンス情報が交換されることを示します。
ステップ 8	**neighbor** *peer-group-name* **activate** 例： `Device(config-router-af)# neighbor fingroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。 （注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、ユニキャストアドレスプレフィックスだけを交換します。この例で設定しているマルチキャストなど、その他のアドレスプレフィックスタイプを BGP が交換できるようにするには、**neighbor activate** コマンドを使用してネイバーをアクティブ化することも必要です。
ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 peer-group fingroup`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ピア セッション テンプレートの設定

次に説明する作業では、ピア セッション テンプレートを作成し、設定します。

基本的なピア セッション テンプレートの設定

一般的な BGP ルーティング セッション コマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピア セッション テンプレートを作成するには、この作業を実行します。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている一般的なセッション コマンドのいずれとでも置き換えが可能です。

（注） ピア セッション テンプレートには、次の制約事項が適用されます。

- ピアセッションテンプレートが直接継承できるセッションテンプレートは1つだけです。また、継承されたセッション テンプレートはそれぞれ、間接継承されたセッション テンプレートを1つ含むことができます。したがって、ネイバー、またはネイバー グループの設定には、直接適用されたピア セッション テンプレートを 1 個だけと、間接継承されたピア セッション テンプレートを 7 個使用できます。
- BGP ネイバーを、ピア グループとピア テンプレートの両方と連動するようには設定できません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートだけからポリシーを継承するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **remote-as** *autonomous-system-number*
6. **timers** *keepalive-interval hold-time*
7. **end**
8. **show ip bgp template peer-session** [*session-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* 例： `Router(config-router)# template peer-session INTERNAL-BGP`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**remote-as** *autonomous-system-number* 例： `Router(config-router-stmp)# remote-as 202`	（任意）指定された自律システムでリモート ネイバーとのピアリングを設定します。 （注） ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 6	**timers** *keepalive-interval hold-time* 例： `Router(config-router-stmp)# timers 30 300`	（任意）BGP キープアライブとホールドタイマーを設定します。 • ホールドタイムは、少なくともキープアライブ タイムの 2 倍の長さが必要です。 （注） ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 7	**end** 例： `Router(config-router)# end`	セッション テンプレート 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 bgp template peer-session** [*session-template-name*] 例： `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、この

	コマンドまたはアクション	目的
		コマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定

この作業は、**inherit peer-session** コマンドを使用して、ピア セッション テンプレートの継承を設定します。これは、ピア セッション テンプレートを作成、設定し、別のピア セッション テンプレートからコンフィギュレーションを継承できるようにします。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている一般的なセッション コマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **description** *text-string*
6. **update-source** *interface-type interface-number*
7. **inherit peer-session** *session-template-name*
8. **end**
9. **show ip bgp template peer-session** [*session-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* 例： `Router(config-router)# template peer-session CORE1`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**description** *text-string* 例： `Router(config-router-stmp)# description CORE-123`	（任意）説明を設定します。 • text-string には最大 80 文字を使用できます。 （注） ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 6	**update-source** *interface-type interface-number* 例： `Router(config-router-stmp)# update-source loopback 1`	（任意）ルーティング テーブル アップデートを受信するための特定のソース、またはインターフェイスを選択するようにルータを設定します。 • この例では、ループバック インターフェイスを使用します。このコンフィギュレーションの利点は、ループバック インターフェイスはフラッピング インターフェイスの効果の影響を受けにくいところにあります。 （注） ここでは、サポートされている一般セッション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 7	**inherit peer-session** *session-template-name* 例： `Router(config-router-stmp)# inherit peer-session INTERNAL-BGP`	別のピア セッション テンプレートのコンフィギュレーションを継承するように、このピア セッション テンプレートを設定します。 • この例では、INTERNAL-BGP からコンフィギュレーションを継承するようにピア セッション テンプレートを設定しています。このテンプレートはネイバーに適用可能で、コンフィギュレーション INTERNAL-BGP は間接的に適用さ

	コマンドまたはアクション	目的
		れます。その他のピア セッション テンプレートは直接適用できません。ただし、直接継承されたテンプレートは最高 7 個の間接継承されたピア セッション テンプレートを持つことができます。
ステップ 8	**end** 例： `Router(config-router)# end`	セッション テンプレート 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。
ステップ 9	**show ip bgp template peer-session** [*session-template-name*] 例： `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • オプションの *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

neighbor inherit peer-session コマンドを使用したピア セッション テンプレートの継承の設定

この作業では、**neighbor inherit peer-session** コマンドを使用して、ピア セッション テンプレートをネイバーに送信し、指定されたピア セッション テンプレートからコンフィギュレーションを継承させるようにルータを設定します。次の手順に従って、ピア セッション テンプレート コンフィギュレーションをネイバーに送信し、継承させます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **inherit peer-session** *session-template-name*
6. **end**
7. **show ip bgp template peer-session** [*session-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 172.16.0.1 remote-as 202`	指定されたネイバーを使ってピアリング セッションを設定します。 • 手順 5 の neighbor inherit 文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、手順 5 で指定されたネイバーはセッション テンプレートを受け付けません。
ステップ 5	**neighbor** *ip-address* **inherit peer-session** *session-template-name* 例： `Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1`	ネイバーがコンフィギュレーションを継承できるように、このネイバーにピア セッション テンプレートを送信します。 • この例では、ピア セッション テンプレート CORE1 を 172.16.0.1 ネイバーに送信し、継承させるようにルータを設定しています。このテンプレートはネイバーに適用できます。また、別のピア セッション テンプレートが CORE1 で間接継承された場合、間接継承されたコンフィギュレーションも適用されます。その他のピア セッション テンプレートは直接適用できません。ただし、直接継承されたテンプレートも、さらに最高 7 個の間接継承されたピア セッション テンプレートを継承することができます。
ステップ 6	**end** 例： `Router(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。

	コマンドまたはアクション	目的
ステップ 7	**show ip bgp template peer-session** [*session-template-name*] 例： `Router# show ip bgp template peer-session`	ローカルに設定されたピア セッション テンプレートを表示します。 • オプションの *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア ポリシー テンプレートを作成する方法については、ピア ポリシー テンプレートの設定（157 ページ）を参照してください。

ピア ポリシー テンプレートの設定

基本的なピア ポリシー テンプレートの設定

BGP ポリシー コンフィギュレーション コマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピア ポリシー テンプレートを作成するには、この作業を実行します。

（注） ステップ 5 ～ 7 のコマンドは任意で、サポートされている BGP ポリシー コンフィギュレーション コマンドのいずれとでも置き換えが可能です。

（注） ピア ポリシー テンプレートには、次の制約事項が適用されます。

- ピア ポリシー テンプレートは、直接的、または間接的に、最高 8 個のピア ポリシー テンプレートを継承できます。
- BGP ネイバーを、ピア グループとピア テンプレートの両方と連動するようには設定できません。BGP ネイバーは、1 つのピア グループだけに属するように設定するか、またはピア テンプレートだけからポリシーを継承するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*

5. **maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval* | **warning-only**]
6. **weight** *weight-value*
7. **prefix-list** *prefix-list-name* {**in** | **out**}
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Device(config-router)# template peer-policy GLOBAL`	ポリシーテンプレート コンフィギュレーションモードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval*	**warning-only**] 例： `Device(config-router-ptmp)# maximum-prefix 10000`	（任意）このピアがネイバーから受け入れるプレフィックスの最大数を設定します。 （注） ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピア ポリシー テンプレート」の項を参照してください。
ステップ 6	**weight** *weight-value* 例： `Device(config-router-ptmp)# weight 300`	（任意）このネイバーから送信されるルートのデフォルトの重みを設定します。 （注） ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピア ポリシー テンプレート」の項を参照してください。

	コマンドまたはアクション	目的
ステップ 7	**prefix-list** *prefix-list-name* {**in** | **out**} 例： `Device(config-router-ptmp)# prefix-list NO-MARKETING in`	（任意）ルータにより受信、またはルータから送信されるプレフィックスをフィルタします。 • この例のプレフィックスリストは、インバウンド内部アドレスをフィルタします。 （注） ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピア ポリシー テンプレート」の項を参照してください。
ステップ 8	**end** 例： `Device(config-router-ptmp)# end`	ポリシーテンプレート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。

次の作業

ピア ポリシー テンプレートの作成後、ピア ポリシー テンプレートのコンフィギュレーションを、別のピア ポリシー テンプレートに継承、または適用することができます。ピア ポリシーの継承の詳細については、「inherit peer-policy コマンドを使用したピア ポリシーテンプレートの継承の設定」の項または「neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定」の項を参照してください。

inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業は、**inherit peer-policy** コマンドを使用して、ピア ポリシー テンプレートの継承を設定します。これは、ピア ポリシー テンプレートを作成、設定し、別のピア ポリシー テンプレートからコンフィギュレーションを継承できるようにします。

BGP ネイバーが継承したピア テンプレートを使用する場合、特定のテンプレートに関連付けられているポリシーを判断するのが難しいことがあります。Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースでは、**show ip bgp template peer-policy** コマンドに、特定のテンプレートに関連付けられているローカル ポリシーおよび継承されたポリシーの詳しいコンフィギュレーションを表示するためのキーワード **detail** が追加されました。

（注） ステップ 5 と 6 のコマンドは任意で、サポートされている BGP ポリシー コンフィギュレーション コマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **route-map** *map-name* {**in**| **out**}
6. **inherit peer-policy** *policy-template-name* *sequence-number*
7. **end**
8. **show ip bgp template peer-policy** [*policy-template-name*[**detail**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Router(config-router)# template peer-policy NETWORK1`	ポリシーテンプレートコンフィギュレーションモードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**route-map** *map-name* {**in**| **out**} 例： `Router(config-router-ptmp)# route-map ROUTE in`	（任意）指定されたルート マップをインバウンド ルート、またはアウトバウンド ルートに適用します。 （注） ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。サポートされているコマンドのリストについては、ピア ポリシー テンプレート （97 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 6	**inherit peer-policy** *policy-template-name sequence-number* 例： `Router(config-router-ptmp)# inherit peer-policy GLOBAL 10`	別のピア ポリシーテンプレートのコンフィギュレーションを継承するように、このピア ポリシー テンプレートを設定します。 • *sequence-number* 引数は、ピア ポリシー テンプレートの評価順序を設定します。ルートマップのシーケンス番号と同様、最も小さいシーケンス番号が最初に評価されます。 • この例では、GLOBAL からコンフィギュレーションを継承するようにピア ポリシー テンプレートを設定しています。これらの手順で作成されたテンプレートをネイバーに適用すると、コンフィギュレーション GLOBAL も間接的に継承され、適用されます。GLOBAL からはさらに最高 6 個のピア ポリシー テンプレートが間接継承され、合計 8 個のピア ポリシー テンプレートが直接適用、および間接継承されます。 • 他のテンプレートで、これより小さいシーケンス番号が設定されていなければ、この例のこのテンプレートが最初に評価されます。
ステップ 7	**end** 例： `Router(config-router-ptmp)# end`	ポリシーテンプレート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 bgp template peer-policy** [*policy-template-name*[**detail**]] 例： `Router# show ip bgp template peer-policy NETWORK1 detail`	ローカルに設定されたピア ポリシー テンプレートを表示します。 • *policy-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。 • 詳細なポリシー情報を表示するには、**detail** キーワードを使用します。 （注） **detail** キーワードがサポートされているのは、Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースだけです。

例

次の例は、**show ip bgp template peer-policy** コマンドに **detail** キーワードを付けた場合の出力で、NETWORK1 というポリシーの詳細が表示されています。この例の出力からは、GLOBAL テンプレートが継承されたことがわかります。ルートマップおよびプレフィックス リスト コンフィギュレーションの詳細も表示されています。

```
Router# show ip bgp template peer-policy NETWORK1 detail
Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
 Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
   seq 5 permit 10.1.1.0/24
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
   seq 5 deny 10.2.2.0/24
```

neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業では、**neighbor inherit peer-policy** コマンドを使用して、ピア ポリシー テンプレートをネイバーに送信し、継承させるようにルータを設定します。次の手順に従って、ピア ポリシー テンプレート コンフィギュレーションをネイバーに送信し、継承させます。

BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースでは、指定されたネイバーで継承されたポリシーと、直接設定されたポリシーを表示するためのキーワード **policy** と **detail** が **show ip bgp neighbors** コマンドに追加されました。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*

7. **end**
8. **show ip bgp neighbors** [*ip-address*[**policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定されたネイバーを使ってピアリング セッションを設定します。 • 手順 6 の **neighbor inherit** 文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、手順 6 で指定されたネイバーはセッション テンプレートを受け付けません。
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ固有のコマンド コンフィギュレーションを使用するようにネイバーを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例： `Router(config-router-af)# neighbor 192.168.1.2 inherit peer-policy GLOBAL`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。 • この例では、ピア ポリシー テンプレート GLOBAL を 192.168.1.2 ネイバーに送信し、継承させるようにルータを設定しています。このテンプレートはネイバーに適用できます。また、別のピア ポリシー テンプレートが GLOBAL から間接継承された場合、間接継承されたコンフィギュレーションも適用されます。GLOBAL からは、さらに最高 7 個のピア ポリシー テンプレートを間接継承できます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show ip bgp neighbors** [*ip-address*[**policy** [**detail**]]] 例： `Router# show ip bgp neighbors 192.168.1.2 policy`	ローカルに設定されたピア ポリシー テンプレートを表示します。 • *policy-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。 • このネイバーに適用されているポリシーをアドレス ファミリごとに表示するには、**policy** キーワードを使用します。 • 詳細なポリシー情報を表示するには、**detail** キーワードを使用します。 • **policy** および **detail** キーワードがサポートされているのは、Cisco IOS Release 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB、およびそれ以降のリリースだけです。 （注） この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力例に表示されているのは、192.168.1.2 にあるネイバーに適用されたポリシーです。この出力には、継承されたポリシーと、このネイバーデバイスで設定されたポリシーの両方が表示されています。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。

```
Router# show ip bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

BGP ダイナミック アップデート グループのモニタリングとメンテナンス

ダイナミック BGP アップデート グループの処理に関する情報の表示およびクリアには、この作業を使用します。BGP アップデート グループを使用すると、BGP アップデート メッセージ生成のパフォーマンスが向上します。BGP ピア テンプレートが設定され、ダイナミック BGP アップデート ピア グループがサポートされたことにより、ネットワーク オペレータはBGP でピア グループを設定する必要がなくなります。また、コンフィギュレーションの柔軟性とシステム パフォーマンスの向上による恩恵を受けます。BGP ピア テンプレートの使用については、「ピア セッション テンプレートの設定」の項および「ピア ポリシー テンプレートの設定」の項を参照してください。

手順の概要

1. **enable**
2. **clear ip bgp update-group** [*index-group* | *ip-address*]
3. **show ip bgp replication** [*index-group* | *ip-address*]
4. **show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip bgp update-group** [*index-group*	*ip-address*] 例： `Device# clear ip bgp update-group 192.168.2.2`	BGP アップデート グループ メンバーシップをクリアし、BGPアップデートグループを再計算します。 • この例では、ネイバー 192.168.2.2 のメンバーシップは、アップデートグループからクリアされます。
ステップ 3	**show ip bgp replication** [*index-group*	*ip-address*] 例： `Device# show ip bgp replication`	BGPアップデートグループのアップデートのレプリケーション統計情報を表示します。
ステップ 4	**show ip bgp update-group** [*index-group*	*ip-address*] [**summary**] 例： `Device# show ip bgp update-group`	BGP アップデート グループの情報を表示します。

トラブルシューティングのヒント

BGP アップデート グループの処理に関する情報を表示するには、**debug ip bgp groups** コマンドを使用します。すべてのアップデート グループ、個々のアップデート グループ、または特定の BGP ネイバーに関する情報を表示できます。このコマンドからは非常に詳しい情報が表示されます。問題のトラブルシューティングを行う場合を除き、運用中のネットワークでは、このコマンドを使用しないでください。

基本 BGP ネットワークの設定例

例：BGP プロセスの設定とピアのカスタマイズ

次の例は、上の（「BGP ピアのカスタマイズ」の項）に示されている異なる自律システムにある 2 つのネイバー ピア（ルータ A のピアとルータ E のピア）を使って BGP プロセスが設定されているルータ B のコンフィギュレーションを示しています。IPv4 ユニキャスト ルートは両方のピアと交換され、IPv4 マルチキャスト ルートはルータ E の BGP ピアと交換されます。

ルータ B

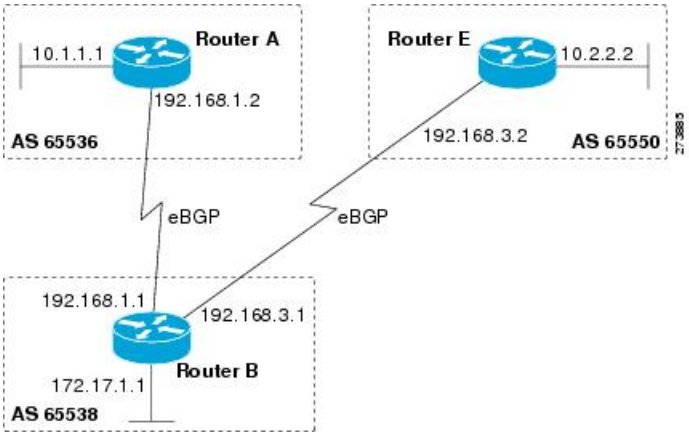
```
router bgp 45000
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 !
 address-family ipv4 multicast
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 advertisement-interval 25
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定

asplain 形式

次に示すのは、下の図におけるボーダー ゲートウェイ プロトコル（BGP）プロセスを使ったルータ A、B、E のコンフィギュレーションの例で、このプロセスは、asplain 表記法を使用して設定された別々の 4 バイト自律システムのルータ A、B、E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 *14 : asplain* 形式の *4* バイト自律システム番号を使用する *BGP* ピア



ルータ A

```
router bgp 65536
 bgp router-id 10.1.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 65538
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 65536
```

```
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

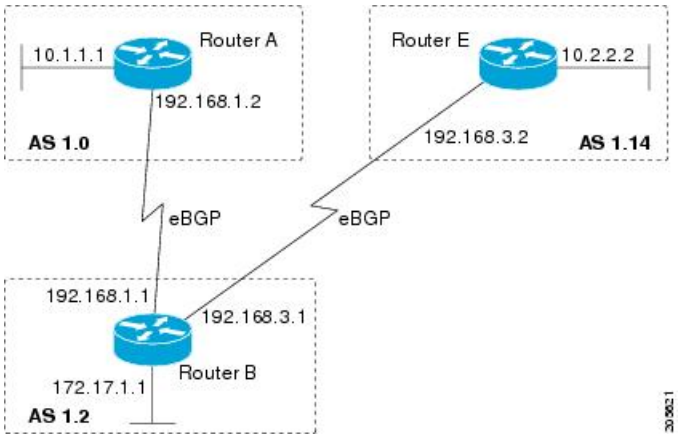
ルータ E

```
router bgp 65550
 bgp router-id 10.2.2.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

asdot 形式

次に示すのは、下の図における BGP プロセスを使ったルータ A、B、E のコンフィギュレーションを作成する方法の例で、このプロセスは、デフォルトの asdot 形式を使用して設定された別々の 4 バイト自律システムのルータ A、B、E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 *15 : asdot* 形式の *4* バイト自律システム番号を使用する *BGP* ピア



ルータ A

```
router bgp 1.0
 bgp router-id 10.1.1.99
```

```
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 1.2
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ E

```
router bgp 1.14
 bgp router-id 10.2.2.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

例：4バイトのBGP自律システム番号を使用したVRFおよび拡張コミュニティの設定

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次の例は、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースで使用可能です。この例は、4 バイト自律システム番号 65537 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルートマップにより許可されたルートの拡張コミュニティ値 65537:100 を設定する方法を示しています。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 65537:100
 exit
route-map red_map permit 10
 set extcommunity rt 65537:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 65537 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map
route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

4 バイト自律システム番号の RD サポート

次の例は、4 バイト AS 番号 65536 を含むルート識別子、および 4 バイト自律システム番号 65537 を含むルート ターゲットを使用して、VRF を作成する方法を示しています。

```
ip vrf vpn_red
 rd 65536:100
 route-target both 65537:100
 exit
```

コンフィギュレーションの完了後、**show vrf** コマンドを使用して、4 バイト AS 番号ルート識別子が 65536:100 に設定されていることを確認します。

```
RouterB# show vrf vpn_red
Current configuration : 36 bytes
vrf definition x
 rd 65536:100
!
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次の例は、Cisco IOS Release 12.0(32)S12 および 12.4(24)T で使用可能です。この例は、4 バイト自律システム番号 1.1 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルート マップにより許可されたルートの拡張コミュニティ値 1.1:100 を設定する方法を示しています。

（注） Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースでは、この例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して、asdot をデフォルトの表示形式として設定した場合だけです。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 1.1:100
 exit
route-map red_map permit 10
 set extcommunity rt 1.1:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 1.1 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map
route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:1.1:100
  Policy routing matches: 0 packets, 0 bytes
```

4 バイト自律システム番号の RD サポートの asdot デフォルト形式

次の例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して asdot をデフォルトの表示形式として設定した場合です。

```
ip vrf vpn_red
 rd 1.0:100
 route-target both 1.1:100
 exit
```

例：NLRI から AFI へのコンフィギュレーション

次の例は、既存のルータ コンフィギュレーション ファイルを NLRI 形式から AFI 形式にアップグレードし、AFI 形式のコマンドだけを使用するようにルータの CLI を設定します。

```
router bgp 60000
 bgp upgrade-cli
```

既存のルータ コンフィギュレーション ファイルが NLRI 形式から AFI 形式にアップグレードされていることを確認するには、特権 EXEC モードで **show running-config** コマンドを使用し

ます。以下の各項では、NLRI 形式のルータ コンフィギュレーション ファイルからの出力例と、ルータ コンフィギュレーション モードで **bgp upgrade-cli** コマンドを使って、このファイルを AFI 形式にアップグレードした後の出力例を示します。

（注） **bgp upgrade-cli** コマンドを使って、AFI 形式から NLRI 形式にルータをアップグレードすると、NLRI コマンドを使用したり、設定したりできなくなります。

アップグレード前の NLRI 形式のルータ コンフィギュレーション ファイル

次に示すのは、特権 EXEC モードでの **show running-config** コマンドからの出力例です。この出力例には、**bgp upgrade-cli** コマンドを使って AFI 形式にアップグレードする前のルータ コンフィギュレーション ファイルが NLRI 形式で表示されています。この出力例は、ルータ コンフィギュレーションのうち、影響を受ける部分だけが表示されるようにフィルタ処理されています。

```
Router# show running-config | begin bgp

router bgp 101
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 505 nlri unicast multicast
 no auto-summary
!
ip default-gateway 10.4.9.1
ip classless
!
!
route-map REDISTRIBUTE-MULTICAST permit 10
 match ip address prefix-list MULTICAST-PREFIXES
 set nlri multicast
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
 match ip address prefix-list UNICAST-PREFIXES
 set nlri unicast
!
!
!
line con 0
line aux 0
line vty 0 4
 password PASSWORD
 login
!
end
```

アップグレード後の AFI 形式のルータ コンフィギュレーション ファイル

次に示すのは、AFI 形式にアップグレードした後のルータ コンフィギュレーション ファイルの出力例です。この出力例は、ルータ コンフィギュレーション ファイルのうち、影響を受ける部分だけが表示されるようにフィルタ処理されています。

```
Router# show running-config | begin bgp

router bgp 101
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 505
 no auto-summary
 !
 address-family ipv4 multicast
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family ipv4
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
!
ip default-gateway 10.4.9.1
ip classless
!
!
route-map REDISTRIBUTE-MULTICAST_mcast permit 10
 match ip address prefix-list MULTICAST-PREFIXES
!
route-map REDISTRIBUTE-MULTICAST permit 10
 match ip address prefix-list MULTICAST-PREFIXES
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
 match ip address prefix-list UNICAST-PREFIXES
!
!
!
line con 0
line aux 0
line vty 0 4
 password PASSWORD
 login
!
end
```

例：再配布の例を使用した BGP コンフィギュレーション コマンドの削除

次の例は、ルート マップを使用して EIGRP への BGP ルートの再配布を有効にする CLI コンフィギュレーションと、再配布とルート マップを削除する CLI コンフィギュレーションを示しています。BGP コンフィギュレーション コマンドの中には、他の CLI コマンドに影響を与えるものもありますが、この例は、あるコマンドの削除が他のコマンドにどのような影響を与えるかを示しています。

1 つ目のコンフィギュレーション例では、ルートマップは、自律システム番号をマッチングおよび設定するように設定されています。3つの異なる自律システムにあるBGPネイバーが設定およびアクティブ化されます。EIGRP ルーティング プロセスが開始され、ルート マップを使用して、EIGRP への BGP ルートの再配布が設定されます。

EIGRP への BGP ルート再配布を有効にする CLI

```
route-map bgp-to-eigrp permit 10
 match tag 50000
 set tag 65000
 exit
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4
  neighbor 172.16.1.2 remote-as 45000
  neighbor 172.21.1.2 remote-as 45000
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.3.2 remote-as 50000
  neighbor 172.16.1.2 activate
  neighbor 172.21.1.2 activate
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 exit
router eigrp 100
 redistribute bgp 45000 metric 10000 100 255 1 1500 route-map bgp-to-eigrp
 no auto-summary
 exit
```

2 つ目のコンフィギュレーション例では、**route-map** コマンドと **redistribute** コマンドの両方が無効になっています。route-map コマンドだけを削除した場合、再配布が自動的に無効になることはありません。再配布は行われますが、マッチングやフィルタリングは行われません。再配布コンフィギュレーションを削除するには、**redistribute** コマンドも無効にする必要があります。

EIGRP への BGP ルート再配布を削除する CLI

```
configure terminal
 no route-map bgp-to-eigrp
 router eigrp 100
  no redistribute bgp 45000
  end
```

例：BGP ソフト リセット

次の例は、BGP ピア 192.168.1.1 の接続をリセットする 2 通りの方法を示しています。

例：ダイナミック インバウンド ソフト リセット

次に、BGP ピア 192.168.1.1 でダイナミック ソフト再構成を開始するコマンドの例を示します。このコマンドを使用するには、ピアでルート リフレッシュ機能がサポートされている必要があります。

```
clear ip bgp 192.168.1.1 soft in
```

例：格納された情報を使用したインバウンド ソフト リセット

次の例では、ネイバー 192.168.1.1 に対してインバウンド ソフト再構成を有効にする方法を示しています。このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。インバウンドソフトウェア再構成を後で行う場合、格納された情報を使用して、新たに一連のインバウンド アップデートが生成されます。

```
router bgp 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 soft-reconfiguration inbound
```

次の例では、ネイバー 192.168.1.1 のセッションがクリアされます。

```
clear ip bgp 192.168.1.1 soft in
```

例：4 バイト自律システム番号を使用した BGP ピアのリセット

次の例は、4バイト自律システム番号を使用する自律システムに属するBGPピアをクリアする方法を示しています。BGP ルーティング テーブルの初期状態が、**show ip bgp** コマンドを使用して示されています。また、4 バイトの自律システム 65536 と 65550 にあるピアも表示されます。

```
RouterB# show ip bgp

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

4 バイトの自律システム 65550 にある BGP ピアをすべて削除するために、**clear ip bgp 65550** コマンドが実行されます。ADJCHANGE メッセージからは、192.168.3.2 にある BGP ピアがリセットされていることがわかります。

```
RouterB# clear ip bgp 65550
RouterB#
*Nov 30 23:25:27.043: %BGP-5-ADJCHANGE: neighbor 192.168.3.2 Down User reset
```

もう一度、**show ip bgp** コマンドが実行されますが、今度は 4 バイトの自律システム 65536 内のピアだけが表示されます。

```
RouterB# show ip bgp

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

その直後、次の ADJCHANGE メッセージが表示され、4 バイトの自律システム 65550 で、192.168.3.2 の BGP ピアが稼働状態になったことが示されます。

```
RouterB#
*Nov 30 23:25:55.995: %BGP-5-ADJCHANGE: neighbor 192.168.3.2 Up
```

例：基本 BGP 情報のリセットおよび表示

次に、基本 BGP 情報をリセットおよび表示する例を示します。

clear ip bgp * コマンドは BGP ネイバー セッションをすべてクリアし、リセットします。Cisco IOS Release 12.2(25)S 以降の構文では **clear ip bgp all** です。特定のネイバーをクリアするには *neighbor-address* 引数、自律システムにあるすべてのピアをクリアするには *autonomous-system-number* 引数を使用します。引数が指定されていない場合、このコマンドは BGP ネイバー セッションをすべてクリアし、リセットします。

（注） また、**clear ip bgp *** コマンドは内部 BGP 構造をすべてクリアするため、トラブルシューティング ツールとして便利です。

```
Router# clear ip bgp *
```

show ip bgp コマンドは、BGP ルーティング テーブルのすべてのエントリを表示するために使用します。次に、10.1.1.0 ネットワークの BGP ルーティング テーブル情報を表示する例を示します。

```
Router# show ip bgp 10.1.1.0 255.255.255.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1
  40000
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

show ip bgp neighbors コマンドは、TCP および BGP 接続に関する情報をネイバーに表示するために使用します。次の例は、上の図（「IPv4 VRF アドレス ファミリ用に BGP ピアを設定」の項）のルータ B から、ルータ E にある BGP ネイバー 192.168.3.2 にアドバタイズされるルートを示しています。

```
Router# show ip bgp neighbors 192.168.3.2 advertised-routes

BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
Total number of prefixes 2
```

show ip bgp paths コマンドは、データベース内のすべての BGP パスを表示するために使用します。次に、上の図（「BGP ピアのカスタマイズ」の項）のルータ B に対する BGP パス情報を表示する例を示します。

```
Router# show ip bgp paths

Address    Hash Refcount Metric Path
0x2FB5DB0     0        5      0 i
0x2FB5C90     1        4      0 i
0x2FB5C00  1361        2      0 50000 i
0x2FB5D20  2625        2      0 40000 i
```

show ip bgp summary コマンドは、すべての BGP 接続のステータスを表示するために使用します。次に、上の図（「BGP ピアのカスタマイズ」の項）のルータ B に対する BGP ルーティング テーブル情報を表示する例を示します。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 45000
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 882 total bytes of memory
BGP activity 14/10 prefixes, 16/12 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.2     4 40000     667     672        3    0    0 00:03:49        1
192.168.3.2     4 50000     468     467        0    0    0 00:03:49 (NoNeg)
```

例：BGP を使用したプレフィックスの集約

次の例は、集約ルートを BGP に再配布するか、または BGP 条件付き集約ルーティング機能を使用することにより、BGP で集約ルートを使用する方法を示します。

次の例では、**redistribute static** ルータ コンフィギュレーション コマンドを使用して、集約ルート 10.0.0.0 が再配布されます。

```
ip route 10.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

次のコンフィギュレーションは、少なくとも 1 つのルートが指定された範囲に含まれる場合に、BGP ルーティング テーブルに集約エントリを作成する方法を示します。自律システムから受け取られるに従って、集約ルートはアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、atomic aggregate 属性が設定されています（デフォルトでは、**aggregate-address** ルータ コンフィギュレーション コマンドで **as-set** キーワードを使用しない限り、atomic aggregate は設定されています）。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0
```

次の例は、直前の例と同じルールを使用して集約エントリを作成する方法を示していますが、このルートでアドバタイズされるパスは、要約されているパスすべてに含まれるすべての要素から構成される AS_SET です。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 as-set
```

次の例は、10.0.0.0 に対する集約ルートを作成しながら、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する方法を示します。

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

次の例は、非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# bgp suppress-inactive
Device(config-router-af)# end
```

次の例は、RED という名前の VRF でルートの上限を設定し、RED という名前の VRF 経由で非アクティブなルートをアドバタイズしないように BGP を設定します。

```
Device(config)# ip vrf RED
Device(config-vrf)# rd 50000:10
Device(config-vrf)# maximum routes 1000 10
Device(config-vrf)# exit
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 vrf RED
Device(config-router-af)# bgp suppress-inactive
Device(config-router-af)# end
```

例：BGP ピア グループの設定

次の例は、アドレス ファミリを使用して、ピア グループのすべてのメンバがユニキャストとマルチキャストの両方に対応できるようにピア グループを設定する方法を示しています。

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 unicast
  neighbor mygroup peer-group
  neighbor 192.168.1.2 peer-group mygroup
  neighbor 192.168.3.2 peer-group mygroup
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 multicast
  neighbor mygroup peer-group
  neighbor 192.168.1.2 peer-group mygroup
  neighbor 192.168.3.2 peer-group mygroup
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
```

例：ピア セッション テンプレートの設定

次の例は、セッション テンプレート コンフィギュレーション モードで、INTERNAL-BGP という名前のピア セッション テンプレートを作成します。

```
router bgp 45000
 template peer-session INTERNAL-BGP
 remote-as 50000
 timers 30 300
 exit-peer-session
```

次の例は、ピア セッション テンプレート CORE1 を作成します。この例は、INTERNAL-BGP というピア セッション テンプレートのコンフィギュレーションを継承します。

```
router bgp 45000
 template peer-session CORE1
 description CORE-123
 update-source loopback 1
 inherit peer-session INTERNAL-BGP
 exit-peer-session
```

次の例は、CORE1 ピア セッション テンプレートを継承するように、192.168.3.2 ネイバーを設定します。192.168.3.2 ネイバーも、ピア セッション テンプレート INTERNAL-BGP から間接的にコンフィギュレーションを継承します。neighbor inherit 文を動作させるには、**remote-as** 文を明示的に使用する必要があります。ピアリングが設定されていない場合、指定されたネイバーはセッション テンプレートを受け付けません。

```
router bgp 45000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 inherit peer-session CORE1
```

例：ピア ポリシー テンプレートの設定

次の例は、GLOBAL という名前のピア ポリシー テンプレートを作成し、ポリシー テンプレート コンフィギュレーション モードを開始します。

```
router bgp 45000
 template peer-policy GLOBAL
  weight 1000
  maximum-prefix 5000
  prefix-list NO_SALES in
  exit-peer-policy
```

次の例は、PRIMARY-IN という名前のピア ポリシー テンプレートを作成し、ポリシー テンプレート コンフィギュレーション モードを開始します。

```
router bgp 45000
 template peer-policy PRIMARY-IN
  prefix-list ALLOW-PRIMARY-A in
  route-map SET-LOCAL in
  weight 2345
  default-originate
  exit-peer-policy
```

次の例は、ピア ポリシー テンプレート CUSTOMER-A を作成します。このピア ポリシー テンプレートは、PRIMARY-IN および GLOBAL という名前のピア ポリシー テンプレートからコンフィギュレーションを継承するように設定されています。

```
router bgp 45000
 template peer-policy CUSTOMER-A
  route-map SET-COMMUNITY in
  filter-list 20 in
  inherit peer-policy PRIMARY-IN 20
  inherit peer-policy GLOBAL 10
  exit-peer-policy
```

次の例は、アドレス ファミリ モードでピア ポリシー テンプレート CUSTOMER-A を継承するように 192.168.2.2 ネイバーを設定します。この例は上の例の続きと仮定しており、上のピア ポリシー テンプレート CUSTOMER-A は PRIMARY-IN および GLOBAL という名前のテンプレートからコンフィギュレーションを継承しているため、192.168.2.2 ネイバーもピア ポリシー テンプレート PRIMARY-IN および GLOBAL から間接的に継承します。

```
router bgp 45000
 neighbor 192.168.2.2 remote-as 50000
 address-family ipv4 unicast
  neighbor 192.168.2.2 inherit peer-policy CUSTOMER-A
  end
```

例：BGP ダイナミック アップデート ピア グループのモニタリングおよびメンテナンス

ピア グループの BGP ダイナミック アップデート グループを有効にするための設定は必要ありません。アルゴリズムは自動的に実行されます。次の例は、BGP アップデート グループ情報をクリアまたは表示する方法を示しています。

clear ip bgp update-group の例

次の例は、アップデート グループから、ネイバー 10.0.0.1 のメンバーシップをクリアします。

```
Router# clear ip bgp update-group 10.0.0.1
```

debug ip bgp groups の例

次に示す **debug ip bgp groups** コマンドからの出力例では、**clear ip bgp groups** コマンドの実行後に、アップデート グループが再計算されていることがわかります。

```
Router# debug ip bgp groups

5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.5 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.5 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.8 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.8 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.21 flags 0x0 cap 0x0 and updgrp 1 f0
```

```
5w4d: BGP-DYN(0): Update-group 1 flags 0x0 cap 0x0 policies same as 10.4.9.21 f0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Up
```

show ip bgp replication の例

次の **show ip bgp replication** コマンドからの出力例には、すべてのネイバーに関するアップデート グループ レプリケーション情報が表示されます。

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
```

show ip bgp update-group の例

次の **show ip bgp update-group** コマンドからの出力例には、すべてのネイバーに関するアップデート グループ情報が表示されます。

```
Router# show ip bgp update-group

BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
  10.4.9.5 10.4.9.8
```

次の作業

- 外部サービス プロバイダーに接続する場合は、「外部 BGP を使用したサービス プロバイダーとの接続」モジュールを参照してください。
- BGP ネイバー セッション オプションを設定する場合は、「BGP ネイバー セッション オプションの設定」モジュールに進んでください。
- iBGP 機能を設定する場合は、「内部 BGP 機能の設定」モジュールを参照してください。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『Cisco IOS IPv6 Command Reference』
Cisco BGP のコンセプト情報の概要と各 BGP モジュールへのリンク	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「Cisco BGP 概要」モジュール
IPv4 VRF アドレス ファミリを使ったマルチプロトコル ラベル スイッチング（MPLS）および BGP コンフィギュレーションの例	『*MPLS: Layer 3 VPNs Inter-AS and CSC Configuration Guide*』の「MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels」モジュール

標準

標準	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB のリンク
CISCO-BGP4-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

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』

RFC	タイトル
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4893	『*BGP Support for Four-octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 BGP ネットワーク設定の機能情報

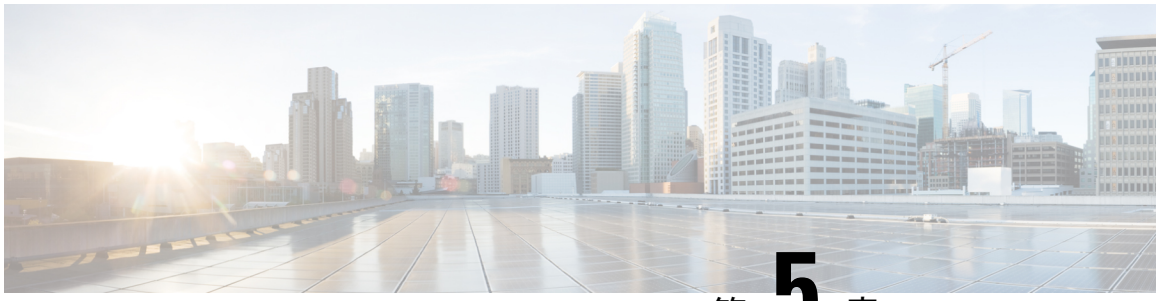
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *13*：基本 *BGP* ネットワーク設定の機能情報

機能名	リリース	機能の設定情報
BGP 条件付きルートインジェクション	12.0(22)S 12.2(4)T 12.2(14)S 15.0(1)S Cisco IOS XE 3.1.0SG	BGP 条件付きルート挿入機能を使用すると、通常のルート集約を通じて選択されたあまり具体的ではないプレフィックスよりも、より具体的なプレフィックスを BGP ルーティング テーブルに挿入することができます。より具体的なプレフィックスを使用すると、集約されたルートを使う場合よりも、よりきめ細かなトラフィック エンジニアリングや管理制御を行うことができます。
ピア テンプレートを使用した BGP 設定	12.0(24)S 12.2(18)S 12.2(27)SBC 12.3(4)T 15.0(1)S	ピア テンプレートを使用した BGP コンフィギュレーション機能により、ポリシーを共有する BGP ネイバーに対して、ネイバー コンフィギュレーションをグループ化する新しいメカニズムが導入されます。このタイプのポリシー コンフィギュレーションは、伝統的に BGP ピア グループを使って設定されています。ただし、ピア グループ コンフィギュレーションは、アップデート グループと特定セッションの特性に左右されるため、ピア グループには何らかの制限があります。コンフィギュレーション テンプレートはピア グループ コンフィギュレーションに代わるものを提供し、ピア グループの制約の一部を解決します。

機能名	リリース	機能の設定情報
BGP ダイナミック アップデート ピア グループ	12.0(24)S 12.2(18)S 12.2(27)SBC 12.3(4)T 15.0(1)S Cisco IOS XE 3.1.0SG	BGP ダイナミック アップデート ピア グループ機能により、同じアウトバウンド ポリシーを共有し、同じアップデート メッセージを共有できるネイバーのアップデート グループをダイナミックに計算し、最適化する新しいアルゴリズムが導入されます。Cisco IOS ソフトウェアの古いバージョンでは、BGP アップデート メッセージは、ピア グループ コンフィギュレーションに基づいてグループ化されていました。このグループ化の方法により、限定されたアウトバウンド ポリシーと特定のセッション コンフィギュレーションがアップデートされます。BGP ダイナミック アップデート ピア グループ機能では、アップデート グループ レプリケーションはピア グループ コンフィギュレーションから分離されるため、ネイバー コンフィギュレーションのコンバージェンス時間が短縮され、柔軟性が高まります。
BGP ハイブリッド CLI	12.0(22)S 12.2(15)T 15.0(1)S	BGP ハイブリッド CLI 機能は、BGP ネットワークと既存のコンフィギュレーションの NLRI 形式から AFI 形式への移行を簡素化します。この新しい機能により、ネットワーク オペレータは、AFI 形式でコマンドを設定し、この設定を既存の NLRI 形式の設定に保存することができます。この機能により、ネットワーク オペレータは、新しい機能を活用し、NLRI 形式から AFI 形式への移行をサポートできるようになります。
非アクティブなルートに対する BGP アドバタイズメントの抑制	12.2(25)S 12.2(33)SXH 15.0(1)M 15.0(1)S	非アクティブなルートに対する BGP アドバタイズメントの抑制機能では、ルーティング情報ベース（RIB）にインストールされていないルートに対するアドバタイズメントが行われないように設定できます。この機能を設定すると、ボーダー ゲートウェイ プロトコル（BGP）の更新と、トラフィックの転送に使用されるデータとの整合性がより高まります。



第 5 章

BGP 4 ソフト構成

BGP4 ソフト構成では、BGP セッションをクリアせずに BGP4 ポリシーを設定およびアクティブ化できるため、転送キャッシュを無効にする必要がありません。

- 機能情報の確認 （187 ページ）
- BGP 4 ソフト構成に関する情報 （187 ページ）
- BGP 4 ソフト構成の設定方法 （188 ページ）
- BGP 4 ソフト構成の設定例 （192 ページ）
- その他の参考資料 （193 ページ）
- BGP 4 ソフト構成の機能情報 （193 ページ）

機能情報の確認

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

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

BGP 4 ソフト構成に関する情報

BGP セッションのリセット

設定変更のためにルーティング ポリシーに変更が生じた場合は、必ず **clear ip bgp** コマンドを使用して、BGP ピアリング セッションをリセットする必要があります。シスコ ソフトウェア

は、BGP ピアリング セッションのリセットとして、次の 3 つのメカニズムをサポートしています。

- ハード リセット：ハード リセットは、TCP 接続を含む指定されたピアリング セッションを終了し、指定されたピアから到着したルートを削除します。
- ソフト リセット：ソフト リセットは、保存されたプレフィックス情報を使用し、既存のピアリング セッションを廃棄せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しいBGPポリシーを適用することができます。ソフト再構成は、インバウンドセッション、またはアウトバウンド セッションに対して設定できます。
- ダイナミック インバウンド ソフト リセット：これは RFC 2918 に定義されているルート リフレッシュ機能で、サポートしているピアへのルート リフレッシュ要求を交換することにより、ローカル デバイスがインバウンド ルーティング テーブルを動的にリセットできるようにするものです。ルート リフレッシュ機能は、中断を伴わないポリシー変更についてはアップデート情報をローカルに保存しません。その代わり、サポートしているピアとの動的な交換に依存します。ルート リフレッシュは、最初にピア間のBGP機能ネゴシエーションを通じてアドバタイズされる必要があります。すべての BGP デバイスが、ルート リフレッシュ機能をサポートしていなければなりません。BGP デバイスがこの機能をサポートしているかどうかを確認するには、**show ip bgp neighbors** コマンドを使用します。デバイスがルート リフレッシュ機能をサポートしている場合、次のメッセージが出力されます。

```
Received route refresh capability from peer.
```

bgp soft-reconfig-backup コマンドは、ルート リフレッシュ機能をサポートしていないピアに対してインバウンド ソフト再構成を実行するように BGP を設定するために導入されました。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。

BGP 4 ソフト構成の設定方法

ルート リフレッシュ機能が失われたときのインバウンド ソフト再構成を設定

ルート リフレッシュ機能をサポートしていない BGP ピアに対して、**bgp soft-reconfig-backup** コマンドを使用してインバウンド ソフト再構成を設定するには、この作業を実行します。このコマンドを設定しても、ルート リフレッシュ機能をサポートしている BGP ピアは影響されません。インバウンド更新情報を格納するためのメモリ要件は非常に大きくなる可能性があることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **bgp soft-reconfig-backup**
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 を繰り返します。
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **set ip next-hop** *ip-address*
13. **end**
14. **show ip bgp neighbors** [*neighbor-address*]
15. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングを有効にします。
ステップ 5	**bgp soft-reconfig-backup** 例： `Device(config-router)# bgp soft-reconfig-backup`	ルート リフレッシュ機能をサポートしていないピアに対して、インバウンド ソフトウェア再構成を実行するように、BGP スピーカーを設定します。

	コマンドまたはアクション	目的
		• このコマンドは、ルート リフレッシュ機能をサポートしていないピアに対して、インバウンドソフトウェア再構成を実行するように、BGP スピーカーを設定するために使用します。このコマンドの設定により、必要な場合にだけ、アップデート（ソフト再構成）を格納するように、BGP を設定することができます。このコマンドを設定しても、ルート リフレッシュ機能をサポートしているピアは影響されません。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**] 例： `Device(config-router)# neighbor 192.168.1.2 soft-reconfiguration inbound`	アップデートの格納を開始するように、シスコ ソフトウェアを設定します。 • このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。着信ソフト再設定が後で行われるときは、格納されている情報を使用して新しい着信アップデートのセットが生成されます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router)# neighbor 192.168.1.2 route-map LOCAL in`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、LOCAL という名前のルートマップが着信ルートに適用されます。
ステップ 9	インバウンド ソフト再構成を使用して設定される各ピアについて、手順 6 ～ 8 を繰り返します。	-
ステップ 10	**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 11	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map LOCAL permit 10`	ルート マップを設定し、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。 • この例では、LOCAL という名前のルートマップが作成されます。

	コマンドまたはアクション	目的
ステップ 12	**set ip next-hop** *ip-address* 例： `Device(config-route-map)# set ip next-hop 192.168.1.144`	ポリシー ルーティング用のルート マップの match 句を満たしたパケットの送出先を指定します。 • この例では、IP アドレスは 192.168.1.144 に設定されています。
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show ip bgp neighbors** [*neighbor-address*] 例： `Device# show ip bgp neighbors 192.168.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 15	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、BGP ネイバー 192.168.2.1 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされています。

```
BGP neighbor is 192.168.1.2,  remote AS 40000, external link
 Neighbor capabilities:
   Route refresh: advertised and received(new)
```

次に、BGP ネイバー 192.168.3.2 への TCP および BGP 接続に関する情報を表示する **show ip bgp neighbors** コマンドの出力例の一部を示します。このピアでは、ルート リフレッシュがサポートされておらず、インバウンド ポリシー アップデートを更新する方法が他にはないため、BGP ピア 192.168.3.2 の soft-reconfig inbound パスが保存されます。

```
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Neighbor capabilities:
   Route refresh: advertised
```

次の **show ip bgp** コマンドの出力例には、ネットワーク 172.17.1.0 のエントリがあります。BGP ピアは両方とも 172.17.1.0/24 をアドバタイズしていますが、192.168.3.2 については、received-only パスだけが格納されます。

```
BGP routing table entry for 172.17.1.0/24, version 11
Paths: (3 available, best #3, table Default-IP-Routing-Table, RIB-failure(4))
Flag: 0x820
 Advertised to update-groups:
    1
 50000
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external
 50000, (received-only)
   192.168.3.2 from 192.168.3.2 (172.17.1.0)
     Origin incomplete, metric 0, localpref 100, valid, external
 40000
   192.168.1.2 from 192.168.1.2 (172.16.1.0)
     Origin incomplete, metric 0, localpref 200, valid, external, best
```

BGP 4 ソフト構成の設定例

例：BGP ソフト リセット

次の例は、BGP ピア 192.168.1.1 の接続をリセットする 2 通りの方法を示しています。

例：ダイナミック インバウンド ソフト リセット

次に、BGP ピア 192.168.1.1 でダイナミック ソフト再構成を開始するコマンドの例を示します。このコマンドを使用するには、ピアでルート リフレッシュ機能がサポートされている必要があります。

```
clear ip bgp 192.168.1.1 soft in
```

例：格納された情報を使用したインバウンド ソフト リセット

次の例では、ネイバー 192.168.1.1 に対してインバウンド ソフト再構成を有効にする方法を示しています。このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。インバウンドソフトウェア再構成を後で行う場合、格納された情報を使用して、新たに一連のインバウンド アップデートが生成されます。

```
router bgp 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 soft-reconfiguration inbound
```

次の例では、ネイバー 192.168.1.1 のセッションがクリアされます。

```
clear ip bgp 192.168.1.1 soft in
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

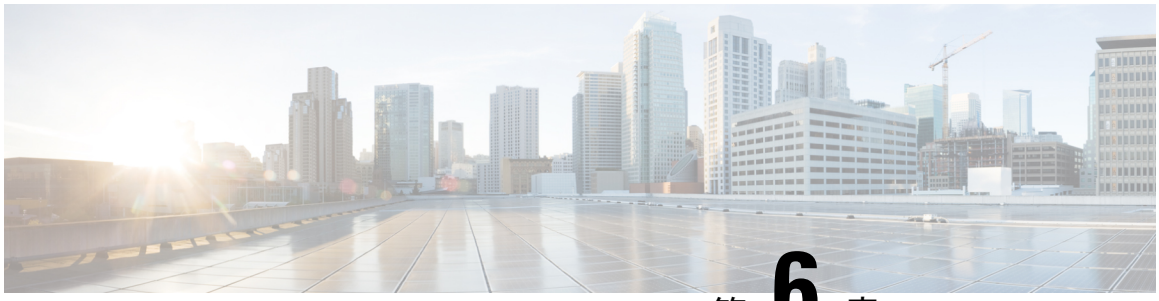
BGP 4 ソフト構成の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *14 : BGP 4* ソフト構成の機能情報

機能名	リリース	機能情報
BGP 4 ソフト構成		BGP 4 ソフト構成では、BGP セッションをクリアせずに BGP4 ポリシーを設定およびアクティブ化できるため、転送キャッシュを無効にする必要がありません。



第 6 章

4 バイト ASN に対する BGP サポート

シスコが採用している 4 バイト自律システム（AS）番号は、AS 番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用しています。ただし、RFC 5396 に記載されているとおり、4 バイト AS 番号を asplain 形式および asdot 形式の両方で設定できます。また、4 バイト自律番号に対する 4 バイトの ASN ルート識別子（RD）およびルート ターゲット（RT）の BGP のサポートが追加されています。

- 機能情報の確認 （195 ページ）
- 4 バイト ASN に対する BGP サポートに関する情報 （196 ページ）
- 4 バイト ASN に対する BGP サポートの設定方法 （199 ページ）
- 4 バイト ASN に対する BGP サポートの設定例 （207 ページ）
- 4 バイト ASN に対する BGP サポートに関する追加情報 （211 ページ）
- 4 バイト ASN に対する BGP サポートの機能情報 （212 ページ）

機能情報の確認

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

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

4 バイト ASN に対する BGP サポートに関する情報

BGP 自律システム番号の形式

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム（AS）番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。現在は、AS 番号の需要増加に伴い、Internet Assigned Numbers Authority（IANA）によって割り当てられる AS 番号は 65536 ～ 4294967295 の範囲の 4 オクテットの番号になりました。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、AS 番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト AS 番号をその 10 進数値で表します。たとえば、65526 は 2 バイト AS 番号、234567 は 4 バイト AS 番号になります。
- asdot：自律システム ドット付き表記。2 バイト AS 番号は 10 進数で、4 バイト AS 番号はドット付き表記で表されます。たとえば、65526 は 2 バイト AS 番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト AS 番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

asdot だけを使用する自律システム番号形式

Cisco IOS XE Release 2.3 では、4 オクテット（4 バイト）の AS 番号は asdot 表記法だけで入力および表示されます。たとえば、1.10 または 45000.64000 です。4 バイト AS 番号のマッチングに正規表現を使用する場合、asdot 形式には正規表現で特殊文字となるピリオドが含まれていることに注意します。正規表現でのマッチングに失敗しないよう、（1\.14 のように）ピリオドの前にバックスラッシュを入力する必要があります。次の表は、asdot 形式だけが使用できる Cisco IOS イメージで、2 バイトおよび 4 バイト AS 番号の設定、正規表現とのマッチング、および **show** コマンド出力での表示に使用される形式をまとめたものです。

表 *15 : asdot* だけを使用する *4* バイト *AS* 番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

asplain をデフォルトとする AS 番号形式

Cisco IOS XE Release 2.4 およびそれ以降のリリースでは、シスコ実装の 4 バイト AS 番号で asplain がデフォルトの AS 番号表示形式として使用されていますが、4 バイト AS 番号は asplain および asdot 形式のどちらにも設定できます。また、正規表現で 4 バイト AS 番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト AS 番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力を変更

して、4 バイトの自律システム番号を asdot 形式で表示する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式が有効にされている場合、正規表現の 4 バイト AS 番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト AS 番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト AS 番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。**show** コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト AS 番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドを有効にした後、**clear ip bgp *** コマンドを入力してすべての BGP セッションに対してハード リセットを開始する必要があります。

（注） 4 バイト AS 番号をサポートしているイメージにアップグレードしている場合でも、2 バイト AS 番号を使用できます。4 バイト AS 番号に設定された形式にかかわらず、2 バイト AS の **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

表 *16 : asplain* をデフォルトとする *4* バイト *AS* 番号形式

書式	設定形式	**show** コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295

表 *17 : asdot* を使用する *4* バイト *AS* 番号形式

書式	設定形式	**show**コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

予約済みおよびプライベートの AS 番号

Cisco IOS XE Release 2.3 およびそれ以降のリリースでは、シスコ実装の BGP は、RFC 4893 をサポートします。RFC 4893 は、2 バイト AS 番号から 4 バイト AS 番号への段階的移行を BGP がサポートできるように開発されました。新しい予約済み（プライベート）AS 番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を AS 番号として設定できません。

RFC 5398『*Autonomous System (AS) Number Reservation for Documentation Use*』では、文書化を目的として新たに予約された AS 番号について説明されています。予約済み番号を使用することで、設定例を正確に文書化しつつ、その設定がそのままコピーされた場合でも製品ネットワークに競合が発生することを防止できます。予約済み番号は IANA AS 番号レジストリに記載されています。予約済み 2 バイト AS 番号は 64496 ～ 64511 の連続したブロック、予約済み 4 バイト AS 番号は 65536 ～ 65551 をその範囲としています。

64512 ～ 65534 を範囲とするプライベートの 2 バイト AS 番号は依然有効で、65535 は特殊な目的のために予約されています。プライベート AS 番号は内部ルーティング ドメインで使用できますが、インターネットにルーティングされるトラフィックについては変換が必要です。プライベート AS 番号を外部ネットワークへアドバタイズするように BGP を設定しないでください。Cisco IOS ソフトウェアは、デフォルトではルーティング アップデートからプライベート AS 番号を削除しません。ISP がプライベート AS 番号をフィルタ処理することを推奨します。

（注） パブリック ネットワークおよびプライベート ネットワークに対する AS 番号の割り当ては、IANA が管理しています。予約済み番号の割り当てや AS 番号の登録申込など、AS 番号に関する情報については、http://www.iana.org/ を参照してください。

シスコが採用している 4 バイト自律システム番号

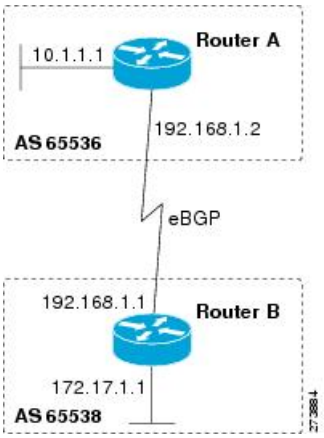
Cisco IOS XE Release 2.4 およびそれ以降のリリースでは、シスコが採用している 4 バイト自律システム（AS）番号は、AS 番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト AS 番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト AS 番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドの後に **clear ip bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。4 バイト AS 番号形式の詳細については、「BGP 自律システム番号の形式」の項を参照してください。

Cisco IOS XE Release 2.3 では、シスコが採用している 4 バイト AS 番号は、設定形式、正規表現とのマッチング、および出力表示として、asdot（たとえば、1.2）だけを使用しています。asplain はサポートしていません。4 バイト番号を使用する 2 つの自律システム内の BGP ピアの例については、下の図を参照してください。asdot 表記法を使用して設定された、異なる 4 バイトの自律システムにある 3 つのネイバー ピアの間での設定例については、「例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定」を参照してください。

シスコは、BGP が 2 バイト AS 番号から 4 バイト AS 番号へ段階的に移行できるように開発された RFC 4893 もサポートしています。スムーズな移行を確実に行うには、4 バイト AS 番号を使用して識別される AS 内の BGP スピーカーをすべて、4 バイト AS 番号をサポートするようにアップグレードすることを推奨します。

（注） 新しいプライベート AS 番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を AS 番号として設定できません。

図 *16 : 4* バイト番号を使用する *2* つの自律システム内の *BGP* ピア



4 バイト ASN に対する BGP サポートの設定方法

BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定

4 バイト自律システム（AS）番号を使用する AS にボーダー ゲートウェイ プロトコル（BGP）ピアが配置されているときに、BGP ルーティング プロセスおよび BGP ピアを設定するには、この作業を実行します。ここで設定するアドレス ファミリは、デフォルトの IPv4 ユニキャスト アドレス ファミリで、設定は上の図（「シスコが採用している 4 バイト自律システム番号」の項）のルータ A で行われています。この作業にある 4 バイト AS 番号は、デフォルトの asplain（10 進数値）形式にフォーマットされています。たとえば、上の図にあるルータ B の AS 番号は 65538 です。BGP ピアとなりうるネイバー ルータすべてについて、必ず、この作業を実行してください。

始める前に

（注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. 必要に応じて、手順 4 を繰り返し、その他の BGP ネイバーを定義します。
6. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
7. **neighbor** *ip-address* **activate**
8. 必要に応じて、手順 7 を繰り返し、その他の BGP ネイバーをアクティブ化します。
9. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
10. **end**
11. **show ip bgp** [*network*] [*network-mask*]
12. **show ip bgp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 65538`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 65536`	指定された AS のネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、4 バイト AS 番号 65536 は asplain 表記法で定義されています。
ステップ 5	必要に応じて、手順 4 を繰り返し、その他の BGP ネイバーを定義します。	--
ステップ 6	**address-family ipv4** [**unicast**	**multicast**	**vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4

	コマンドまたはアクション	目的
		ユニキャストアドレスファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.2 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 8	必要に応じて、手順 7 を繰り返し、その他の BGP ネイバーをアクティブ化します。	--
ステップ 9	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この AS にローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp 10.1.1.0`	（任意）BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 12	**show ip bgp summary** 例：	（任意）BGP 接続すべての状況を表示します。

	コマンドまたはアクション	目的
	Device# show ip bgp summary	

例

次の例は、上の図のルータ B で実行された **show ip bgp** コマンドの出力ですが、ここにはルータ A で 192.168.1.2 にある BGP ネイバーから学習されたネットワーク 10.1.1.0 に対する BGP ルーティング テーブル エントリと、デフォルトの asplain 形式で表した 4 バイト AS 番号 65536 が表示されています。

```
RouterB# show ip bgp 10.1.1.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1)
  Advertised to update-groups:
     2
  65536
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

次の例は、**show ip bgp summary** コマンドの出力ですが、ここには、上の図のルータ B でこの作業を設定した後で、ルータ A にある BGP ネイバー 192.168.1.2 の 4 バイト AS 番号が 65536 であることが表示されています。

```
RouterB# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
3/2 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 806 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  Stated
192.168.1.2     4        65536       6       6        3    0    0 00:01:33       1
```

トラブルシューティングのヒント

BGPデバイス間の基本的なネットワーク接続性を確認するには、**ping** コマンドを使用します。

4 バイト自律システム番号で使用される出力および正規表現とのマッチング形式のデフォルトを変更

4 バイト自律システム（AS）番号のデフォルト出力形式を asplain 形式から asdot 表記法形式に変更するには、この作業を実行します。4 バイト AS 番号の出力形式の変化を表示するには、**show ip bgp summary** コマンドを使用します。

手順の概要

1. **enable**
2. **show ip bgp summary**
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **bgp asnotation dot**
6. **end**
7. **clear ip bgp ***
8. **show ip bgp summary**
9. **show ip bgp regexp** *regexp*
10. **configure terminal**
11. **router bgp** *autonomous-system-number*
12. **no bgp asnotation dot**
13. **end**
14. **clear ip bgp ***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp summary** 例： `Device# show ip bgp summary`	すべてのボーダーゲートウェイ プロトコル（BGP）接続のステータスを表示します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65538`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 5	**bgp asnotation dot** 例： `Device(config-router)# bgp asnotation dot`	BGP 4 バイト AS 番号のデフォルト出力形式を asplain（10 進数値）からドット表記法に変更します。

	コマンドまたはアクション	目的
		（注） 4 バイト AS 番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 6	**end** 例： `Device(config-router)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**clear ip bgp *** 例： `Device# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト AS 番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**show ip bgp summary** 例： `Device# show ip bgp summary`	BGP 接続すべての状況を表示します。
ステップ 9	**show ip bgp regexp** *regexp* 例： `Device# show ip bgp regexp ^1\.0$`	AS パスの正規表現と一致するルートを表示します。 • この例では、4 バイトの AS パスをマッチングする正規表現は、asdot 形式で設定されています。
ステップ 10	**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 11	**router bgp** *autonomous-system-number* 例：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 65538`	• この例では、4 バイト AS 番号 65538 は asplain 表記法で定義されています。
ステップ 12	**no bgp asnotation dot** 例： `Device(config-router)# no bgp asnotation dot`	BGP 4 バイト AS 番号のデフォルト出力形式を asplain（10 進数値）にリセットします。 （注） 4 バイト AS 番号は、asplain 形式、または asdot 形式を使用して設定できます。このコマンドの影響を受けるのは、**show** コマンドの出力、または正規表現のマッチングだけです。
ステップ 13	**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 14	**clear ip bgp *** 例： `Device# clear ip bgp *`	現在の BGP セッションをすべてクリアし、リセットします。 • この例では、4 バイト AS 番号形式の変更がすべての BGP セッションに反映されていることを確認するために、ハード リセットが実行されています。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp summary** コマンドの出力は、4 バイト AS 番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト AS 番号 65536 および 65550 に注意してください。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハードリセットする **clear ip bgp *** コマンドが続きます）、出力は、次の **show ip bgp summary** コマンドの出力に示すように、asdot 表記法の形式に変換されます。asdot 形式で表された 4 バイト AS 番号 1.0 および 1.14 に注意してください。これらは AS 番号 65536 と 65550 を asdot 変換したものです。

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24      0
```

bgp asnotation dot コマンドの設定後（これに、現在の BGP セッションをすべてハードリセットする **clear ip bgp *** コマンドが続きます）、4 バイトの AS パスで使用される正規表現とのマッチング形式は asdot 表記法の形式に変更されます。4 バイト AS 番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト AS 番号だけがマッチングされます。下の先頭の例では、**show ip bgp regexp** コマンドは、asplain 形式で表された 4 バイト AS 番号を使って設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの AS パスに関する情報が asdot 表記法を使って表示されます。

（注） この asdot 表記法で使用されているピリオドは、シスコの正規表現では特殊文字です。特殊な意味を取り除くには、ピリオドの前にバックスラッシュをつけます。

```
Router# show ip bgp regexp ^65536$

Router# show ip bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

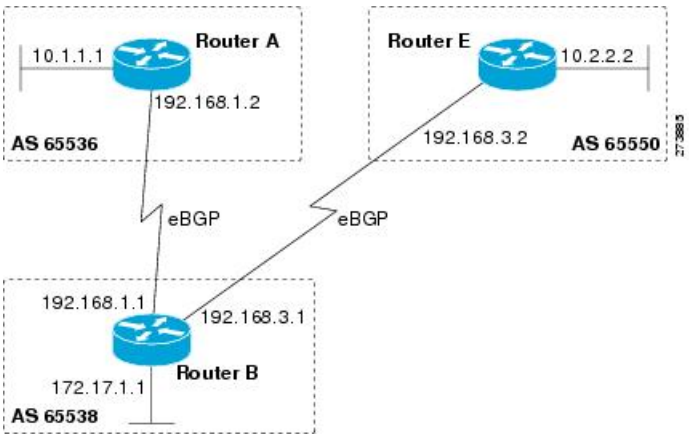
4 バイト ASN に対する BGP サポートの設定例

例：BGP ルーティング プロセスと 4 バイト自律システム番号を使用したピアの設定

asplain 形式

次に示すのは、下の図におけるボーダー ゲートウェイ プロトコル（BGP）プロセスを使ったルータ A、B、E のコンフィギュレーションの例で、このプロセスは、asplain 表記法を使用して設定された別々の 4 バイト自律システムのルータ A、B、E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 *17 : asplain* 形式の *4* バイト自律システム番号を使用する *BGP* ピア



ルータ A

```
router bgp 65536
 bgp router-id 10.1.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 65538
```

```
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

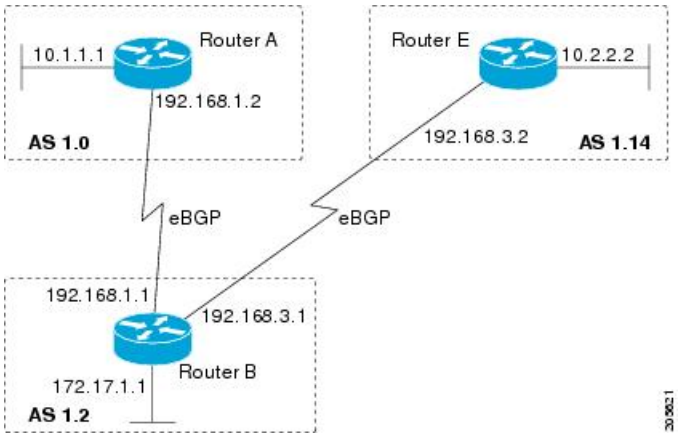
ルータ E

```
router bgp 65550
 bgp router-id 10.2.2.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 65538
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

asdot 形式

次に示すのは、下の図における BGP プロセスを使ったルータ A、B、E のコンフィギュレーションを作成する方法の例で、このプロセスは、デフォルトの asdot 形式を使用して設定された別々の 4 バイト自律システムのルータ A、B、E にある 3 つのネイバー ピアの間に設定されています。IPv4 ユニキャスト ルートはすべてのピアと交換されます。

図 *18 : asdot* 形式の *4* バイト自律システム番号を使用する *BGP* ピア



ルータ A

```
router bgp 1.0
 bgp router-id 10.1.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.1.1 activate
  no auto-summary
  no synchronization
  network 10.1.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ B

```
router bgp 1.2
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

ルータ E

```
router bgp 1.14
 bgp router-id 10.2.2.99
 no bgp default ipv4-unicast
 bgp fast-external-fallover
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.3.1 remote-as 1.2
 !
 address-family ipv4
  neighbor 192.168.3.1 activate
  no auto-summary
  no synchronization
  network 10.2.2.0 mask 255.255.255.0
  exit-address-family
```

例：4バイトのBGP自律システム番号を使用したVRFおよび拡張コミュニティの設定

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次の例は、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースで使用可能です。この例は、4 バイト自律システム番号 65537 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルートマップにより許可されたルートの拡張コミュニティ値 65537:100 を設定する方法を示しています。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 65537:100
 exit
route-map red_map permit 10
 set extcommunity rt 65537:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 65537 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map
route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

4 バイト自律システム番号の RD サポート

次の例は、4 バイト AS 番号 65536 を含むルート識別子、および 4 バイト自律システム番号 65537 を含むルート ターゲットを使用して、VRF を作成する方法を示しています。

```
ip vrf vpn_red
 rd 65536:100
 route-target both 65537:100
 exit
```

コンフィギュレーションの完了後、**show vrf** コマンドを使用して、4 バイト AS 番号ルート識別子が 65536:100 に設定されていることを確認します。

```
RouterB# show vrf vpn_red
Current configuration : 36 bytes
vrf definition x
 rd 65536:100
!
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次の例は、Cisco IOS Release 12.0(32)S12 および 12.4(24)T で使用可能です。この例は、4 バイト自律システム番号 1.1 を使用するルート ターゲットを使って VRF を作成する方法、およびルート ターゲットに、ルート マップにより許可されたルートの拡張コミュニティ値 1.1:100 を設定する方法を示しています。

（注） Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースでは、この例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して、asdot をデフォルトの表示形式として設定した場合だけです。

```
ip vrf vpn_red
 rd 64500:100
 route-target both 1.1:100
 exit
route-map red_map permit 10
 set extcommunity rt 1.1:100
 end
```

コンフィギュレーションの完了後、**show route-map** コマンドを使用して、拡張コミュニティが、4 バイト自律システム番号 1.1 を含むルート ターゲットに設定されていることを確認します。

```
RouterB# show route-map red_map
route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:1.1:100
  Policy routing matches: 0 packets, 0 bytes
```

4 バイト自律システム番号の RD サポートの asdot デフォルト形式

次の例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して asdot をデフォルトの表示形式として設定した場合です。

```
ip vrf vpn_red
 rd 1.0:100
 route-target both 1.1:100
 exit
```

4 バイト ASN に対する BGP サポ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』

関連項目	マニュアル タイトル
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 4893	『*BGP Support for Four-octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous System (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』
RFC 5668	『*4-Octet AS Specific BGP Extended Community*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

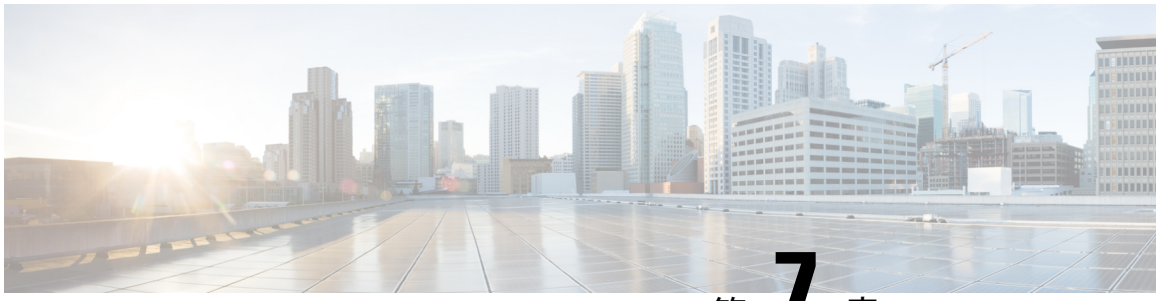
4 バイト ASN に対する BGP サポートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *18 : 4* バイト *ASN* に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
4 バイト ASN に対する BGP サポート		4 バイト ASN に対する BGP サポート機能により、4バイト自律システム番号がサポートされるようになりました。 次のコマンドが導入または変更されました。**bgp asnotation dot**、**bgp confederation identifier**、**bgp confederation peers**、自律システム番号を設定するすべての **clear ip bgp** コマンド、**ip as-path access-list**、**ip extcommunity-list**、**match source-protocol**、**neighbor local-as**、**neighbor remote-as**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、自律システム番号を表示するすべての **show ip bgp** コマンド、**show ip extcommunity-list**
BGP—4 バイト ASN RD および RT のサポート		4 バイト ASN RD および RT に対する BGP サポート機能により、4バイト自律システム番号がサポートされるようになりました。



第 7 章

IPv6ルーティング：マルチプロトコルBGP for IPv6 拡張

- 機能情報の確認 （215 ページ）
- IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張に関する情報 （215 ページ）
- マルチプロトコル BGP for IPv6 の設定方法 （216 ページ）
- マルチプロトコル BGP for IPv6 の設定例 （222 ページ）
- その他の参考資料 （224 ページ）
- IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張の機能情報 （225 ページ）

機能情報の確認

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

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

IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張に関する情報

Multiprotocol BGP Extensions for IPv6

マルチプロトコル BGP は、IPv6 でサポートされている外部ゲートウェイ プロトコル（EGP）です。マルチプロトコル BGP for IPv6 拡張では、IPv4 BGP と同じ機能および機能性の多くが

サポートされています。マルチプロトコル BGP に対する IPv6 拡張には、IPv6 アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、および IPv6 アドレスを使用するネクスト ホップ（宛先パス内の次のデバイス）属性のサポートが含まれています。

マルチプロトコル BGP for IPv6 の設定方法

IPv6 BGP ルーティング プロセスおよび BGP ルータ ID の設定

IPv6 BGP ルーティング プロセスを設定し、オプションの BGP 対応デバイス用 BGP ルータ ID を設定するには、次の作業を実行します。

BGP では、ルータ ID を使用して、BGP スピーキング ピアを識別します。BGP ルータ ID は、32 ビット値であり、多くの場合、IPv4 アドレスで表されます。デフォルトでは、ルータ ID は、デバイスのループバック インターフェイスの IPv4 アドレスに設定されます。デバイス上でループバック インターフェイスが設定されていない場合は、BGP ルータ ID を表すためにデバイスの物理インターフェイスに設定されている最上位の IPv4 アドレスがソフトウェアによって選択されます。

IPv6 だけが有効になっているデバイス（IPv4 アドレスを持っていないデバイス）で BGP を設定する場合、そのデバイスの BGP ルータ ID を手動で設定する必要があります。IPv4 アドレス構文を使用して 32 ビット値で表される BGP ルータ ID は、デバイスの BGP ピアで一意である必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **bgp router-id** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	前の手順で指定した BGP ルーティング プロセスの IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** コマンドを設定した場合は例外です。
ステップ 5	**bgp router-id** *ip-address* 例： `Device(config-router)# bgp router-id 192.168.99.70`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル デバイスの ID として設定します。 （注） **bgp router-id** コマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションがすべてリセットされます。

2 つのピア間での IPv6 マルチプロトコル BGP の設定

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address* [**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
5. **address-family ipv6** [**unicast** | **multicast**]
6. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* [**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*] 例： `Device(config-router)# neighbor 2001:DB8:0:CC00::1 remote-as 64600`	指定された自律システムのネイバーの IPv6 アドレスを、ローカル デバイスの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv6** [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドにキーワードが指定されていない場合、デバイスは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* **%**} **activate** 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 activate`	ローカル デバイスとの間で IPv6 アドレス ファミリのプレフィックスを交換できるようにネイバーを設定します。

IPv6 BGP ピア間での IPv4 ルートのアドバタイズ

IPv6 ネットワークによって 2 つの別々の IPv4 ネットワークが接続されている場合は、IPv6 を使用して IPv4 ルートをアドバタイズできます。IPv4 アドレス ファミリ内の IPv6 アドレスを使用して、ピアリングを設定します。アドバタイズされるネクストホップは、通常、到着不能であるため、スタティック ルートまたはインバウンド ルート マップを使用してネクスト ホップを設定します。2 つの IPv4 ピア間での IPv6 ルートのアドバタイズも同じモデルを使用して実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
6. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
7. **neighbor** *ipv6-address* **peer-group** *peer-group-name*
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}
9. **exit**
10. **exit**
11. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
12. **set ip next-hop** *ip-address* [*... ip-address*] [**peer-address**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** 例：	マルチプロトコル BGP ピア グループを作成します。

	コマンドまたはアクション	目的
	`Device(config-router)# neighbor 6peers peer-group`	
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*] 例： `Device(config-router)# neighbor 6peers remote-as 65002`	指定された自律システムのネイバーの IPv6 アドレスを、ローカル デバイスの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** *ipv6-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 2001:DB8:1234::2 peer-group 6peers`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 6peers route-map rmap out`	着信ルートまたは発信ルートにルート マップを適用します。 • ルートマップへの変更は、ピアリングがリセットされるまで、またはソフト リセットが実行されるまで、現在のピアでは有効になりません。**soft** キーワードと **in** キーワードを指定して **clear bgp ipv6** コマンドを使用すると、ソフト リセットが実行されます。
ステップ 9	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、デバイスをルータ コンフィギュレーション モードに戻します。
ステップ 10	**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、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 11	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map rmap permit 10`	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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**set ip next-hop** *ip-address* [*... ip-address*] [**peer-address**] 例： `Device(config-route-map)# set ip next-hop 10.21.8.10`	IPv4 パケットのピアにアドバタイズされるネクスト ホップをオーバーライドします。

外部 BGP ピアのクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]
3. **clear bgp ipv6** {**unicast** | **multicast**} **peer-group** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear bgp ipv6** {**unicast**	**multicast**} **external** [**soft**] [**in**	**out**] 例： `Device# clear bgp ipv6 unicast external soft in`	外部 IPv6 BGP ピアをクリアします。
ステップ 3	**clear bgp ipv6** {**unicast**	**multicast**} **peer-group** *name* 例： `Device# clear bgp ipv6 unicast peer-group marketing`	IPv6 BGP ピア グループのすべてのメンバをクリアします。

BGP IPv6 アドミニストレーティブ ディスタンスの設定

•

始める前に

•

手順の概要

1.

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例：	

例

次のタスク

-

マルチプロトコル BGP for IPv6 の設定例

例：BGP プロセス、BGP ルータ ID、IPv6 マルチプロトコル BGP ピアの設定

次の例では、IPv6 をグローバルに有効にし、BGP プロセスを設定して、BGP ルータ ID を確立します。また、IPv6 マルチプロトコル BGP ピア 2001:DB8:0:CC00::1 を設定してアクティブ化します。

```
ipv6 unicast-routing
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp router-id 192.168.99.70
 neighbor 2001:DB8:0:CC00::1 remote-as 64600
 address-family ipv6 unicast
  neighbor 2001:DB8:0:CC00::1 activate
```

例：IPv6 マルチプロトコル BGP ピア グループの設定

次に、group1 という名前の IPv6 マルチプロトコル BGP ピア グループを設定する例を示します。

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:DB8:0:CC00::1 remote-as 64600
address-family ipv6 unicast
 neighbor group1 activate
 neighbor 2001:DB8:0:CC00::1 peer-group group1
```

例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ

次に、ローカルデバイスのIPv6ユニキャストデータベースにIPv6ネットワーク2001:DB8::/24を挿入する例を示します（BGPは、ネットワークをアドバタイズする前に、ネットワークのルートがローカルデバイスのIPv6ユニキャストデータベースに存在することを確認します）。

```
router bgp 65000
 no bgp default ipv4-unicast
address-family ipv6 unicast
  network 2001:DB8::/24
```

例：IPv6マルチプロトコルBGPプレフィックスのルートマップの設定

次に、rtp という名前のルート マップを設定して、ネットワーク 2001:DB8::/24 からの IPv6 ユニキャスト ルートが cisco という名前のプレフィックス リストに一致する場合は、その IPv6 ユニキャスト ルートを許可する例を示します。

```
router bgp 64900
no bgp default ipv4-unicast
neighbor 2001:DB8:0:CC00::1 remote-as 64700
address-family ipv6 unicast
 neighbor 2001:DB8:0:CC00::1 activate
 neighbor 2001:DB8:0:CC00::1 route-map rtp in
ipv6 prefix-list cisco seq 10 permit 2001:DB8::/24
route-map rtp permit 10
 match ipv6 address prefix-list cisco
```

例：IPv6 マルチプロトコル BGP へのプレフィックスの再配布

次の例では、RIP ルートをローカル デバイスの IPv6 ユニキャスト データベースに再配布しています。

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 unicast
 redistribute rip
```

例：IPv6 ピア間での IPv4 ルートのアドバタイズ

次の例では、IPv6 ネットワークが 2 つの個別 IPv4 ネットワークに接続している場合に、IPv6 ピア間で IPv4 ルートをアドバタイズしています。ピアリングは、IPv4 アドレス ファミリ コンフィギュレーション モードで IPv6 アドレスを使用して設定されています。アドバタイズされたネクスト ホップは到達不能である可能性があるため、rmap という名前のインバウンド ルート マップによってネクスト ホップが設定されます。

```
router bgp 65000
!
 neighbor 6peers peer-group
 neighbor 2001:DB8:1234::2 remote-as 65002
 address-family ipv4
```

```
 neighbor 6peers activate
 neighbor 6peers soft-reconfiguration inbound
 neighbor 2001:DB8:1234::2 peer-group 6peers
 neighbor 2001:DB8:1234::2 route-map rmap in
!
route-map rmap permit 10
 set ip next-hop 10.21.8.10
```

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 Command List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MB	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

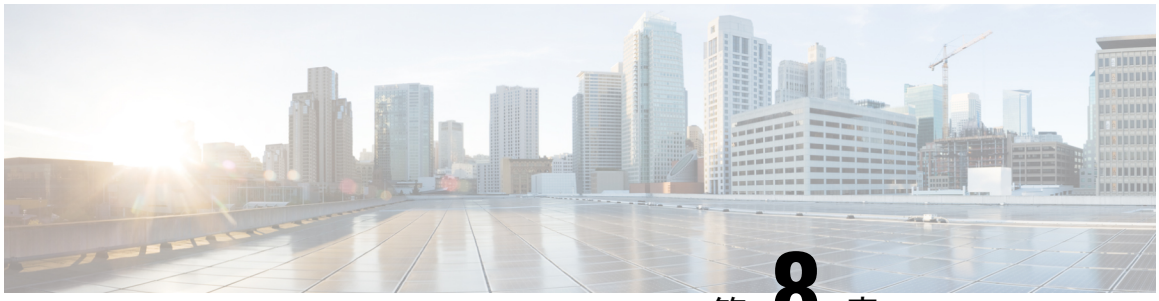
IPv6 ルーティング マルチプロトコル BGP for IPv6 拡張の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *19 : IPv6* ルーティング マルチプロトコル *BGP for IPv6* 拡張の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：マルチプロトコル BGP for IPv6 拡張	Cisco IOS XE Release 2.1	マルチプロトコル BGP for IPv6 拡張では、IPv4 BGP と同じ機能および機能性がサポートされています。



第 8 章

IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリング

- 機能情報の確認 （227 ページ）
- IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングに関する情報 （228 ページ）
- IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定方法 （228 ページ）
- IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定例 （233 ページ）
- その他の参考資料 （234 ページ）
- IPv6 ルーティング マルチプロトコル BGP リンクローカル アドレス ピアリングの機能情報 （235 ページ）

機能情報の確認

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

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

IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングに関する情報

リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアリング

リンクローカル アドレスを使用して、2 つの IPv6 デバイス（ピア）間で IPv6 マルチプロトコル BGP を設定できます。この機能を動作させるには、**neighbor update-source** コマンドを使用してネイバーのインターフェイスを識別する必要があり、IPv6 グローバル ネクスト ホップを設定するようにルート マップを設定する必要があります。

ボーダー ゲートウェイ プロトコル（BGP）では、同じインターフェイス上の IPv6 リンクローカル アドレスを介した複数のピアとのピアリングのためにサードパーティ ネクスト ホップを使用します。異なるインターフェイス上のリンクローカルアドレスを介したピアリングでは、サードパーティ ネクスト ホップは使用できません。リンクローカル アドレスを使用してピアリングするネイバーは、インターフェイスごとに 1 つのアップデート グループに分けられます。BGP では、リンクローカル アドレスを持つネイバーのアップデート グループ メンバーシップは、そのネイバーとの通信に使用されるインターフェイスに基づいて分けられます。

IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定方法

Configuring an IPv6 Multiprotocol BGP Peer Using a Link-Local Address

リンクローカル アドレスを使用して 2 台の IPv6 ルータ（ピア）間に IPv6 マルチプロトコル BGP を設定する場合は、ネイバーのインターフェイスが **update-source** コマンドを使用して識別され、IPv6 グローバル ネクスト ホップを設定するようにルート マップが設定されている必要があります。

（注）
- デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。IPv6 プレフィックスなど、その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。
- デフォルトでは、**neighbor route-map** コマンドを使用してルータ コンフィギュレーション モードで適用されるルート マップは、IPv4 ユニキャスト アドレス プレフィックスだけに適用されます。IPv6 アドレス ファミリなどのその他のアドレス ファミリのルート マップは、**neighbor route-map** コマンドを使用してアドレス ファミリ コンフィギュレーション モードで適用される必要があります。ルート マップは、指定したアドレス ファミリの下にあるネイバーの着信ルーティング ポリシーまたは発信ルーティング ポリシーとして適用されます。各アドレス ファミリ タイプで個別のルート マップを設定すると、各アドレス ファミリの複雑なポリシーまたはさまざまなポリシーを簡単に管理できるようになります。
- ネクストホップの変更に使用するルートマップは、アウトバウンドにのみ適用する必要があります。ネクストホップ IPv6 アドレスを変更するためのインバウンド ルートマップはサポートされていません。インバウンド ルートマップは、IPV4 アドレス ファミリでのみサポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
5. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* **%**} **activate**
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*[**%**]} **route-map** *map-name* {**in** | **out**
9. **exit**
10. ステップ 9 を繰り返します。
11. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
12. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*
13. **set ipv6 next-hop** *ipv6-address* [*link-local-address*] [**peer-address**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] 例： `Device(config-router)# neighbor FE80::1234:BFF:FE0E:A471% remote-as 64600`	指定したリモート自律システム内のネイバーのリンクローカル IPv6 アドレスをローカル ルータの IPv6 マルチプロトコル BGP ネイバーテーブルに追加します。 • 省略可能な **%** キーワードは、IPv6 リンクローカルアドレス識別子です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number* 例： `Device(config-router)# neighbor FE80::1234:BFF:FE0E:A471% update-source gigabitethernet0/0/0`	ピアリングが発生するリンクローカル アドレスを指定します。 • 省略可能な **%** キーワードは、IPv6 リンクローカルアドレス識別子です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。 • ネイバーへの接続が複数存在し、**neighbor update-source** コマンドで *interface-type* 引数と *interface-number* 引数を使用してネイバー インターフェイスを指定していない場合は、リンクローカルアドレスを使用してネイバーとの TCP 接続を確立することはできません。

	コマンドまたはアクション	目的
ステップ 6	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6** 例： `Device(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv6** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* **%**} **activate** 例： `Device(config-router-af)# neighbor FE80::1234:BFF:FE0E:A471% activate`	ネイバーが、指定したリンクローカル アドレスを使用して IPv6 アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。 • 省略可能な **%** キーワードは、IPv6 リンクローカルアドレス識別子です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*[**%**]} **route-map** *map-name* {**in** | **out** 例： `Device(config-router-af)# neighbor FE80::1234:BFF:FE0E:A471% route-map nh6 out`	着信ルートまたは発信ルートにルート マップを適用します。 • 省略可能な **%** キーワードは、IPv6 リンクローカルアドレス識別子です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 9	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、デバイスをルータ コンフィギュレーション モードに戻します。
ステップ 10	ステップ 9 を繰り返します。 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、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 11	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例：	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 モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# route-map nh6 permit 10`	
ステップ 12	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name* 例： `Device(config-route-map)# match ipv6 address prefix-list cisco`	プレフィックス リストで許可されている宛先 IPv6 ネットワーク番号アドレスを持つすべてのルートを配布するか、パケットに対してポリシー ルーティングを実行します。
ステップ 13	**set ipv6 next-hop** *ipv6-address* [*link-local-address*] [**peer-address** 例： `Device(config-route-map)# set ipv6 next-hop 2001:DB8::1`	ポリシー ルーティング用のルート マップの match 句を渡す IPv6 パケットのピアにアドバタイズされるネクスト ホップを上書きします。 • *ipv6-address* 引数には、ネクスト ホップの IPv6 グローバル アドレスを指定します。隣接ルータである必要はありません。 • *link-local-address* 引数には、ネクスト ホップの IPv6 リンクローカル アドレスを指定します。隣接ルータである必要があります。 （注） ルートマップによって、BGP アップデートに IPv6 ネクストホップ アドレス（グローバルおよびリンクローカル）が設定されます。ルート マップが設定されていない場合、デフォルトでは、BGP アップデートのネクストホップ アドレスは未指定の IPv6 アドレス（::）に設定され、ピアで拒否されます。手順 5 の **neighbor update-source** コマンドでネイバー インターフェイス（*interface-type* 引数）を指定した後に、**set ipv6 next-hop** コマンドでグローバル IPv6 ネクストホップ アドレス（*ipv6-address* 引数）だけを指定した場合は、*interface-type* 引数で指定したインターフェイスのリンクローカル アドレスが BGP アップデートのネクストホップとして含まれます。したがって、リンクローカル アドレスを使用する複数の BGP ピアに必要となるのは、BGP アップデートにグローバル IPv6 ネクストホップ アドレスを設定する 1 つのルート マップだけとなります。

IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリングの設定例

例：リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定

次の例では、GigabitEthernet インターフェイス 0/0 上で IPv6 マルチプロトコル BGP ピア FE80::1234:BFF:FE0E:A471 を設定し、GigabitEthernet インターフェイス 0/0 の IPv6 ネクストホップ グローバル アドレスを BGP アップデートに含めるために nh6 という名前のルート マップを設定します。IPv6 ネクストホップ リンクローカル アドレスは、nh6 ルート マップ（次の例には記載なし）によって、または **neighbor update-source** コマンド（この例を参照）で指定したインターフェイスから設定できます。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 5
Device(config-router)# neighbor internal peer-group
Device(config-router)# neighbor  FE80::1234:BFF:FE0E:A471% peer-group
Device(config-router)# neighbor internal remote-as 100
Device(config-router)# neighbor FE80::1234:BFF:FE0E:A471% remote-as 64600
Device(config-router)# neighbor FE80::1234:BFF:FE0E:A471% update-source Gigabitethernet
 0/0
Device(config-router)# address-family ipv6
Device(config-router-af)# neighbor FE80::1234:BFF:FE0E:A471% activate
Device(config-router-af)# neighbor FE80::1234:BFF:FE0E:A471% route-map nh6 out
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# route-map nh6permit 10
Device(config-router-map)# match ipv6 address prefix-list cisco
Device(config-router-map)# set ipv6 next-hop 2001:DB8:526::1
Device(config-router-map)# exit
Device(config)# ipv6 prefix-list cisco permit 2001:DB8:2F22::/48 le 128
Device(config)# ipv6 prefix-list cisco deny ::/0
Device(config)# end
```

（注） **neighbor update-source** コマンドでネイバー インターフェイス（*interface-type* 引数）を指定した後に、**set ipv6 next-hop** コマンドでグローバル IPv6 ネクストホップ アドレス（*ipv6-address* 引数）だけを指定した場合は、*interface-type* 引数で指定したインターフェイスのリンクローカルアドレスが BGP アップデートのネクストホップとして含まれます。したがって、リンクローカル アドレスを使用する複数の BGP ピアに必要となるのは、BGP アップデートにグローバル IPv6 ネクストホップ アドレスを設定する 1 つのルート マップだけとなります。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MB	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

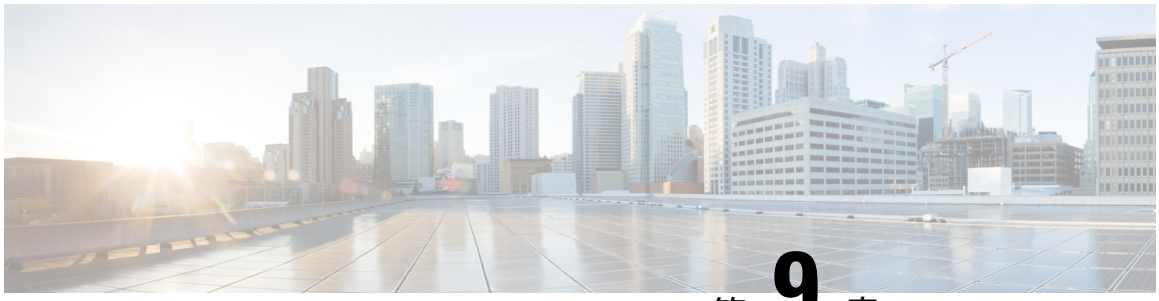
IPv6 ルーティング マルチプロトコル BGP リンクローカル アドレス ピアリングの機能情報

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

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *20 : IPv6* ルーティング：マルチプロトコル *BGP* リンクローカル アドレス ピアリングの機能情報

機能名	リリース	機能情報
IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリング	Cisco IOS XE Release 2.1	この機能は、サポートされています。



第 9 章

IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポート

- 機能情報の確認 （237 ページ）
- IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する情報 （238 ページ）
- IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの実装方法（239 ページ）
- IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの設定例（248 ページ）
- その他の参考資料 （249 ページ）
- IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する機能情報 （250 ページ）

機能情報の確認

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

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

IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する情報

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、および IPv6 アドレスを使用するネクスト ホップ（宛先へのパス内の次のルータ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPv6 は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するために、個別の BGP ルーティング テーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの実装方法

IPv6 ピア グループでマルチキャスト BGP ルーティングを実行するための設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family ipv6** [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router)# neighbor group1 peer-group`	BGP ピア グループを作成します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* 例： `Device(config-router)# neighbor 2001:DB8:0:CC00::1 remote-as 64600`	指定した自律システムにおけるネイバーのIPv6アドレスをローカル ルータの IPv6 マルチキャスト BGP ネイバーテーブルに追加します。 • **neighbor remote-as** コマンドの *ipv6-address* 引数には、RFC 2373 に記載されている形式を使用する必要があります。その場合、16 ビット値を使用した 16 進数でアドレスを指定し、コロンで区切ります。
ステップ 6	**address-family ipv6** [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6 multicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドにキーワードが指定されていない場合、ルータはIPv6ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 activate`	ネイバーが、指定したファミリ タイプのプレフィックスをネイバーおよびローカル ルータと交換できるようにします。 • 各ネイバーでの追加の設定手順を回避するために、この手順の代替として、*peer-group-name* 引数を指定して **neighbor activate** コマンドを使用します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 peer-group group1`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。

IPv6 マルチプロトコル BGP へのルートのアドバタイズ

デフォルトでは、**network** コマンドを使用してルータ コンフィギュレーション モードで定義されたネットワークは、IPv4ユニキャストデータベースに挿入されます。IPv6 BGP データベースなど、別のデータベースにネットワークを挿入するには、IPv6 BGP データベースの場合と同様に、そのデータベースについて、アドレス ファミリ コンフィギュレーション モードで **network** コマンドを使用してネットワークを定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast**	**multicast**	**vpnv6**] 例： `Device(config-router)# address-family ipv6 unicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドにキーワードが指定されていない場合、デバイスは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 5	**network** {*network-number* [**mask** *network-mask*]	*nsap-prefix*} [**route-map** *map-tag*] 例： `Device(config-router-af)# network 2001:DB8::/24`	指定したプレフィックスを IPv6 BGP データベースにアドバタイズ（挿入）します（まず、IPv6 ユニキャスト ルーティング テーブルでルートを見つける必要があります）。 • 前の手順で指定したアドレス ファミリのデータベースにプレフィックスが挿入されます。

	コマンドまたはアクション	目的
		• ルートには指定したプレフィックスによって「local origin」のタグが付けられます。 • **network** コマンドの *ipv6-prefix* 引数には、RFC 2373 に記載されている形式を使用する必要があります。その場合、16 ビット値を使用した 16 進数でアドレスを指定し、コロンで区切ります。 • *prefix-length* 引数は、アドレスのうち連続する上位何ビットがプレフィックス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 6	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、デバイスをルータ コンフィギュレーション モードに戻します。 • この手順を繰り返して、ルータ 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。

IPv6 マルチプロトコル BGP へのプレフィックスの再配布

再配布とは、あるルーティング プロトコルから別のルーティング プロトコルにプレフィックスを再配布、つまり挿入するプロセスです。ここでは、あるルーティング プロトコルのプレフィックスを IPv6 マルチプロトコル BGP に挿入する方法について説明します。具体的には、**redistribute** ルータ コンフィギュレーション コマンドを使用して IPv6 マルチプロトコル BGP に再配布されたプレフィックスは、IPv6 ユニキャスト データベースに挿入されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **redistribute bgp** [*process-id*] [**metric** *metric-value*] [**route-map** *map-name*] [*source-protocol-options*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] 例： `Device(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドにキーワードが指定されていない場合、デバイスはIPv6ユニキャストアドレスファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 5	**redistribute bgp** [*process-id*] [**metric** *metric-value*] [**route-map** *map-name*] [*source-protocol-options*] 例： `Device(config-router-af)# redistribute bgp 64500 metric 5`	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。
ステップ 6	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、デバイスをルータ コンフィギュレーション モードに戻します。 • この手順を繰り返して、ルータ 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。

BGP のアドミニストレーティブ ディスタンスの割り当て

⚠

注意 BGP 内部ルートのアドミニストレーティブ ディスタンスの変更は推奨されません。発生する可能性のある 1 つの問題は、ルーティング テーブルの不整合が累積され、それによってルーティングが中断する可能性があることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**}
5. **distance bgp** *external-distance internal-distance local-distance*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast**	**multicast**} 例： `Device(config-router)# address-family ipv6 multicast`	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**distance bgp** *external-distance internal-distance local-distance* 例： `Device(config-router)# distance bgp 20 20 200`	BGP アドミニストレーティブ ディスタンスを割り当てます。

IPv6 マルチキャスト BGP の変換アップデートの生成

一般的に、マルチキャスト BGP の変換アップデート機能は、BGP 対応ルータだけが存在するカスタマー サイトとピアであるマルチキャスト BGP 対応ルータで使用されます。カスタマー サイトは、ルータをマルチキャスト BGP 対応イメージにアップグレードしません（できません）。カスタマー サイトはマルチキャスト BGP アドバタイズメントの起点となることはできないため、そのピアであるルータが BGP プレフィックスをマルチキャスト BGP プレフィックスに変換します。この変換後のプレフィックスがマルチキャスト送信元の RPF ルックアップで使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**}
5. **neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast**	**multicast**} 例： `Device(config-router)# address-family ipv6 multicast`	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**] 例：	ピアから受信したユニキャスト IPv6 アップデートに対応するマルチプロトコル IPv6 BGP アップデートを生成します。

	コマンドまたはアクション	目的
	`Device(config-router)# neighbor 2001:DB8:7000::2 translate-update ipv6 multicast`	

IPv6 BGP セッションのリセット

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | **peer-group** *peer-group-name*} [**soft**] [**in** | **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear bgp ipv6** {**unicast**	**multicast**} {*****	*autonomous-system-number*	*ip-address*	*ipv6-address*	**peer-group** *peer-group-name*} [**soft**] [**in**	**out**] 例： `Device# clear bgp ipv6 unicast peer-group marketing soft out`	IPv6 BGP セッションをリセットします。

外部 BGP ピアのクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]
3. **clear bgp ipv6** {**unicast** | **multicast**} **peer-group** *name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**] 例： `Device# clear bgp ipv6 unicast external soft in`	外部 IPv6 BGP ピアをクリアします。
ステップ 3	**clear bgp ipv6** {**unicast** | **multicast**} **peer-group** *name* 例： `Device# clear bgp ipv6 unicast peer-group marketing`	IPv6 BGP ピア グループのすべてのメンバをクリアします。

IPv6 BGP ルート減衰情報のクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*] 例： `Device# clear bgp ipv6 unicast dampening 2001:DB8::/64`	IPv6 BGP ルート ダンプニング情報をクリアし、抑制されたルートの抑制を解除します。

IPv6 BGP フラップ統計情報のクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*] 例： `Device# clear bgp ipv6 unicast flap-statistics filter-list 3`	IPv6 BGP フラップ統計情報をクリアします。

IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートの設定例

例：IPv6 マルチプロトコル BGP ピア グループの設定

次に、group1 という名前の IPv6 マルチプロトコル BGP ピア グループを設定する例を示します。

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:DB8:0:CC00::1 remote-as 64600
address-family ipv6 unicast
 neighbor group1 activate
 neighbor 2001:DB8:0:CC00::1 peer-group group1
```

例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ

次に、ローカルデバイスの IPv6 ユニキャスト データベースに IPv6 ネットワーク 2001:DB8::/24 を挿入する例を示します（BGP は、ネットワークをアドバタイズする前に、ネットワークのルートがローカルデバイスの IPv6 ユニキャスト データベースに存在することを確認します）。

```
router bgp 65000
 no bgp default ipv4-unicast
address-family ipv6 unicast
  network 2001:DB8::/24
```

例：IPv6 マルチプロトコル BGP へのプレフィックスの再配布

次の例では、RIP ルートをローカル デバイスの IPv6 ユニキャスト データベースに再配布しています。

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 unicast
 redistribute rip
```

例：IPv6 マルチキャスト BGP の変換アップデートの生成

次に、ユニキャスト IPv6 アップデートに対応する IPv6 マルチキャスト BGP アップデートを生成する例を示します。

```
router bgp 64900
 no bgp default ipv4-unicast
address-family ipv6 multicast
 neighbor 2001:DB8:7000::2 translate-update ipv6 multicast
```

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 Command List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

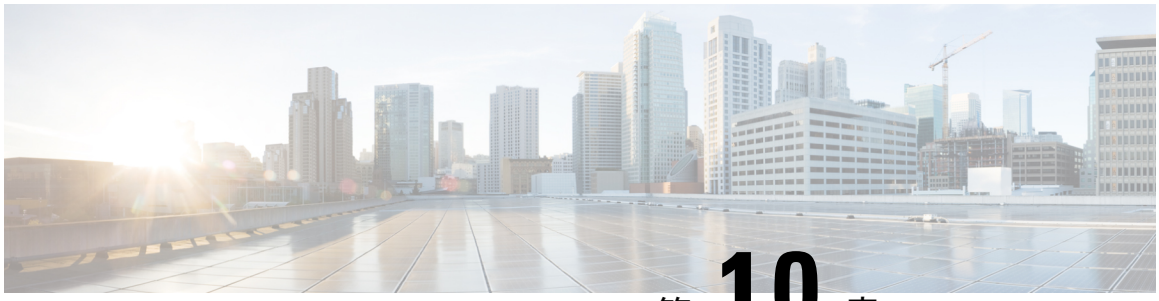
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポートに関する機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *21 : IPv6* マルチキャスト アドレス ファミリでのマルチプロトコル *BGP* のサポートに関する機能情報

機能名	リリース	機能情報
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポート	Cisco IOS XE Release 2.1	この機能は、IPv6 のマルチキャスト BGP 拡張を提供し、IPv4 BGP と同じ機能をサポートしています。



第 10 章

CLNS に対するマルチプロトコル BGP（MP-BGP）サポートの設定

このモジュールでは、コネクションレス型ネットワーク サービス（CLNS）ネットワークをスケーリングする機能を提供する、CLNS に対するマルチプロトコル BGP（MP-BGP）サポートを設定する作業について説明します。ボーダー ゲートウェイ プロトコル（BGP）のマルチプロトコル拡張は、ルーティング ドメインをマージせずに個別の開放型システム間相互接続（OSI）ルーティング ドメインを相互接続する機能を追加することによって、大規模な OSI ネットワークを確立する機能を実現します。

- 機能情報の確認 （251 ページ）
- CLNS に対する MP-BGP サポートの設定に関する制約事項 （252 ページ）
- CLNS に対する MP-BGP サポートの設定の概要 （252 ページ）
- CLNS に対する MP-BGP サポートの設定方法 （257 ページ）
- CLNS に対する MP-BGP サポートの設定例 （279 ページ）
- その他の参考資料 （289 ページ）
- CLNS に対する MP-BGP サポートの設定に関する機能情報 （289 ページ）
- 用語集 （292 ページ）

機能情報の確認

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

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

CLNSに対するMP-BGPサポートの設定に関する制約事項

CLNS に対する MP-BGP サポートの設定は、CLNS ネットワーク内の BGP コンフェデレーションの作成と使用をサポートしていません。大規模な内部 BGP メッシュの問題を解決するために、ルート リフレクタを使用することを推奨します。

BGP 拡張コミュニティは、CLNS に対する MP-BGP サポート機能ではサポートされていません。

次の BGP コマンドは、CLNS に対する MP-BGP サポート機能ではサポートされていません。

- **auto-summary**
- **neighbor advertise-map**
- **neighbor distribute-list**
- **neighbor soft-reconfiguration**
- **neighbor unsuppress-map**

CLNS に対する MP-BGP サポートの設定の概要

アドレス ファミリ ルーティング情報

デフォルトでは、**router bgp** コマンド下で入力されたコマンドは IPv4 アドレス ファミリに適用されます。この状態は、**router bgp** コマンド下の最初のコマンドとして **no bgp default ipv4-unicast** コマンドを入力しない限り継続します。**no bgp default ipv4-unicast** コマンドは、BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にするために、ルータで設定されます。

CLNS に対する MP-BGP サポートの設計機能

CLNS に対する MP-BGP サポートの設定により、CLNS をネットワーク層プロトコルとして使用するネットワーク内のドメイン間ルーティング プロトコルとして BGP を使用できます。この機能は、多数のネットワーク要素がリモート管理されるデータ通信ネットワーク（DCN）でのスケーリング問題を解決するために開発されました。DCN の問題、およびこの機能を DCN トポロジ内に実装する方法の詳細については、DCN ネットワーク トポロジ （254 ページ）を参照してください。

BGP は、外部ゲートウェイ プロトコル（EGP）として、インターネットによって生成されるルーティング情報の量を処理するように設計されています。BGP ネイバー関係（ピアリング）が手動で設定され、ルーティング アップデートがインクリメンタル ブロードキャストを使用するため、ネットワーク管理者は BGP ルーティング情報を制御できます。一方、Intermediate

System-to-Intermediate System（IS-IS）などの内部ルーティング プロトコルには、一種の自動ネイバー探索やブロードキャスト アップデートを定期的な間隔で使用するものもあります。

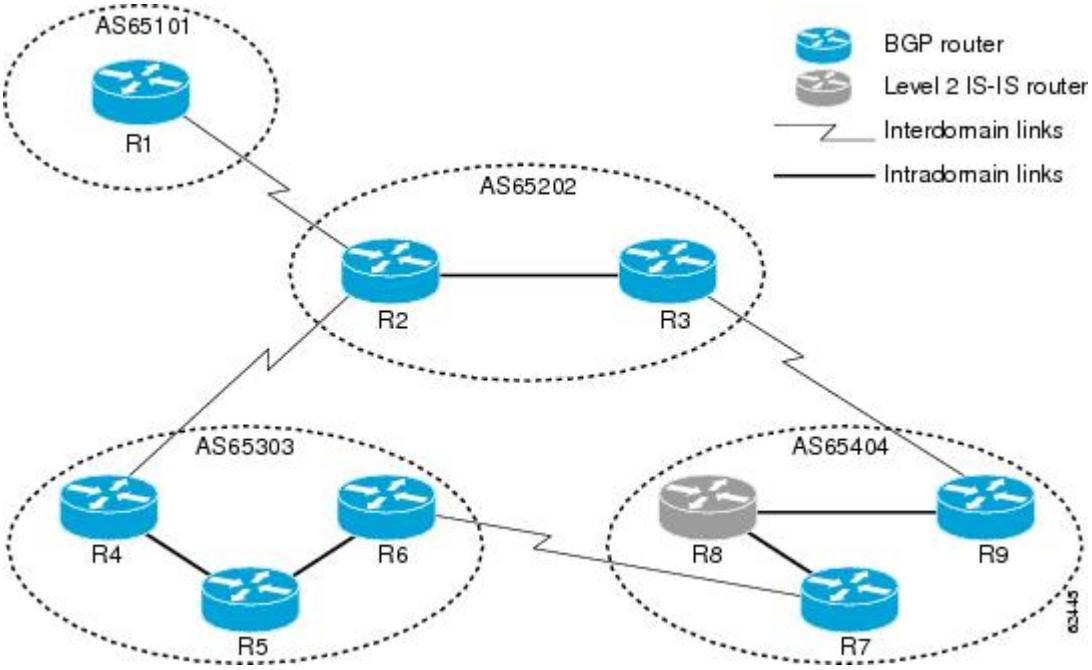
CLNS はネットワーク サービス アクセス ポイント（NSAP）アドレスを使用して、そのすべてのネットワーク要素を識別します。BGP アドレス ファミリ サポートにより、NSAP アドレス プレフィックスは BGP を使用して転送できます。CLNS では、BGP プレフィックスが CLNS レベル 2 プレフィックス テーブルに挿入されます。この機能を使用すると、BGP をドメイン間ルーティング プロトコルとして個別の CLNS ルーティング ドメイン間で使用できます。

各内部ネットワークのエッジのルータに BGP を実装すると、既存の内部プロトコルを変更する必要がないため、ネットワークの中断が最小化されます。

汎用 BGP CLNS ネットワーク トポロジ

下の図に、4 つの異なる自律システム（BGP 用語）またはルーティング ドメイン（OSI 用語）にグループ分けされる 9 つのルータを含む汎用 BGP CLNS ネットワークを示します。混乱を避けるために、BGP 用語である自律システムを使用します。各自律システムには番号が付いているため、図中や設定上の説明で識別が容易であるからです。

図 *19* : 汎用 *BGP CLNS* ネットワークのコンポーネント



各自律システムでは、IS-IS がイントラドメイン ルーティング プロトコルとして使用されます。自律システム間で、BGP およびそのマルチプロトコル拡張は、ドメイン間ルーティング プロトコルとして使用されます。各ルータは、BGP またはレベル 2 IS-IS ルーティング プロセスのいずれかを実行します。この機能を支援するために、BGP ルータはレベル 2 IS-IS プロセスも実行しています。図にリンクが示されていませんが、各レベル 2 IS-IS ルータが複数のレベル 1 IS-IS ルータに接続され、次に、各レベル 1 IS-IS ルータが複数の CLNS ネットワークに接続されています。

この例では、各自律システムは、さまざまな BGP 機能およびその機能と CLNS が連動してスケーラブルなドメイン間ルーティング ソリューションを提供する方法を示すように構成されています。上の図では、自律システム AS65101 には 1 つのレベル 2 IS-IS ルータの R1 があり、他の 1 つの自律システム AS65202 だけと接続されています。残りのネットワークとの接続が R2 によって可能になり、R1 が R2 に AS65101 外部の宛先 NSAP アドレスを持つすべてのパケットを送信するために、デフォルト ルートが生成されます。

AS65202 には R2 と R3 の 2 つのルータがあり、その両方が異なる外部 BGP（eBGP）ネイバーを持ちます。ルータ R2 および R3 は、お互いの間の内部接続上で内部 BGP（iBGP）を実行するように設定されています。

AS65303 は BGP ピア グループの使用方法を示し、ルート リフレクションはルータ間の TCP 接続の必要性を最小化できます。ルータ間の接続数が少ないため、ネットワーク設計が簡略化され、ネットワーク内のトラフィック量が少なくなります。

AS65404 は、BGP を実行していないレベル 2 IS-IS ルータと到着可能性情報を通信するための再配布の使用方法を示します。

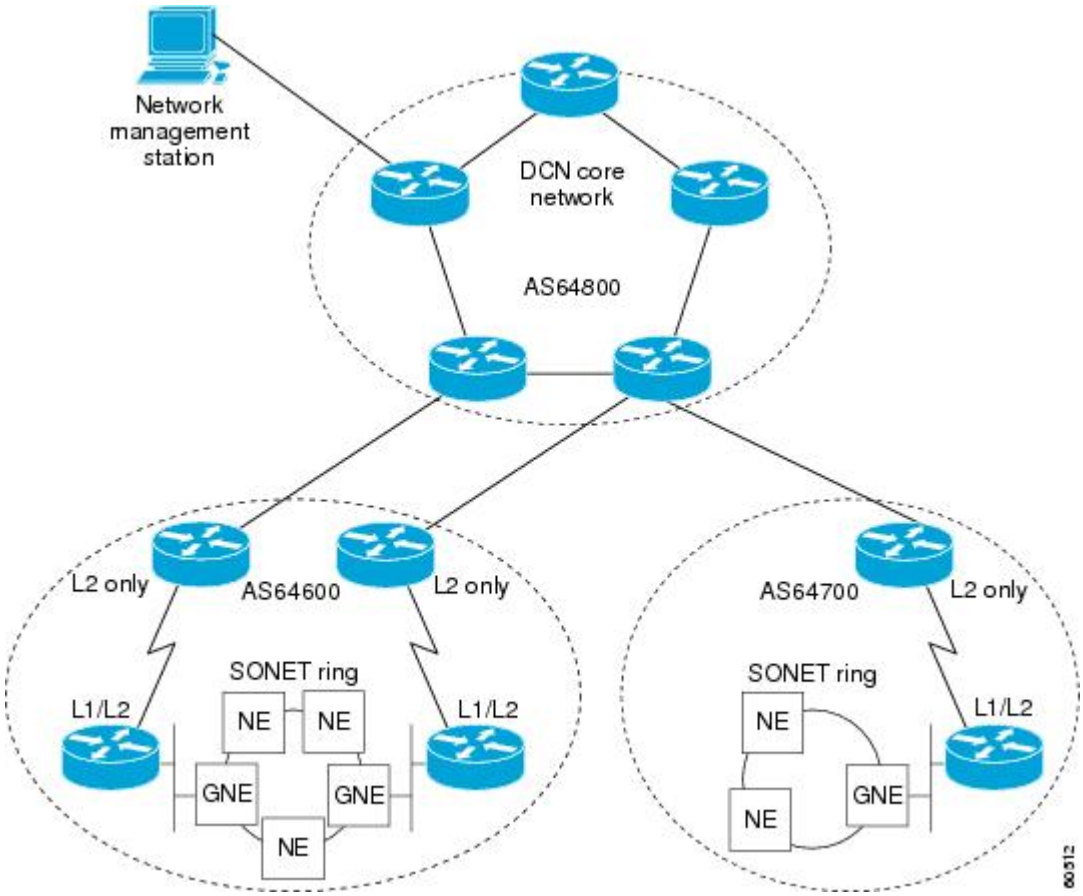
設定作業と例は、上の図に示されている汎用ネットワーク設計に基づいています。この図にあるすべてのルータの設定は、CLNS に対する MP-BGP サポートの実装の例 （283 ページ）に示されています。

DCN ネットワーク トポロジ

CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能は、多数のリモート SONET リングを管理する DCN に利点を提供できます。SONET は通常、光ファイバ ネットワークをとしてデータを送信する電気通信会社によって使用されます。

下の図に、DCN ネットワークの一部のコンポーネントを示します。BGP 用語との整合性をとるため、図には、3 つのルーティング ドメインではなく、自律システムを示すラベルがあります。SONET リングのネットワーク要素（図 2 の NE）は、File Transfer, Access, and Management（FTAM）および共通管理情報プロトコル（CMIP）などの OSI プロトコルによって管理されます。FTAM および CMIP は CLNS ネットワーク層プロトコルで実行されます。つまり、接続を提供するルータは OSI ルーティング プロトコルを実行する必要があります。

図 *20 : DCN* ネットワークのコンポーネント



IS-IS は、この例では、CLNS をルーティングするために使用されるリンクステートのプロトコルです。各ルーティング ノード（ネットワーキングデバイス）は、中継システム（IS）と呼ばれます。ネットワークは、ルーティング ノードのコレクションとして定義される領域に分割されます。1 つの領域内のルーティングは、レベル 1 ルーティングと呼ばれます。領域間のルーティングは、レベル 2 ルーティングと呼ばれます。レベル 1 領域とレベル 2 領域をリンクするルータは、レベル 1-2 ルータとして定義されます。DCN コアへのパスを提供するレベル 2 ルータに接続されるネットワーク要素は、ゲートウェイ ネットワーク要素（図 2 の GNE）によって表されます。ここでのネットワーク トポロジは、各ネットワーク要素ルータ間のポイントツーポイント リンクです。この例では、レベル 1 IS-IS ルータは NE ルータと呼ばれます。

サービスプロバイダーのセントラル オフィス（CO）のシェルフ スペースが非常に高価であるため、Cisco 2600 シリーズなどの小規模の Cisco ルータが選択されて、レベル 1-2 ルータとして実行されています。Cisco 2600 シリーズ ルータは、4 つ、または 5 つの異なるレベル 1 領域のレベル 1 ルータとして動作している場合、その処理電力が制限されます。この設定の下のレベル 1 領域の数は、約 200 に制限されています。レベル 2 ネットワーク全体も、最も遅いレベル 2 ルータの速度によって制限されます。

NE ルータ間を接続できるようにするには、インバンド シグナリングを使用します。インバンド シグナリングは、データ通信チャネル（DCC）上の SONET/Synchronous Digital Hierarchy（SDH）フレームで伝送されます。DCC は 192 KB チャネルであり、管理トラフィックが非常

に制限された量の帯域幅です。IS-IS を実行している NE ルータでは、ネットワーク要素間のシグナリング帯域幅が制限され、また、処理電力量とメモリ容量も制限されているため、各領域はルータの最大数が 30 ～ 40 に制限されます。各 SONET リングは、平均で 10 ～ 15 のネットワーク要素で構成されています。

領域あたり 10 ～ 15 のネットワーク要素を含む、最大 200 の領域により、1 つの自律システム内のネットワーク要素ルータの合計数は 3000 より少なくなる必要があります。サービス プロバイダーは、ネットワークが増大するにつれて 10,000 を超えるネットワーク要素を実装しようとしますが、1 つの領域のネットワーク要素の潜在数は制限されています。現在のソリューションは、DCN を多数のより小さい自律システムに分解し、スタティック ルートまたは ISO Interior Gateway Routing Protocol（IGRP）を使用して各システムを接続します。ISO IGRP は、将来の機器実装オプションを制限できる独自のプロトコルです。ネットワークの増大が、ネットワーク管理者のスタティック ルートを維持する能力を超える場合があるため、スタティック ルートはスケーリングしません。BGP は、100,000 ルートを超えるスケーリングを行うように示されています。

この例では、CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能を実装するために、DCN コア ネットワーク（図 2 の AS64800）の各ルータで実行する BGP を設定して、すべての自律システム間でルーティング情報を交換します。AS64600 および AS64700 の自律システムでは、レベル 2 ルータだけが BGP を実行します。BGP は TCP を使用して BGP 対応のネイバー ルータと通信します。つまり、IP アドレスのネットワークと NSAP アドレスのネットワークの両方が、自律システム AS64600 と AS64700 のすべてのレベル 2 IS-IS ルータ、および DCN コア ネットワークのすべてのルータを対象とするように設定される必要があります。

各自律システム（たとえば、図 2 の AS64600 および AS64700）が最大 3000 ノードの同じサイズのままであるとすると、この機能によってサポートできる DCN ネットワークの規模を示すことが可能です。各自律システムは、1 つのアドレス プレフィックスをコア自律システムにアドバタイズします。各自律システムとコア自律システムとの間には 2 つのリンクがあるため、各アドレス プレフィックスは、冗長性を得るために、そのリンクに 2 つのパスを関連付けできます。BGP は 100,000 のルートをサポートするように示され、各自律システムが数個のルートしか生成しないため、コア自律システムは他の多数の直接リンクされた自律システムをサポートできます。コア自律システムは、約 2000 の直接リンクされた自律システムをサポートできると考えられます。各自律システムがコア自律システムに直接リンクされて、中継自律システムとして動作していないハブ アンド スポーク設計で、コア自律システムはデフォルト ルートをリンクされた各自律システムに生成できます。デフォルト ルートを使用すると、リンクされた自律システムのレベル 2 ルータは、追加ルーティング情報を少量しか処理しません。2000 のリンクされた自律システムに、各自律システムの 3000 ノードを掛けると、最大 6,000,000 のネットワーク要素が許容されることになります。

CLNS に対する MP-BGP サポートの利点

CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能は、ルーティング ドメインをマージせずに個別の OSI ルーティング ドメインを相互接続する機能を追加することによって、大規模な OSI ネットワークを確立する機能を提供します。この機能を使用する利点は、DCN ネットワーク内に限定されるのではなく、CLNS とともに OSI ルーティング プロトコルを使用してネットワークのスケーリングを容易にするように実装できることです。

CLNS に対する MP-BGP サポートの設定方法

CLNS をサポートするための BGP ネイバーの設定とアクティブ化

BGP ルーティング プロセス、および CLNS をサポートする、関連付けられた BGP ネイバー（ピア）の設定とアクティブ化を行うには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family nsap** [**unicast**]
7. **neighbor** *ip-address* **activate**
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65101`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータが存在する自律システムを識別します。有効値は、0～65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512～65535 です。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* 例： `Router(config-router)# neighbor 10.1.2.2 remote-as 64202`	指定された自律システム内の BGP ネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。

ステップ 6	**address-family nsap** [**unicast**]
	例：
	`Router(config-router)#`
	`address-family nsap`
		NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
		• オプションの **unicast** キーワードは、NSAP ユニキャスト アドレス プレフィックスを指定します。デフォルトでは、**address-family nsap** コマンドに **unicast** キーワードが指定されていない場合、ルータはユニキャスト NSAP アドレス ファミリのコンフィギュレーション モードになります。

ステップ 7	**neighbor** *ip-address* **activate**
	例：
	`Router(config-router-af)#`
	`neighbor 10.1.2.2 activate`
		BGP ネイバーが、NSAP アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。
		（注） ピア グループを BGP ネイバーとして設定した場合は、このコマンドを使用しないでください。これは、ピア グループ パラメータの設定時にピア グループが自動的にアクティブにされるためです。

ステップ 8	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IS-IS ルーティング プロセスの設定

Integrated IS-IS ルーティング プロセスを設定する場合、最初に設定される IS-IS ルーティング プロセスのインスタンスは、デフォルトで、レベル 1-2（領域内および領域間）ルータです。CLNS を実行しているネットワーク上の、後続の IS-IS ルーティング プロセスはすべてレベル 1 として設定されます。IP を実行しているネットワーク上の、後続の IS-IS ルーティング プロセスはすべてレベル 1-2 として設定されます。CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能を使用するには、レベル 2 ルーティング プロセスを設定します。

IS-IS ルーティング プロセスを設定してレベル 2 専用のプロセスとして割り当てるには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **net** *network-entity-title*
5. **is-type** [**level-1** | **level-1-2** | **level-2-only**]
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router isis** *area-tag* 例： `Router(config)# router isis osi-as-101`	IS-IS ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • *area-tag* 引数には、ルーティング プロセスの意味のある名前を指定します。この名前は、特定のルータのすべての IP ルーティング プロセスおよびCLNSルーティング プロセスの間で一意である必要があります。
ステップ 4	**net** *network-entity-title* 例： `Router(config-router)# net 49.0101.1111.1111.1111.1111.00`	ルーティング プロセスの Network Entity Title（NET）を設定します。 • マルチエリア IS-IS を設定する場合は、各ルーティング プロセスの NET を指定する必要があります。
ステップ 5	**is-type** [**level-1**	**level-1-2**	**level-2-only**] 例： `Router(config-router)# is-type level-1`	ルータを、レベル 1（領域内）ルータ、レベル 1 ルータおよびレベル 2（領域間）ルータ、または領域内専用ルータとして設定します。

	コマンドまたはアクション	目的
		• マルチエリア IS-IS コンフィギュレーションでは、最初に設定される IS-IS ルーティング プロセスのインスタンスは、デフォルトで、レベル 1-2（領域内および領域間）ルータです。CLNS を実行しているネットワーク上の、後続の IS-IS ルーティング プロセスはすべてレベル 1 として設定されます。IP を実行しているネットワーク上の、後続の IS-IS ルーティング プロセスはすべてレベル 1-2 として設定されます。

ステップ 6	**end**
	例：
	`Router(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。

BGP ネイバーに接続するインターフェイスの設定

IS-IS を実行しているルータが直接 eBGP ネイバーに接続される場合、2 つの eBGP ネイバー間のインターフェイスは、**clns enable** コマンドを使用してアクティブになり、これにより、CLNS パケットをインターフェイス間で転送できます。**clns enable** コマンドは、End System-to-Intermediate System（ES-IS）プロトコルをアクティブにして、ネイバー OSI システムを検索します。

（注） eBGP ネイバーと接続されている同じインターフェイス間で IS-IS を実行すると、2 つの OSI ルーティング ドメインが 1 つのドメインにマージされた場合に望ましくない結果になる場合があります。

ネイバー OSI システムが検出された場合、BGP は、そのシステムが、NSAP アドレス ファミリに設定された eBGP ネイバーでもあることを確認します。前の条件が満たされた場合、BGP は、専用の BGP ネイバー ルートを CLNS レベル 2 プレフィックス ルーティング テーブルに作成します。専用の BGP ネイバー ルートはレベル 2 ルーティング アップデートに自動的に再配布され、ローカル OSI ルーティング ドメイン内の他のレベル 2 IS-IS ルータすべてが、この eBGP ネイバーへの到達方法を認識するようにします。

eBGP ネイバーとの接続に使用されているインターフェイスを設定するには、次の手順のステップを実行します。このインターフェイスは通常、eBGP ネイバーに直接接続されます。

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **clns enable**
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface serial 2/0/0`	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 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.1.2.2 255.255.255.0`	IPアドレスを使用してインターフェイスを設定します。

ステップ 5	**clns enable**
	例：
	`Router(config-if)#`
	`clns enable`
		CLNS パケットをインターフェイス間で転送できるように指定します。
		• ES-IS プロトコルがアクティブになり、隣接OSIシステムの検索が開始されます。

ステップ 6	**no shutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをオンにします。
ステップ 7	**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 モードに戻ります。

ローカル OSI ルーティング ドメインと接続されているインターフェイスの設定

ローカル OSI ルーティング ドメインと接続されているインターフェイスを設定するには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **clns router isis** *area-tag*
6. **ip router isis** *area-tag*
7. **no shutdown**
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface gigabitethernet 0/1/1`	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 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.2.3.1 255.255.255.0`	IP アドレスを使用してインターフェイスを設定します。 （注） このステップは、インターフェイスが iBGP ネイバーと通信する必要がある場合だけ必要になります。
ステップ 5	**clns router isis** *area-tag* 例： `Router(config-if)#`	ネットワーク プロトコルが ISO CLNS である場合にインターフェイスが IS-IS をアクティブにルーティングするように指定し、このルーティング プロセスに関連付けられた領域を識別します。

	コマンドまたはアクション	目的
	`clns router isis osi-as-202`	
ステップ 6	**ip router isis** *area-tag* 例： `Router(config-if)# ip router isis osi-as-202`	ネットワーク プロトコルが IP である場合にインターフェイスが IS-IS をアクティブにルーティングするように指定し、このルーティング プロセスに関連付けられた領域を識別します。 （注） このステップは、インターフェイスが iBGP ネイバーと通信する必要があり、かつ、IGP が IS-IS である場合だけ必要になります。
ステップ 7	**no shutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをオンにします。
ステップ 8	**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 モードに戻ります。

ネットワーキング プレフィックスのアドバタイジング

NSAP アドレス プレフィックスをアドバタイジングすると、プレフィックスが BGP ルーティング テーブルに強制的に追加されます。ネットワーキング プレフィックスのアドバタイズメントを設定するには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family nsap** [**unicast**]
7. **network** *nsap-prefix* [**route-map** *map-tag*]
8. **neighbor** *ip-address* **activate**
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65101`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* 例： `Router(config-router)# neighbor 10.1.2.2 remote-as 64202`	指定された自律システム内の BGP ネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。
ステップ 6	**address-family nsap** [**unicast**] 例： `Router(config-router)# address-family nsap`	NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • オプションの **unicast** キーワードは、NSAP ユニキャスト アドレス プレフィックスを指定します。デフォルトでは、**address-family nsap** コマンドに **unicast** キーワードが指定されていない場合、ルータはユニキャスト NSAP アドレス ファミリ コンフィギュレーション モードになります。
ステップ 7	**network** *nsap-prefix* [**route-map** *map-tag*] 例： `Router(config-router-af)#`	ローカル OSI ルーティング ドメインの 1 つのプレフィックスをアドバタイズし、そのプレフィックスを BGP ルーティング テーブルに入力します。

	コマンドまたはアクション	目的
	network 49.0101.1111.1111.1111.1111.00	（注） 1 つのプレフィックスをアドバタイズできるのは、そのプレフィックスが、ローカル OSI ルーティング ドメインの一意の NSAP アドレスプレフィックスである場合です。または、それぞれが OSI ルーティング ドメインの小さい部分をカバーする、より長い複数のプレフィックスを使用すると、異なる領域を選択的にアドバタイズできます。 • NSAP アドレス プレフィックスのアドバタイジングは、オプションの **route-map** キーワードを使用することで制御できます。ルートマップが指定されない場合は、すべての NSAP アドレス プレフィックスが再配布されます。
ステップ 8	**neighbor** *ip-address* **activate** 例： `Router(config-router-af) neighbor 10.1.2.2 activate`	NSAP ルーティング情報が、指定された BGP ネイバーに送信されるように指定します。 （注） このコマンドの使用の詳細については、「その他の参考資料」に示されているマニュアル内の **neighbor** コマンドの説明を参照してください。

ステップ 9	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP から IS-IS へのルートの再配布

ルート再配布を実行する場合は注意が必要です。フルセットの BGP ルートを IS-IS に挿入することは、過剰なトラフィックが IS-IS に加えられるため推奨されません。ルート マップを使用すると、再配布されるダイナミック ルートを制御できます。

BGP から IS-IS へのルート再配布を設定するには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **net** *network-entity-title*

5. **redistribute** *protocol as-number* [*route-type*] [**route-map** *map-tag*]
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router isis** *area-tag* 例： `Router(config)# router isis osi-as-404`	IS-IS ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。 （注） BGP ルートをレベル 1 専用の IS-IS ルーティング プロセスに再配布できません。
ステップ 4	**net** *network-entity-title* 例： `Router(config-router)# net 49.0404.7777.7777.7777.7777.00`	ルーティング プロセスの NET を設定します。 • マルチエリア IS-IS を設定する場合は、各ルーティング プロセスの NET を指定する必要があります。
ステップ 5	**redistribute** *protocol as-number* [*route-type*] [**route-map** *map-tag*] 例： `Router(config-router)# redistribute bgp 65404 clns`	*protocol* 引数が **bgp** に設定され、*route-type* 引数が **clns** に設定されている場合は、NSAP プレフィックス ルートを BGP から、IS-IS ルーティング プロセスに関連付けられた CLNS レベル 2 ルーティング テーブルに再配布します。 • *as-number* 引数は、CLNS に再配布される BGP ルーティング プロセスの自律システム番号として定義されます。 • ルートの再配布は、オプションの **route-map** キーワードを使用することによって制御できます。ルートマップが指定されない場合は、すべての BGP ルートが再配布されます。
ステップ 6	**end** 例：	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。

	コマンドまたはアクション	目的
	`Router(config-router)#` `end`	

IS-IS から BGP への再配布ルート

ルート再配布は、その情報がルーティングテーブルに格納されるため、注意して実行する必要があります。大容量のルーティング テーブルの場合は、ルーティング プロセスが遅くなることがあります。ルート マップを使用すると、再配布されるダイナミック ルートを制御できます。

IS-IS から BGP へのルート再配布を設定するには、次の手順のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **address-family nsap** [**unicast**]
6. **redistribute** *protocol* [*process-id*] [*route-type*] [**route-map** *map-tag*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65202`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。

	コマンドまたはアクション	目的

ステップ 5	**address-family nsap** [**unicast**]
	例：
	`Router(config-router)#`
	`address-family nsap`
		NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6	**redistribute** *protocol* [*process-id*] [*route-type*] [**route-map** *map-tag*] 例： `Router(config-router-af)# redistribute isis osi-as-202 clns route-map internal-routes-only`	*protocol* 引数が **isis** に設定され、*route-type* 引数が **clns** に設定されている場合は、IS-IS ルーティング プロセスに関連付けられた CLNS レベル 2 ルーティング テーブルから BGP に、ルートを NSAP プレフィックスとして再配布します。 • *process-id* 引数は、再配布される関連 IS-IS ルーティング プロセスの領域名として定義されます。 • ルートの再配布は、オプションの **route-map** キーワードを使用することによって制御できます。ルート マップが指定されない場合は、すべてのレベル 2 ルートが再配布されます。

ステップ 7	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP ピア グループおよびルート リフレクタの設定

BGP ピア グループは、BGP **neighbor** コマンドを複数のネイバーに適用することによって、コンフィギュレーション コマンドの数を減らします。BGP ルート リフレクタとして設定されたローカル ルータとともに BGP ピア グループを使用すると、グループの 1 つのメンバから受信された BGP ルーティング情報を他のすべてのグループ メンバに複製できます。ピア グループがない場合は、各ルート リフレクタ クライアントを IP アドレスごとに指定する必要があります。

BGP ピア グループを作成し、そのグループを BGP ルート リフレクタ クライアントとして使用するには、次の手順のステップを実行します。これは任意の作業であり、内部 BGP ネイバーで使用されます。この作業では、一部の BGP 構文が *peer-group-name* 引数だけとともに表示され、1 つだけのネイバーがピア グループのメンバとして設定されます。他の BGP ネイバーをピア グループのメンバとして設定するには、ステップ 9 を繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** *peer-group-name* **remote-as** *as-number*
7. **address-family nsap** [**unicast**]
8. **neighbor** *peer-group-name* **route-reflector-client**
9. **neighbor** *ip-address* **peer-group** *peer-group*
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65303`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Router(config-router)# neighbor ibgp-peers peer-group`	BGP ピア グループを作成します。
ステップ 6	**neighbor** *peer-group-name* **remote-as** *as-number* 例： `Router(config-router)# neighbor ibgp-peers remote-as 65303`	指定された自律システム内の BGP ネイバーのピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的

ステップ 7	**address-family nsap** [**unicast**]
	例：
	`Router(config-router)#`
	`address-family nsap`
		NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 8	**neighbor** *peer-group-name* **route-reflector-client**
	例：
	`Router(config-router-af)#`
	`neighbor ibgp-peers route-reflector-client`
		ルータを BGP ルート リフレクタとして設定し、そのクライアントとして、指定されたピア グループを設定します。

ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group*
	例：
	`Router(config-router-af)#`
	`neighbor 10.4.5.4 peer-group ibgp-peers`
		BGP ネイバーを BGP ピア グループに割り当てます。

ステップ 10	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NSAP プレフィックスに基づくインバウンド ルートのフィルタリング

NSAP プレフィックスに基づいてインバウンド BGP ルートをフィルタリングするには、この作業を実行します。インバウンド ルートをフィルタ処理するには、**neighbor prefix-list in** コマンドをアドレス ファミリ コンフィギュレーション モードで設定します。

始める前に

neighbor コマンドを設定する前に、CLNS フィルタ セットまたは CLNS フィルタ表現を指定する必要があります。詳細については、**clns filter-expr** コマンドおよび **clns filter-set** コマンドの説明を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **address-family nsap** [**unicast**]

6. **neighbor** {*ip-address*| *peer-group-name*}**prefix-list** {*clns-filter-expr-name*| *clns-filter-set-name*} **in**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65200`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。

ステップ 5	**address-family nsap** [**unicast**]
	例：
	`Router(config-router)#`
	`address-family nsap`
		アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6	**neighbor** {*ip-address*| *peer-group-name*}**prefix-list** {*clns-filter-expr-name*| *clns-filter-set-name*} **in**
	例：
	`Router(config-router-af)#`
	`neighbor 10.23.4.1 prefix-list abc in`
		インバウンド BGP ルートのフィルタリングに使用される CLNS フィルタ セットまたは CLNS フィルタリング表現を指定します。
		• *clns-filter-expr-name* 引数は、**clns filter-expr** コンフィギュレーション コマンドで定義されます。
		• *clns-filter-set-name* 引数は、**clns filter-set** コンフィギュレーション コマンドで定義されます。

ステップ 7	**end** 例： `Router(config-router-af)#`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`end`	

NSAPプレフィックスに基づくアウトバウンドBGPアップデートのフィルタリング

アドレス ファミリ コンフィギュレーション モードで **neighbor prefix-list out** コマンドを使用し、NSAPプレフィックスに基づいてアウトバウンドBGPルートをフィルタ処理するには、この作業を実行します。この作業は、上の図（「汎用BGP CLNSネットワーク トポロジ」の項）のルータ 7 で設定します。この作業では、CLNS フィルタが 2 つのエントリで作成されて、49.0404 で始まる NSAP プレフィックスを拒否し、49 で始まる他のすべての NSAP プレフィックスを許可します。BGP ピア グループが作成され、ピア グループのメンバであるネイバーのアウトバウンド BGP アップデートにフィルタが適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **clns filter-set** *name* [**deny**] **template**
4. **clns filter-set** *name* [**permit**] **template**
5. **router bgp** *as-number*
6. **no bgp default ipv4-unicast**
7. **neighbor** *peer-group-name* **peer-group**
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
9. **address-family nsap** [**unicast**]
10. **neighbor** {*ip-address* | *peer-group-name*} **prefix-list** {*clns-filter-expr-name* | *clns-filter-set-name*} **out**
11. **neighbor** *ip-address* **peer-group** *peer-group*
12. **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**clns filter-set** *name* [**deny**] **template** 例： `Router(config)# clns filter-set routes0404 deny 49.0404...`	CLNS フィルタリング表現に使用する拒否条件の NSAP プレフィックスのマッチングを定義します。 • この例では、アドレスが 49.0404 で始まる場合は拒否動作が戻ります。
ステップ 4	**clns filter-set** *name* [**permit**] **template** 例： `Router(config)# clns filter-set routes0404 permit 49...`	CLNS フィルタリング表現に使用する許可条件の NSAP プレフィックスのマッチングを定義します。 • この例では、アドレスが 49 で始まる場合は許可動作が戻ります。 （注） このステップの許可例では 49 で始まるすべての NSAP アドレスを許可しますが、ステップ 3 の一致条件が最初に処理されるため、49.0404 で始まる NSAP アドレスは引き続き拒否されます。
ステップ 5	**router bgp** *as-number* 例： `Router(config)# router bgp 65404`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 6	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。
ステップ 7	**neighbor** *peer-group-name* **peer-group** 例： `Router(config-router)# neighbor ebgp-peers peer-group`	BGP ピア グループを作成します。 • この例では、ebgp-peers という名前の BGP ピア グループが作成されます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* 例： `Router(config-router)# neighbor ebgp-peers remote-as 65303`	指定された自律システム内の BGP ネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。 • この例では、ebgp-peers という名前の BGP ピア グループが BGP ネイバー テーブルに追加されます。
ステップ 9	**address-family nsap** [**unicast**] 例：	NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-router)#` `address-family nsap`	

ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **prefix-list** {*clns-filter-expr-name* | *clns-filter-set-name*} **out**
	例：
	`Router(config-router-af)#`
	` neighbor ebgp-peers prefix-list routes0404 out`
		アウトバウンド BGP アップデートのフィルタリングに使用される CLNS フィルタ セットまたは CLNS フィルタ表現を指定します。
		• *clns-filter-expr-name* 引数は、**clns filter-expr** コンフィギュレーション コマンドで定義されます。
		• *clns-filter-set-name* 引数は、**clns filter-set** コンフィギュレーション コマンドで定義されます。
		• この例では、routes0404 という名前のフィルタ セットがステップ 3 と 4 で作成されました。

ステップ 11	**neighbor** *ip-address* **peer-group** *peer-group*
	例：
	`Router(config-router-af)#`
	`neighbor 10.6.7.8 peer-group ebgp-peers`
		BGP ネイバーを BGP ピア グループに割り当てます。

ステップ 12	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ネイバー ルーティング ドメインのデフォルト ルートの送信

ネイバー OSI ルーティング ドメインのためにローカル ルータを指すデフォルト CLNS ルートを作成するには、次の手順のステップを実行します。これは任意の作業であり、通常は外部 BGP ネイバーだけで使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **address-family nsap** [**unicast**]
6. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** map-tag]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 64803`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にします。

ステップ 5	**address-family nsap** [**unicast**]
	例：
	`Router(config-router)#`
	`address-family nsap`
		NSAP アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** map-tag]
	例：
	`Router(config-router-af)#`
	`neighbor 172.16.2.3 default-originate`
		ローカル ルータを指し、かつ、ネイバー OSI ルーティング ドメインにアドバタイズされる、デフォルト CLNS ルートを生成します。

ステップ 7	**end**
	例：
	`Router(config-router-af)#`
	`end`
		アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

CLNS に対する MP-BGP サポートの確認

コンフィギュレーションを確認するには、**show running-config** EXEC コマンドを使用します。出力例は、CLNS に対する MP-BGP サポートの実装の例 （283 ページ）にあります。CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能を確認するには、次の手順を実行します。

手順の概要

1. **show clns neighbors**
2. **show clns route**
3. **show bgp nsap unicast summary**
4. **show bgp nsap unicast**

手順の詳細

ステップ 1 show clns neighbors

このコマンドを使用して、ローカル OSI ルーティング ドメイン内の他のレベル 2 IS-IS ルータとともに、すべての必要な IS-IS 隣接をローカル ルータが作成したことを確認します。ローカル ルータに、直接接続された外部 BGP ピアがある場合、このコマンドの出力は、ES-IS 隣接の形式で、外部ネイバーが検出されたことを示します。

次に、上の図（「汎用 BGP CLNS ネットワーク トポロジ」の項）に示されているルータ R2 に表示される出力例を示します。R2 には、3 つの CLNS ネイバーがあります。R1 および R4 は、R2 と異なる自律システム内にあるノードであるため ES-IS ネイバーです。R3 は、R2 と同じ自律システム内にあるため IS-IS ネイバーです。システム ID が、各コンフィギュレーション ファイルで定義された CLNS ホスト名（r1、r3、および r4）に置き換えられることに注意してください。CLNS ホスト名を指定すると、どのシステム ID がどのホスト名に対応するか覚える必要がありません。

例：

```
Router# show clns neighbors
Tag osi-as-202:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
r1             Se2/0       *HDLC*          Up     274       IS   ES-IS
r3             Et0/1       0002.16de.8481  Up     9         L2   IS-IS
r4             Se2/2       *HDLC*          Up     275       IS   ES-IS
```

ステップ 2 show clns route

このコマンドを使用して、ローカル ルータに、ローカル OSI ルーティング ドメイン内の他の領域への計算されたルートがあることを確認します。上の図（「汎用 BGP CLNS ネットワーク トポロジ」の項）に示されているルータ R2 の次の出力例では、ルーティング テーブル エントリ i 49.0202.3333 [110/10] via R3 から、ルータ R2 がローカル OSI ルーティング ドメイン内の他のローカル IS-IS 領域に関して認識していることがわかります。

例：

```
Router# show clns route
```

```
Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor
C  49.0202.2222 [2/0], Local IS-IS Area
C  49.0202.2222.2222.2222.2222.00 [1/0], Local IS-IS NET
b  49.0101.1111.1111.1111.1111.00 [15/10]
      via r1, Serial2/0
i  49.0202.3333 [110/10]
      via r3, GigabitEthernet0/1/1
b  49.0303.4444.4444.4444.4444.00 [15/10]
      via r4, Serial2/2
B  49.0101 [20/1]
      via r1, Serial2/0
B  49.0303 [20/1]
      via r4, Serial2/2
B  49.0404 [200/1]
      via r9
i  49.0404.9999.9999.9999.9999.00 [110/10]
      via r3, GigabitEthernet0/1/1
```

ステップ 3 show bgp nsap unicast summary

このコマンドを使用して、特定のネイバーへの TCP 接続がアクティブであることを確認します。次の出力例では、ネイバーの IP アドレスに基づいて適切な行を検索します。IState/PfxRcd カラム エントリが数字（ゼロを含む）である場合、そのネイバーの TCP 接続はアクティブです。

例：

```
Router# show bgp nsap unicast summary
BGP router identifier 10.1.57.11, local AS number 65202
BGP table version is 6, main routing table version 6
5 network entries and 8 paths using 1141 bytes of memory
6 BGP path attribute entries using 360 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 5/0 prefixes, 8/0 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.2.1        4 65101      34      34        6    0    0 00:29:11        1
10.2.3.3        4 65202      35      36        6    0    0 00:29:16        3
```

ステップ 4 show bgp nsap unicast

show bgp nsap unicast コマンドを入力すると、ローカル ルータが検出された、すべての NSAP プレフィックス ルートが表示されます。上の図（「汎用 BGP CLNS ネットワーク トポロジ」の項）に示されているルータ R2 の次の出力例では、プレフィックス 49.0101 への 1 つの有効なルートが示されています。* でマーキングされている 2 つの有効なルートが、プレフィックス 49.0404 で示されています。2 番目のルートが *>i シーケンスでマーキングされ、このプレフィックスへのベスト ルートを表しています。

例：

```
Router# show bgp nsap unicast
BGP table version is 3, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0101          49.0101.1111.1111.1111.1111.00
                                                          0 65101 i
* i49.0202.2222     49.0202.3333.3333.3333.3333.00
```

```
                                                    100      0 ?
*>                  49.0202.2222.2222.2222.2222.00
                                                          32768 ?
* i49.0202.3333     49.0202.3333.3333.3333.3333.00
                                                    100      0 ?
*>                  49.0202.2222.2222.2222.2222.00
                                                          32768 ?
*> 49.0303          49.0303.4444.4444.4444.4444.00
                                                              0 65303 i
*  49.0404          49.0303.4444.4444.4444.4444.00
                                                              0 65303 65404 i
*>i                 49.0404.9999.9999.9999.9999.00
                                                    100      0 65404 i
```

CLNS に対する MP-BGP サポートのトラブルシューティング

debug bgp nsap unicast コマンドは、コンソール上に表示される BGP ルーティング プロトコルのCLNSパケットの操作に関連するさまざまなイベントに対する診断出力を有効にします。これらのコマンドは、使用時にソフトウェアが生成する出力量によってルータの性能が著しく低下するため、トラブルシューティング専用となります。これらの **debug** コマンドの使用に関する詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

CLNS に対する MP-BGP サポートの設定に関する問題をトラブルシューティングして、この手順で使用される **debug** コマンドの影響を最小化するには、次の手順を実行します。

手順の概要

1. CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能を含むシスコ ソフトウェア リリースを実行しているルータにコンソールを直接接続します。
2. **no logging console**
3. Telnet を使用して、ルータ ポートにアクセスします。
4. **enable**
5. **terminal monitor**
6. **debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
7. **no terminal monitor**
8. **no debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]
9. **logging console**

手順の詳細

ステップ 1 CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能を含むシスコ ソフトウェア リリースを実行しているルータにコンソールを直接接続します。

（注） コンソール ポートが文字ごとにプロセッサ割り込みを生成しないため、この手順により、**debug bgp nsap unicast** コマンドが作成するルータの負荷が最小化されます。直接コンソールに接続できない場合は、ターミナル サーバを介してこの手順を実行できます。ただし、Telnet 接続を切断しなければならない場合は、**debug bgp nsap unicast** 出力の生成でプロセッサに負荷がかかりルータが応答できないことに起因して、再接続できないことがあります。

ステップ 2 **no logging console**

このコマンドは、コンソール端末へのすべてのロギングをディセーブルにします。

ステップ 3 Telnet を使用して、ルータ ポートにアクセスします。

ステップ 4 **enable**

このコマンドを入力して、特権 EXEC モードにアクセスします。

ステップ 5 **terminal monitor**

このコマンドは、仮想端末へのロギングを有効にします。

ステップ 6 **debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]

特定の **debug bgp nsap unicast** コマンドだけを入力して特定のサブコンポーネントへの出力を隔離し、プロセッサの負荷を最小化します。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。

ステップ 7 **no terminal monitor**

このコマンドは、仮想端末へのロギングを無効にします。

ステップ 8 **no debug bgp nsap unicast** [*neighbor-address* | **dampening** | **keepalives** | **updates**]

終了したら、特定の **no debug bgp nsap unicast** コマンドを入力します。

ステップ 9 **logging console**

このコマンドは、コンソールへのロギングを再び有効にします。

CLNS に対する MP-BGP サポートの設定例

例：CLNS をサポートするための BGP ネイバーの設定とアクティブ化

次の例では、自律システム AS65101 のルータ R1（下の図を参照）が、BGP を実行して CLNS をサポートするためにアクティブになるように設定されています。ルータ R1 は、自律システム AS65101 ではレベル 2 IS-IS 専用ルータであり、AS65202 では、ルータ R2 を介して別の自律システムへの接続を 1 つだけ持ちます。**no bgp default ipv4-unicast** コマンドは、BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にするために、ルータで設定されます。NSAP アドレス ファミリ コンフィギュ

レーション モードが **address-family nsap** コマンドで有効化されると、ルータが 49.0101 の NSAP プレフィックスを BGP ネイバーにアドバタイズして、10.1.2.2 の BGP ネイバーに NSAP ルーティング情報を送信するように設定されます。

```
router bgp 65101
 no bgp default ipv4-unicast
 address-family nsap
  network 49.0101...
  neighbor 10.1.2.2 activate
  exit-address-family
```

例：IS-IS ルーティング プロセスの設定

次の例では、ルータ R1（下の図を参照）が IS-IS プロセスを実行するように設定されます。

```
router isis osi-as-101
 net 49.0101.1111.1111.1111.1111.00
```

デフォルトの IS-IS ルーティング プロセス レベルが使用されます。

インターフェイスの設定の例

次の例では、自律システム AS65202 のルータ R2（下の図を参照）の 2 つのインターフェイスが、CLNS を実行するように設定されています。GigabitEthernet インターフェイス 0/1/1 は、ローカル OSI ルーティング ドメインに接続されており、ネットワーク プロトコルが **clns router isis** コマンドを使用する CLNS である場合に IS-IS を実行するように設定されています。ローカル IP アドレスが 10.1.2.2 のシリアル インターフェイス 2/0 は、eBGP ネイバーに接続されており、**clns enable** コマンドで CLNS を実行するように設定されています。

```
interface serial 2/0
 ip address 10.1.2.2 255.255.255.0
 clns enable
 no shutdown
!
interface gigabitethernet 0/1/1
 ip address 10.2.3.1 255.255.255.0
 clns router isis osi-as-202
 no shutdown
```

ネットワーキング プレフィックスのアドバタイジングの例

次の例では、ルータ R1（下の図を参照）が、49.0101 の NSAP プレフィックスを他のルータにアドバタイズするように設定されています。自律システム AS65101 に対して一意の NSAP プレフィックスがアドバタイズされることにより、他の自律システムは、ネットワーク内に自律システム AS65101 の存在を検出できます。

```
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 64202
 address-family nsap
```

```
 network 49.0101...
 neighbor 10.1.2.2 activate
```

例：BGP から IS-IS へのルートの再配布

次の例では、自律システム AS65404 のルータ R7 および R9（下の図を参照）が、osi-as-404 と呼ばれる IS-IS ルーティング プロセスに BGP ルートを再配布するように設定されています。BGP ルートの再配布により、レベル 2 IS-IS ルータの R8 は、自律システム AS65404 の外部の宛先にルートをアドバタイズできるようになります。ルートマップが指定されない場合は、すべての BGP ルートが再配布されます。

ルータ R7

```
router isis osi-as-404
 net 49.0404.7777.7777.7777.7777.00
 redistribute bgp 65404 clns
```

ルータ R9

```
router isis osi-as-404
 net 49.0404.9999.9999.9999.9999.00
 redistribute bgp 65404 clns
```

例：IS-IS から BGP への再配布ルート

次の例では、自律システム AS65202 のルータ R2（下の図を参照）が、レベル 2 CLNS NSAP を BGP に再配布するように設定されています。ルート マップを使用して、BGP に再配布されるローカル自律システム内からのルートだけを許可します。ルート マップを指定しない場合は、CLNS レベル 2 プレフィックス テーブルから、すべての NSAP ルートが再配布されます。**no bgp default ipv4-unicast** コマンドは、BGP ネイバー ルータとの間で IPv4 アドレッシング情報を交換する BGP ルーティング プロセスのデフォルト動作を無効にするために、ルータで設定されます。

```
clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
 match clns address internal-routes
!
router isis osi-as-202
 net 49.0202.2222.2222.2222.2222.00
!
router bgp 65202
 no bgp default ipv4-unicast
 address-family nsap
 redistribute isis osi-as-202 clns route-map internal-routes-only
```

BGP ピア グループおよびルート リフレクタの設定の例

上の図（「汎用 BGP CLNS ネットワーク トポロジ」の項）のルータ R5 は iBGP ネイバーだけを持ち、両方のインターフェイスで IS-IS を実行します。コンフィギュレーション コマンドの数を減らすには、ibgp-peers と呼ばれる BGP ピア グループのメンバとして R5 を設定します。ピア グループをグループ メンバ間で NSAP ルーティング情報を交換できるようにするルート リフレクタ クライアントとして設定することによって、ピア グループは **address-family nsap** コマンド下で自動的にアクティブになります。BGP ピア グループは、すべての BGP ルータを相互にリンクする必要性を少なくする BGP ルート リフレクタ クライアントとしても設定されます。

次の例では、自律システム AS65303 のルータ R5 が、BGP ピア グループのメンバおよび BGP ルート リフレクタ クライアントとして設定されます。

```
router bgp 65303
 no bgp default ipv4-unicast
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 65303
 address-family nsap
  neighbor ibgp-peers route-reflector-client
  neighbor 10.4.5.4 peer-group ibgp-peers
  neighbor 10.5.6.6 peer-group ibgp-peers
  exit-address-family
```

NSAP プレフィックスに基づくインバウンド ルートのフィルタ処理の例

次の例では、自律システム AS65101 のルータ R1（下の図を参照）が、デフォルト プレフィックス専用のプレフィックス リストで指定されたインバウンド ルートをフィルタ処理するように設定されます。

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router isis osi-as-101
 net 49.0101.1111.1111.1111.1111.00
!
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 64202
 address-family nsap
  network 49.0101.1111.1111.1111.1111.00
  neighbor 10.1.2.2 activate
  neighbor 10.1.2.2 prefix-list default-prefix-only in
```

例：NSAP プレフィックスに基づくアウトバウンド BGP アップデートのフィルタ処理

次の例では、アウトバウンド BGP アップデートが NSAP プレフィックスに基づいてフィルタリングされます。この例は、下の図のルータ 7 で設定されます。この作業では、CLNS フィル

タが 2 つのエントリで作成されて、49.0404 で始まる NSAP プレフィックスを拒否し、49 で始まる他のすべての NSAP プレフィックスを許可します。BGP ピア グループが作成され、ピア グループのメンバであるネイバーのアウトバウンド BGP アップデートにフィルタが適用されます。

```
clns filter-set routes0404 deny 49.0404...
clns filter-set routes0404 permit 49...
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor ebgp-peers remote-as 65303
 address-family nsap
   neighbor ebgp-peers prefix-list routes0404 out
   neighbor 10.6.7.8 peer-group ebgp-peers
```

例：デフォルト ルートの発信およびアウトバウンド ルート フィルタリング

下の図では、自律システム AS65101 は他の 1 つの自律システム AS65202 だけに接続されています。AS65202 のルータ R2 は、デフォルト ルートを R1 に送信することによって、自律システム AS65101 の残りのネットワークと接続します。ローカル レベル 1 ネットワークの外部の宛先 NSAP アドレスを持ち、自律システム AS65101 内にあるレベル 1 ルータからのパケットは、レベル 2 ルータに最も近い R1 に送信されます。ルータ R1 は、デフォルト ルートを使用してパケットをルータ R2 に転送します。

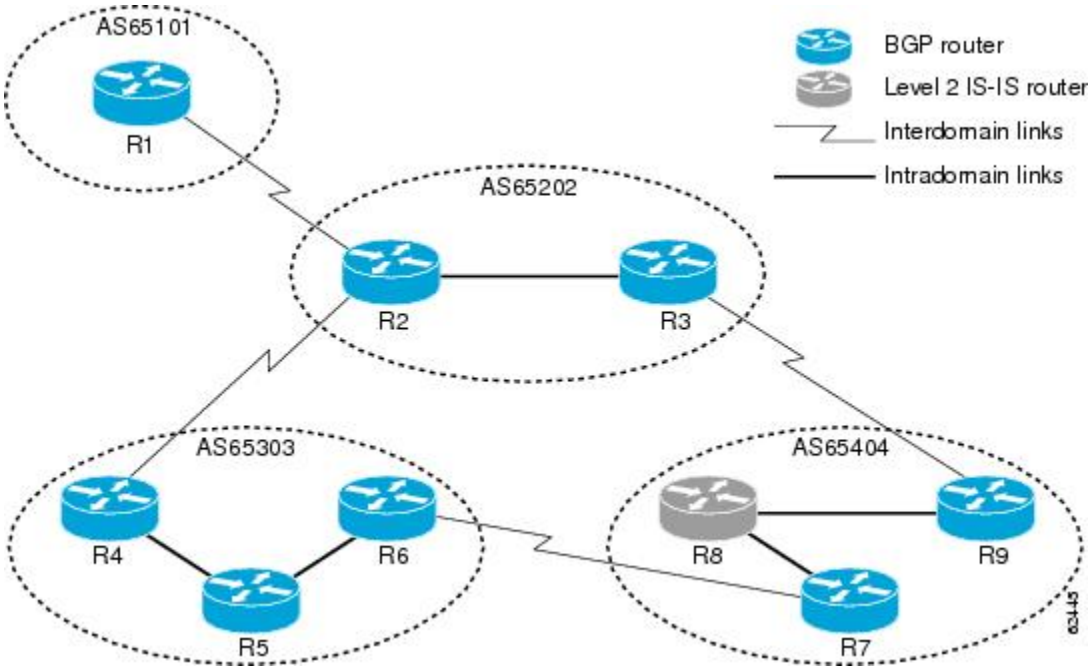
次の例では、自律システム AS65202 のルータ R2（下の図を参照）が、自律システム AS65101 のルータ R1 のデフォルト ルートを生成するように設定され、アウトバウンド フィルタが作成されて、BGP アップデート メッセージ内のデフォルト ルート NSAP アドレッシング情報だけをルータ R1 に送信します。

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 no bgp default ipv4-unicast
 neighbor 10.1.2.1 remote-as 64101
 address-family nsap
  network 49.0202...
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
  neighbor 10.1.2.1 prefix-list default-prefix-only out
```

CLNS に対する MP-BGP サポートの実装の例

下の図に、4 つの異なる自律システム（BGP 用語）またはルーティング ドメイン（OSI 用語）にグループ分けされる 9 つのルータを含む汎用 BGP CLNS ネットワークを示します。この項では、下の図に示されている全ルータのすべてのコンフィギュレーションについて記述します。

図 *21* : 汎用 *BGP CLNS* ネットワークのコンポーネント



次の例で使用されるコマンドについての詳細が必要な場合は、このマニュアルおよびその他の参考資料（289 ページ）に示される資料のコンフィギュレーション作業を参照してください。

自律システム AS65101

ルータ 1

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router isis osi-as-101
 net 49.0101.1111.1111.1111.1111.00
!
router bgp 65101
 no bgp default ipv4-unicast
 neighbor 10.1.2.2 remote-as 65202
 address-family nsap
  neighbor 10.1.2.2 activate
  neighbor 10.1.2.2 prefix-list default-prefix-only in
  network 49.0101...
  exit-address-family
!
interface serial 2/0
 ip address 10.1.2.1 255.255.255.0
 clns enable
 no shutdown
```

自律システム AS65202

ルータ 2

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
  match clns address internal-routes
!
router isis osi-as-202
  net 49.0202.2222.2222.2222.2222.00
!
router bgp 65202
  no bgp default ipv4-unicast
  neighbor 10.1.2.1 remote-as 65101
  neighbor 10.2.3.3 remote-as 65202
  neighbor 10.2.4.4 remote-as 65303
  address-family nsap
    neighbor 10.1.2.1 activate
    neighbor 10.2.3.3 activate
    neighbor 10.2.4.4 activate
    redistribute isis osi-as-202 clns route-map internal-routes-only
    neighbor 10.1.2.1 default-originate
    neighbor 10.1.2.1 prefix-list default-prefix-only out
    exit-address-family
!
interface gigabitethernet 0/1/1
  ip address 10.2.3.2 255.255.255.0
  clns router isis osi-as-202
  no shutdown
!
interface serial 2/0
  ip address 10.1.2.2 255.255.255.0
  clns enable
  no shutdown
!
interface serial 2/2
  ip address 10.2.4.2 255.255.255.0
  clns enable
  no shutdown
```

ルータ 3

```
clns filter-set internal-routes permit 49.0202...
!
route-map internal-routes-only permit 10
  match clns address internal-routes
!
router isis osi-as-202
 net 49.0202.3333.3333.3333.3333.00
!
router bgp 65202
 no bgp default ipv4-unicast
 neighbor 10.2.3.2 remote-as 65202
 neighbor 10.3.9.9 remote-as 65404
 address-family nsap
  neighbor 10.2.3.2 activate
```

```
  neighbor 10.3.9.9 activate
  redistribute isis osi-as-202 clns route-map internal-routes-only
  exit-address-family
!
interface gigabitethernet 0/1/1
 ip address 10.2.3.3 255.255.255.0
 clns router isis osi-as-202
 no shutdown
!
interface serial 2/2
 ip address 10.3.9.3 255.255.255.0
 clns enable
 no shutdown
```

自律システム AS65303

ルータ 4

```
router isis osi-as-303
 net 49.0303.4444.4444.4444.4444.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor 10.2.4.2 remote-as 65202
 neighbor 10.4.5.5 remote-as 65303
 address-family nsap
  no synchronization
  neighbor 10.2.4.2 activate
  neighbor 10.4.5.5 activate
  network 49.0303...
  exit-address-family
!
interface gigabitethernet 0/2/1
 ip address 10.4.5.4 255.255.255.0
 clns router isis osi-as-303
 no shutdown
!
interface serial 2/3
 ip address 10.2.4.4 255.255.255.0
 clns enable
 no shutdown
```

ルータ 5

```
router isis osi-as-303
 net 49.0303.5555.5555.5555.5555.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 65303
 address-family nsap
  no synchronization
  neighbor ibgp-peers route-reflector-client
  neighbor 10.4.5.4 peer-group ibgp-peers
  neighbor 10.5.6.6 peer-group ibgp-peers
  exit-address-family
!
interface gigabitethernet 0/2/1
 ip address 10.4.5.5 255.255.255.0
```

```
 clns router isis osi-as-303
 no shutdown
!
interface gigabitethernet 0/3/1
 ip address 10.5.6.5 255.255.255.0
 clns router isis osi-as-303
 no shutdown
```

ルータ 6

```
router isis osi-as-303
 net 49.0303.6666.6666.6666.6666.00
!
router bgp 65303
 no bgp default ipv4-unicast
 neighbor 10.5.6.5 remote-as 65303
 neighbor 10.6.7.7 remote-as 65404
 address-family nsap
  no synchronization
  neighbor 10.5.6.5 activate
  neighbor 10.6.7.7 activate
  network 49.0303...
!
interface gigabitethernet 0/3/1
 ip address 10.5.6.6 255.255.255.0
 clns router isis osi-as-303
 no shutdown
!
interface serial 2/2
 ip address 10.6.7.6 255.255.255.0
 clns enable
 no shutdown
```

自律システム AS65404

ルータ 7

```
clns filter-set external-routes deny 49.0404...
clns filter-set external-routes permit 49...
!
route-map noexport permit 10
  match clns address external-routes
  set community noexport
!
router isis osi-as-404
 net 49.0404.7777.7777.7777.7777.00
 redistribute bgp 404 clns
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor 10.6.7.6 remote-as 65303
 neighbor 10.8.9.9 remote-as 65404
 address-family nsap
  neighbor 10.6.7.6 activate
  neighbor 10.8.9.9 activate
  neighbor 10.8.9.9 send-community
  neighbor 10.8.9.9 route-map noexport out
  network 49.0404...
!
interface gigabitethernet 1/0/1
```

```
 ip address 10.7.8.7 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
!
interface serial 2/3
 ip address 10.6.7.7 255.255.255.0
 clns enable
 no shutdown
```

ルータ 8

```
router isis osi-as-404
 net 49.0404.8888.8888.8888.8888.00
!
interface gigabitethernet 1/0/1
 ip address 10.7.8.8 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
!
interface gigabitethernet 1/1/1
 ip address 10.8.9.8 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
```

ルータ 9

```
clns filter-set external-routes deny 49.0404...
clns filter-set external-routes permit 49...
!
route-map noexport permit 10
  match clns address external-routes
  set community noexport
!
router isis osi-as-404
 net 49.0404.9999.9999.9999.9999.00
 redistribute bgp 404 clns
!
router bgp 65404
 no bgp default ipv4-unicast
 neighbor 10.3.9.3 remote-as 65202
 neighbor 10.7.8.7 remote-as 65404
 address-family nsap
  network 49.0404...
  neighbor 10.3.9.3 activate
  neighbor 10.7.8.7 activate
  neighbor 10.7.8.7 send-community
  neighbor 10.7.8.7 route-map noexport out
!
interface serial 2/3
 ip address 10.3.9.9 255.255.255.0
 clns enable
 no shutdown
!
interface gigabitethernet 1/1/1
 ip address 10.8.9.9 255.255.255.0
 clns router isis osi-as-404
 ip router isis osi-as-404
 no shutdown
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

CLNSに対するMP-BGPサポート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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *22 : CLNS* に対する *MP-BGP* サポートに関する機能情報

機能名	リリース	機能情報
CLNS に対するマルチプロトコル BGP（MP-BGP）サポート	Cisco IOS XE Release 2.6	

機能名	リリース	機能情報
		CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能により、コネクションレス型ネットワーク サービス（CLNS）ネットワークをスケーリングする機能が提供されます。ボーダー ゲートウェイ プロトコル（BGP）のマルチプロトコル拡張は、ルーティング ドメインをマージせずに個別の開放型システム間相互接続（OSI）ルーティング ドメインを相互接続する機能を追加することによって、大規模な OSI ネットワークを確立する機能を実現します。 この機能により、次のコマンドが導入または変更されました。 • **address-family nsap** • **clear bgp nsap** • **clear bgp nsap dampening** • **clear bgp nsap external** • **clear bgp nsap flap-statistics** • **clear bgp nsap peer-group** • **debug bgp nsap** • **debug bgp nsap dampening** • **debug bgp nsap updates** • **neighbor prefix-list** • **network (BGP and multiprotocol BGP)** • **redistribute (BGP to ISO ISIS)** • **redistribute (ISO ISIS to BGP)** • **show bgp nsap** • **show bgp nsap community** • **show bgp nsap community-list** • **show bgp nsap dampened-paths** • **show bgp nsap filter-list** • **show bgp nsap flap-statistics** • **show bgp nsap inconsistent-as** • **show bgp nsap neighbors** • **show bgp nsap paths** • **show bgp nsap quote-regexp** • **show bgp nsap regexp**

機能名	リリース	機能情報
		• **show bgp nsap summary**

用語集

address family ：ネットワーク アドレスの共通形式を共有するネットワーク プロトコルのグループ。アドレス ファミリは RFC 1700 で定義されています。

AS ：自律システム。独立した独自のルーティング ポリシーを持ち、単一権限によって管理されるルーティング ドメインを表す IP 用語です。OSI 用語「ルーティング ドメイン」に相当します。

BGP ：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとの間で到着可能性情報を交換するドメイン間ルーティング プロトコルです。

CLNS ：Connectionless Network Service（コネクションレス型ネットワーク サービス）。OSI ネットワーク層プロトコルです。

CMIP ：Common Management Information Protocol（共通管理情報プロトコル）。OSI で、異種ネットワークのモニタリングと制御のために ISO によって作成および標準化されるネットワーク管理プロトコルです。

DCC ：Data Communications Channel（データ通信チャネル）。

DCN ：Data Communications Network（データ通信ネットワーク）。

ES-IS ：End System-to-Intermediate System。エンド システム（ホスト）が自身を中継システム（ルータ）にアナウンスする方法を定義する OSI プロトコルです。

FTAM ：File Transfer, Access, and Management。OSI で、さまざまなタイプのコンピュータ間でのネットワーク ファイルの交換と管理用に開発されたアプリケーション層プロトコルです。

IGP ：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報を交換するために使用されるインターネット プロトコルです。

IGRP ：Interior Gateway Routing Protocol。大規模な異種ネットワークのルーティングに関連する問題を解決するために開発されたシスコ独自のプロトコルです。

IS ：Intermediate System（中継システム）。OSI ネットワーク内のルーティング ノードです。

IS-IS ：Intermediate System-to-Intermediate System。DECnet Phase V ルーティングに基づく OSI リンクステート階層型ルーティング プロトコルであり、ルータはこれを使用して、ネットワーク トポロジを決定するために、1 つのメトリックに基づいてルーティング情報を交換します。

ISO ：国際標準化機構。ネットワーキングに関連する標準を含む、広範囲の標準を策定する国際組織。ISO は、著名なネットワーキング参照モデルである開放型システム間相互接続（OSI）参照モデルを開発しました。

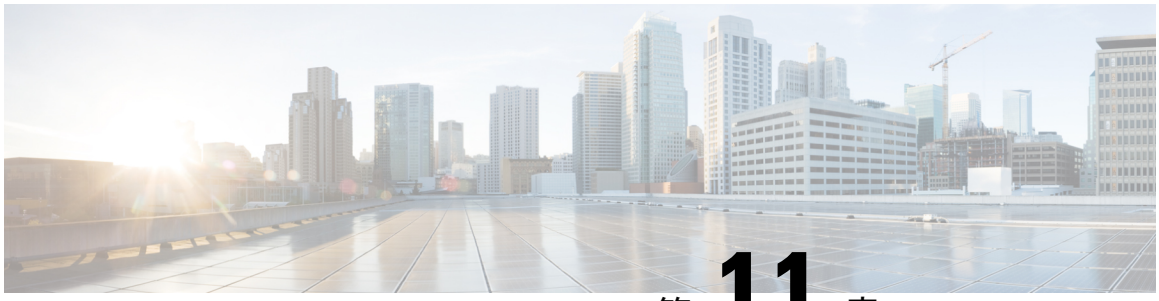
NSAP address ：Network Services Access Point（ネットワーク サービス アクセス ポイント）アドレス。OSI ネットワークによって使用されるネットワーク アドレス形式です。

OSI：Open System Interconnection（オープン システム相互接続）。マルチベンダー機器の相互運用性の向上を目指すデータ ネットワーキングの規格を作るために、ISO と ITU-T が作成した国際標準プログラムです。

routing domain：BGP の自律システムに相当する OSI 用語。

SDH：Synchronous Digital Hierarchy（同期デジタル階層）。一連のレートを定義する規格、また、光信号を使用して光ファイバで送信される形式規格です。

SONET：同期光ネットワーク。光ファイバ上で稼働するように設計された高速同期ネットワーク仕様です。



第 11 章

BGP IPv6 アドミニストレーティブ ディスタンス

BGP IPv6 アドミニストレーティブ ディスタンス機能では、ルートの送信元固有の距離を設定し、プレフィックス リストをルートに関連付けることによって、ネットワーク内の BGP IPv6 ルートに優先順位を付けることができます。RIB では、この送信元からの距離を使用して、ネットワーク内の BGP IPv6 ルートの優先順位を決定します。

- BGP IPv6 アドミニストレーティブ ディスタンスの概要 （295 ページ）
- BGP IPv6 アドミニストレーティブ ディスタンスの設定 （296 ページ）
- BGP IPv6 アドミニストレーティブ ディスタンスに関する追加情報 （298 ページ）
- BGP IPv6 アドミニストレーティブ ディスタンスの機能情報 （298 ページ）

BGP IPv6 アドミニストレーティブ ディスタンスの概要

BGP IPv6 アドミニストレーティブ ディスタンス機能は、RIB での BGP ルートの優先順位付けによって、設定されたプレフィックスに対してルート パスを選択できるようにします。RIB で提供される BGP ルートは、送信元からの設定された距離に基づいて優先順位付けされます。BGP IPv6 アドミニストレーティブ ディスタンス機能により、送信元からの距離を設定でき、ルートをプレフィックス リストに関連付けることができます。その後、送信元固有の距離とプレフィックス リストが設定されたルートを RIB で利用して、BGP IPv6 ルートに優先順位を付けることができます。

BGP IPv6 アドミニストレーティブ ディスタンスの利点

BGP IPv6 アドミニストレーティブ ディスタンス機能を使用すると、ネットワーク内の BGP IPv6 ルートの優先順位を指定または解除できます。

BGP IPv6 アドミニストレーティブ ディスタンスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **router bgp***autonomous-system-number*
5. **address-family ipv6 unicast**
6. **distance** *admin-distance ipv6-address/prefix prelengthinterface nameprefix-list*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6ユニキャストデータグラムの転送を有効にします。
ステップ 4	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 5`	ルータと他の BGP ルータを区別し、渡されたルーティング情報にタグを付ける自律システムの番号を指定します。 • 有効な範囲は 1 ～ 65535 です。
ステップ 5	**address-family ipv6 unicast** 例： `Device(config-router)# address-family ipv6 unicast`	ルーティングセッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**distance** *admin-distance ipv6-address/prefix prelengthinterface nameprefix-list* 例：	BGPルートの送信元固有の距離を設定するために、アドミニストレーティブディスタンス、IPv6アドレス、プレフィックス長、およびプレフィックスリスト名を指定します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# distance 12 2001:DB8:0:CC00::1/128 list1`	インターフェイス名はオプションで、ネイバーアドレスがリンクローカルアドレスである場合にのみ必要です。
ステップ 7	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP アドミニストレーティブ ディスタンス設定の確認

show run sec bgp コマンドを使用して、BGP 設定を確認します。

```
Device(config-device-af)# show run | sec bgp
router bgp 200
bgp log-neighbor-changes
neighbor FE80::A8BB:CCFF:FE02:BE01%Ethernet0/0 remote-as 200
neighbor FE80::A8BB:CCFF:FE02:BE01%Ethernet0/0 update-source Ethernet0/0
!
address-family ipv4
  no neighbor FE80::A8BB:CCFF:FE02:BE01%Ethernet0/0 activate
exit-address-family
!
address-family ipv6
  distance 90 FE80::A8BB:CCFF:FE02:BE01/128 interface Ethernet0/0
  network 1:1:1:1::/120
  neighbor FE80::A8BB:CCFF:FE02:BE01%Ethernet0/0 activate
exit-address-family
```

do show ipv6 route コマンドを使用して、IPv6 ルート設定を確認します。

```
Device(config-device-af)# show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
       lA - LISP away, a - Application
C   1:1:1:1::/120 [0/0]
     via Ethernet0/0, directly connected
L   1:1:1:1::2/128 [0/0]
     via Ethernet0/0, receive
B   3:4:5:6::1/128 [90/0]
     via FE80::A8BB:CCFF:FE02:BF01, Ethernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

BGP IPv6 アドミニストレーティブ ディスタンスに関する追加情報

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』
Cisco IOS IP ルーティング：BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

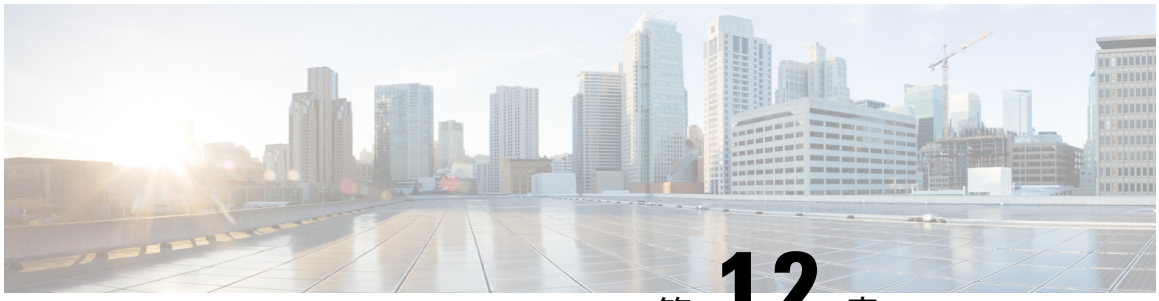
BGP IPv6 アドミニストレーティブ ディスタンスの機能情報

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

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

表 *23 : ASR1K NPTv6* の機能情報

機能名	リリース	機能の設定情報
BGP IPv6 アドミニストレーティブ ディスタンス	Cisco IOS XE Denali 16.3.1	BGP IPv6 アドミニストレーティブ ディスタンス機能では、ルートの送信元固有の距離を設定し、プレフィックス リストをルートに関連付けることによって、ネットワーク内の BGP IPv6 ルートに優先順位を付けることができます。RIB では、この送信元からの距離を使用して、ネットワーク内の BGP IPv6 ルートの優先順位を決定します。 次のコマンドが変更されました。 **distance**



第 12 章

外部BGPを使用したサービスプロバイダーとの接続

このモジュールでは、ボーダー ゲートウェイ プロトコル（BGP）ネットワークが、インターネットサービスプロバイダー（ISP）など外部ネットワークにあるピアデバイスへアクセスできるようにするための設定作業について説明します。BGPは、組織間にループのないルーティングを提供するために設計されたドメイン間ルーティングプロトコルです。異なる自律システムのピアとのルーティングアップデートの交換のために、外部BGP（eBGP）ピアリングセッションが設定されます。トラフィックのフィルタリングのためのBGPポリシー設定作業など、インバウンドとアウトバウンドのトラフィックを管理するための作業について説明します。サービスプロバイダーへの接続に冗長性を持たせるためのマルチホーミングについても説明します。

- 機能情報の確認 （301 ページ）
- 外部 BGP を使用したサービス プロバイダーとの接続の前提条件 （302 ページ）
- 外部BGP を使用したサービスプロバイダーとの接続の制約事項 （302 ページ）
- 外部 BGP を使用したサービス プロバイダーとの接続の概要 （302 ページ）
- 外部 BGP を使用したサービス プロバイダーとの接続方法 （315 ページ）
- 外部 BGP を使用したサービス プロバイダーとの接続の設定例 （375 ページ）
- 次の作業 （385 ページ）
- その他の参考資料 （385 ページ）
- 外部 BGP を使用したサービス プロバイダーとの接続の機能情報 （387 ページ）

機能情報の確認

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

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

外部BGPを使用したサービスプロバイダーとの接続の前提条件

- サービス プロバイダーとの接続前に、BGP プロセスとピアの基本的な設定方法を理解しておく必要があります。詳細については、「Cisco BGP 概要」モジュールおよび「基本 BGP ネットワークの設定」モジュールを参照してください。
- ネットワークをサービス プロバイダーに接続する場合に BGP 機能を設定する際、この章の作業と概念が役立ちます。インターネットへの接続それぞれについて、インターネット割り当て番号局（IANA）から割り当てられた自律システム番号を持っている必要があります。

外部BGP を使用したサービスプロバイダーとの接続の制約事項

- Cisco IOS ソフトウェアを実行するルータは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスと自律システムでは、複数のアドレス ファミリ設定をサポートできます。
- ポリシー リストは、Cisco IOS Release 12.0(22)S および 12.2(15)T よりも前のバージョンの Cisco IOS ソフトウェアではサポートされていません。古いバージョンの Cisco IOS ソフトウェアを実行中のルータをリロードすると、ルーティング ポリシーの設定の一部が失われることがあります。

外部BGPを使用したサービスプロバイダーとの接続の概要

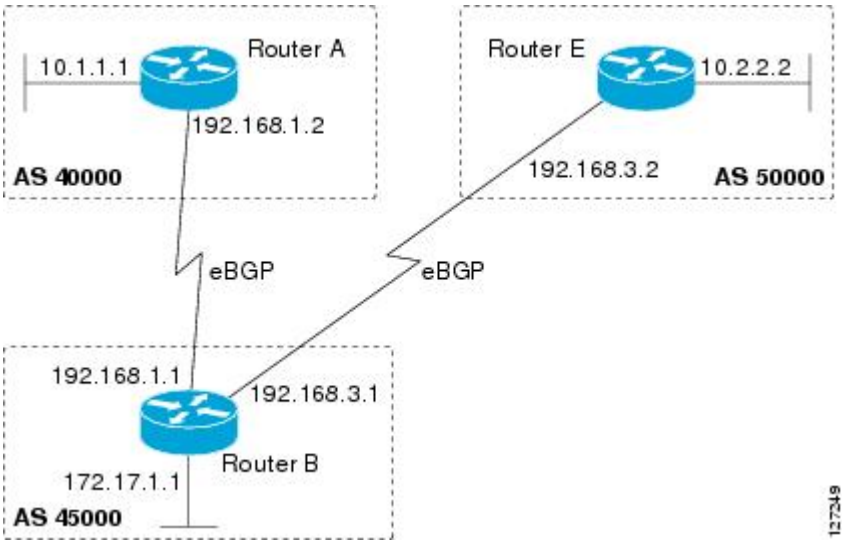
外部 BGP ピアリング

BGP は、組織間にループが発生しないルーティング リンクを実現することを目的としたドメイン間ルーティング プロトコルです。BGP は、信頼できるトランスポート プロトコル上で運用するよう設計され、トランスポート プロトコルとして TCP（ポート 179）を使用します。宛先の TCP ポートは 179 が割り当てられ、ローカル ポートではランダムなポート番号が割り当

てられます。Cisco IOS ソフトウェアは、ISP がインターネット構築に使用している BGP バージョン 4 をサポートしています。RFC 1771 では、プロトコルをインターネット規模での使用に合わせるため、新機能の BGP への追加や検討が多数行われました。

異なる自律システムの BGP ピアとのルーティング アップデートの交換のために、外部 BGP ピアリング セッションが設定されます。BGP ルーティング プロセスは、eBGP ピアが WAN 接続などによって直接接続されるものとして設計されています。しかし、実際の使用においてはこのルールではルーティングできないケースが多々あります。マルチホップ ネイバーのピアリング セッションは **neighbor ebgp-multihop** コマンドで設定します。下の図に、3 つのルータ間のシンプルな eBGP ピアリングを示します。ルータ B は、ルータ A とルータ E にピアリングされています。非常にシンプルなネットワーク設計ですが、下の図では、ルータ A とルータ E との間のピアリング確立に **neighbor ebgp-multihop** コマンドを使用できます。BGP はネットワーク内のネクスト ホップについての情報を NEXT_HOP 属性を使用して転送します。デフォルトでは eBGP ピアリング セッション内のルートをアドバタイズするインターフェイスの IP アドレスに設定されています。発信元インターフェイスは、物理インターフェイスかループバック インターフェイスです。

図 *22 :* 別の自律システム内の *BGP* ピア



eBGP ピアリング セッションの確立にはループバック インターフェイスが好まれます。ループバック インターフェイスの方がインターフェイス フラッピングの影響を受けにくいからです。ネットワーキング デバイスのインターフェイスは、障害が発生したり、メンテナンスのために運転を停止する場合があります。障害やメンテナンスのために管理上あるインターフェイスを起動や停止することを、フラップといいます。ループバック インターフェイスは安定した発信元インターフェイスを実現するもので、IP ルーティング プロトコルがループバック インターフェイスに割り当てられたサブネットをアドバタイズする限り、発信元インターフェイスに割り当てられた IP アドレスがいつでも到達可能になるようにします。ループバック インターフェイスにより、/32 ビット マスクのアドレス 1 つを設定することで、アドレス空間を節約できます。ループバック インターフェイスを eBGP ピアリング セッションのために設定する前に、**neighbor update-source** コマンドを設定してループバック インターフェイスを指定する必要があります。このように設定することで、ループバック インターフェイスが発信元インターフェ

イスとなり、その IP アドレスがこのループバックを通してアドバタイズされるルートのネクスト ホップとしてアドバタイズされます。ループバック インターフェイスをシングルホップ eBGP ピアの接続に使用する場合、事前に **neighbor disable-connected-check** コマンドを設定しておかないと、eBGP ピアリング セッションは確立できません。

外部ネットワークへの接続によって、自分のネットワークから他のネットワークへ、またインターネットを介して、トラフィックを転送できます。ネットワークに入ってくるトラフィックや、場合によっては通過して行くトラフィックもあるでしょう。BGPには、ネットワークへのトラフィックの出入りを変化させたり、インバウンドとアウトバウンドのトラフィックのフィルタリング用 BGP ポリシーを作成したりするための、さまざまな方法が含まれています。トラフィック フローを変化させるのに、BGP はアップデート メッセージに含まれる、または BGP ルーティング アルゴリズムで使用される BGP 属性を使用します。トラフィックのフィルタリング用 BGP ポリシーでは、ルート マップ、AS-path アクセス リストなどのアクセス リスト、フィルタ リスト、ポリシー リスト、および配信リストを伴った BGP 属性の一部も使用されます。バックアップやパフォーマンス向上のために 1 つの ISP への複数接続や複数の ISP への接続が存在する場合、外部接続の管理にマルチホーミング技術が関係してくることがあります。自律システムや物理的境界を超えてさまざまなコミュニティ属性によるタギングを BGP ルートに行うことで、個別に permit 文や deny 文を羅列した巨大なリストを扱わずにすみます。

BGP 自律システム番号の形式

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

asdot だけを使用する自律システム番号形式

Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースでは、4 オクテット（4 バイト）の自律システム番号は asdot 表記法だけで入力および表示されます。たとえば、1.10 または 45000.64000 です。4 バイト自律システム番号のマッチングに正規表現を使用する場合、asdot 形式には正規表現で特殊文字となるピリオドが含まれていることに注意します。正規表現でのマッチングに失敗しないよう、1\.14 のようにピリオドの前にバックスラッシュを入力

する必要があります。次の表は、asdot 形式だけが使用できる Cisco IOS イメージで、2 バイトおよび 4 バイト自律システム番号の設定、正規表現とのマッチング、および **show** コマンド出力での表示に使用される形式をまとめたものです。

表 *24 : asdot* だけを使用する *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

asplain をデフォルトとする自律システム番号形式

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコ実装の 4 バイト自律システム番号で asplain がデフォルトの自律システム番号表示形式として使用されていますが、4 バイト自律システム番号は asplain および asdot 形式のどちらにも設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力を変更して、4 バイトの自律システム番号を asdot 形式で表示する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。**show** コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト自律システム番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドを有効にした後、**clear ip bgp *** コマンドを入力してすべての BGP セッションに対してハード リセットを開始する必要があります。

（注） 4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

表 *25 : asplain* をデフォルトとする *4* バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295

書式	設定形式	showコマンド出力および正規表現のマッチング形式
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295

表 *26 : asdot* を使用する *4* バイト自律システム番号形式

書式	設定形式	showコマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 655354 バイト：65536 ～ 4294967295	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 655354 バイト：1.0 ～ 65535.65535

予約済みおよびプライベートの自律システム番号

Cisco IOS Release 12.0(32)S12、12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、12.4(24)T、およびそれ以降のリリースでは、RFC 4893 がシスコの BGP 実装でサポートされています。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。新しい予約済み（プライベート）自律システム番号（23456）は RFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を自律システム番号として設定できません。

RFC 5398『*Autonomous System (AS) Number Reservation for Documentation Use*』では、文書化を目的として新たに予約された自律システム番号について説明されています。予約済み番号を使用することで、設定例を正確に文書化しつつ、その設定がそのままコピーされた場合でも製品ネットワークに競合が発生することを防止できます。予約済み番号はIANA 自律システム番号レジストリに記載されています。予約済み 2 バイト自律システム番号は 64496 ～ 64511 の連続したブロック、予約済み 4 バイト自律システム番号は 65536 ～ 65551 をその範囲としています。

64512 ～ 65534 を範囲とするプライベートの 2 バイト自律システム番号は依然有効で、65535 は特殊な目的のために予約されています。プライベート自律システム番号は内部ルーティングドメインで使用できますが、インターネットにルーティングされるトラフィックについては変換が必要です。プライベート自律システム番号を外部ネットワークへアドバタイズするように BGP を設定しないでください。Cisco IOS ソフトウェアは、デフォルトではルーティング アップデートからプライベート自律システム番号を削除しません。ISP がプライベート自律システム番号をフィルタリングすることを推奨します。

（注） パブリック ネットワークおよびプライベート ネットワークに対する自律システム番号の割り当ては、IANA が管理しています。予約済み番号の割り当てや自律システム番号の登録申込など、自律システム番号についての情報については、http://www.iana.org/ を参照してください。

BGP 属性

BGPはデフォルトで、宛先ホストまたはネットワークへのベストパスとして、1つだけパスを選択します。どのルートをベストパスとしてBGPルーティング テーブルにインストールするかを決定するために、ベストパス選択アルゴリズムはパスの属性を分析します。それぞれのパスには、BGP ベスト パス分析で使用されるさまざまな属性がついています。Cisco IOS ソフトウェアは、コマンドライン インターフェイス（CLI）を通してそのような属性を変更することで、BGP パス選択に影響を与えられるようになっています。BGP パス選択はまた、標準 BGP ポリシー設定によっても変化させることができます。

BGP では、ベスト パス選択アルゴリズムを使用して、全体的に良好なルートのセットを検索します。このようなルートは、潜在的なマルチパスです。Cisco IOS Release 12.2(33)SRD 以降のリリースでは、全体的に良好なマルチパスが、許可される最大数よりも多く存在する場合、最も古いパスがマルチパスとして選択されます。

BGP は、アップデート メッセージにパス属性情報を含めることができます。BGP 属性はルートの特徴を記述するもので、ソフトウェアがこの属性を使用し、アドバタイズするべきルートの決定に役立たせます。一部の属性情報は、BGP 対応のネットワーキング デバイスでも設定できます。属性には、アップデートメッセージに常に含まれる必須のものと、任意のものとがあります。次のような BGP 属性が設定可能です。

- AS_Path
- Community
- Local_Pref
- Multi_Exit_Discriminator（MED）
- Next_Hop
- Origin

AS_Path

この属性は、ルーティング情報が通過してきた自律システム番号のセットまたはリストを含んでいます。BGP スピーカーは、アップデート メッセージを外部ピアへ転送する際に、自分の自律システム番号をリストに加えます。

Community

ネットワークや自律システム、または物理的境界にかかわりなく、共通のプロパティを持つネットワーキング デバイスをグループ化するには、BGP コミュニティを使用します。大規模ネットワークにおいて、共通のルーティング ポリシーをプレフィックス リストやアクセス リストで適用するには、ネットワーキングデバイスごとに個別のピア文が必要になります。BGP コミュニティ属性を使えば、共通のルーティング ポリシーを持つ BGP ネイバーに、コミュニティタグに基づいてインバウンドやアウトバウンドのルートフィルタをインプリメントでき、個別に permit 文や deny 文を羅列した巨大なリストを扱わずにすみます。

Local_Pref

自律システム内で、Local_Pref 属性は BGP ピア間のアップデート メッセージすべてに含まれます。同一の宛先に対し複数のパスがある場合、最も大きな値を持つローカルプリファレンス属性は、ローカルの自律システムからの優先アウトバウンドパスを示します。ランキングが最高のルートが内部のピアにアドバタイズされます。Local_Pref の値は外部ピアへは転送されません。

Multi_Exit_Discriminator

MED 属性は、（外部ピアに）自律システムへの優先パスを示します。自律システムへのエントリ ポイントが複数ある場合、MED を使って別の自律システムに特定のエントリ ポイントを選択するようはたらきかけることができます。低い値の MED メトリックの方が高い値の MED メトリックより優先されるソフトウェアでは、メトリックが割り当てられます。MED メトリックは自律システムの間で交換されますが、MED が自律システムに転送された後、MED メトリックはデフォルト値である 0 にリセットされます。アップデートが内部 BGP（iBGP）ピアに送られると、MED はまったく変更を加えられずに受け渡されていくため、同一の自律システム内のすべてのピアが一貫したパス選択を行うことができます。

デフォルトでは、ルータは同じ自律システムにある BGP ピアからのパスの MED 属性だけを比較します。**bgp always-compare-med** コマンドを設定することで、ルータに別の自律システムのピアからのメトリックを比較させることができます。

（注） BGP MED についてのインターネット技術特別調査委員会（IETF）の決定では、欠落している MED には無限の値を割り当て、MED 変数の欠落したルートの優先度を最低にしています。シスコ ソフトウェアが稼働する BGP ルータでは、ルートに MED 属性がない場合は MED の値を 0 として処理し、MED 変数の欠落したルートを最優先とすることが、デフォルトの動作になっています。IETF 標準に準拠してルータを設定する場合、**bgp bestpath med missing-as-worst** ルータ コンフィギュレーション コマンドを使用します。

Next_Hop

Next_Hop 属性は、宛先への BGP ネクスト ホップとして使用されるネクスト ホップ IP アドレスを示します。ルータは、再帰的ルックアップによってルーティング テーブルで BGP ネクストホップを検索します。外部 BGP（eBGP）では、ネクストホップはアップデートを送信したピアの IP アドレスです。内部 BGP（iBGP）は、内部で生成されたルートのプレフィックスをアドバタイズしたピアの IP アドレスを、ネクストホップのアドレスとして設定します。eBGP から学習した iBGP へのルートのいずれかがアドバタイズされた場合、Next_Hop 属性は変更されません。

ルータが BGP ルートを使用するためには、BGP ネクストホップの IP アドレスが到達可能でなければなりません。到着可能性情報は通常 IGP によって提供され、IGP での変更はネットワーク バックボーンを介したネクストホップ アドレスの転送に影響を与える可能性があります。

Origin

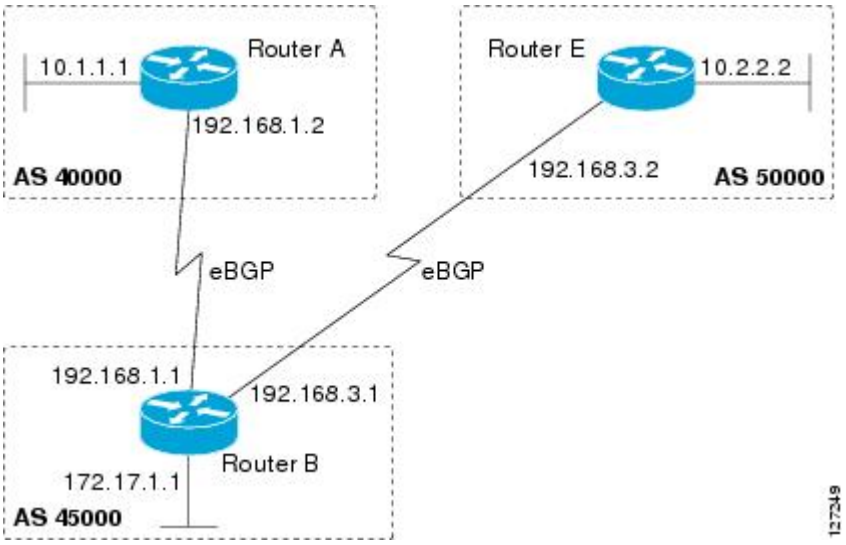
この属性は、ルートがどのように BGP ルーティング テーブルに含まれたかを示します。シスコ ソフトウェアにおいて、BGP **network** コマンドを使用して定義されたルートには、内部ゲートウェイ プロトコル（IGP）の送信コードが与えられています。外部ゲートウェイ プロトコル（EGP）から配信されたルートは、EGP の送信元を使用してコーディングされ、その他のプロトコルから再配布されたルートは「不完全」と定義されます。BGP の送信元決定ポリシーでは、「不完全」よりも EGP が、EGP よりも IGP が優先されます。

マルチホーミング

1 つの自律システムが複数のサービス プロバイダーに接続する場合に、マルチホーミングが定義されます。1 つのサービス プロバイダーの信頼性に何か問題が生じた場合、バックアップ接続を使用できます。パフォーマンスの問題もマルチホーミングで改善する場合があります。宛先ネットワークへのより適したパスを使用できることがあるからです。

自分がサービス プロバイダーでない場合、インターネットのトラフィックが自律システム内を通過して帯域幅を使いきってしまうことがないよう、ルーティング設定を注意深く検討する必要があります。下の図では、自律システム 45000 が自律システム 40000 と自律システム 50000 とにマルチホーミングされています。自律システム 45000 がサービス プロバイダーでないと仮定すると、ロード バランシングや何らかのルーティング ポリシーを使用して、自律システム 45000 からのトラフィックが自律システム 40000 にも自律システム 50000 にも到達できるように、しかし同時に転送トラフィックはあったとしても少なく抑えるように設定する必要があります。

図 *23 :* **マルチホーミング トポロジ**



MED 属性

MED 属性の設定は、別の自律システムへのパス選択を変化させるために BGP が使用できるもう 1 つの方法です。MED 属性は、（外部ピアに）自律システムへの優先パスを示します。自

律システムへのエントリ ポイントが複数ある場合、MED を使って別の自律システムに特定のエントリ ポイントを選択するよう働きかけることができます。低い値の MED メトリックの方が高い値の MED メトリックより優先されるソフトウェアでは、ルート マップを使用してメトリックが割り当てられます。

中継トラフィックと非中継トラフィック

自律システム内のほとんどのトラフィックは、その自律システム内にある発信元または宛先IP アドレスを含んでおり、このトラフィックを非中継（またはローカル）トラフィックと呼びます。その他のトラフィックを中継トラフィックとして定義します。インターネットを介したトラフィックが増えるにつれて、中継トラフィックの制御がいっそう重要になります。

サービス プロバイダーは中継自律システムと考えることができ、他のすべての中継プロバイダーへの接続性を提供できなければなりません。現実には、ほとんどのサービス プロバイダーは中継トラフィックすべてを許容できるだけの帯域幅を持っていないため、それらのプロバイダーはそのような接続性を 1 次プロバイダーから購入する必要があります。

通常は中継トラフィックを許可しない自律システムはスタブ自律システムと呼ばれ、インターネットには 1 つのサービス プロバイダーを通してリンクします。

BGP ポリシー設定

BGP ポリシー設定は、BGP ルーティング プロセスによるプレフィックス処理を制御し、インバウンドおよびアウトバウンドのアドバタイズメントからルートをフィルタリングするために使われます。プレフィックス処理は、BGP タイマーの調整、BGP によるパス属性の扱いの変更、ルーティング プロセスが受け入れるプレフィックスの数の制限、および BGP プレフィックス ダンプニングの設定によって制御できます。インバウンドおよびアウトバウンドのアドバタイズメントは、ルート マップ、フィルタ リスト、IP プレフィックス リスト、自律システム パス アクセス リスト、IP ポリシー リスト、および配信リストを使用してフィルタリングされます。下の図に、BGP ポリシー フィルタの処理順序を示します。

表 *27 : BGP* ポリシー処理順序

着信	発信
ルート マップ	ディストリビュート リスト
フィルタリスト、AS パス アクセス リスト、または IP ポリシー	IP プレフィックス リスト
IP プレフィックス リスト	フィルタリスト、AS パス アクセス リスト、または IP ポリシー
ディストリビュート リスト	ルート マップ

（注） Cisco IOS Release 12.0(22)S、12.2(15)T、12.2(18)S、およびそれ以降のリリースでは、**ip as-path access-list** コマンドを使用して設定できる自律システム アクセス リストの上限値が、199 から 500 に増加しました。

設定変更のためにルーティング ポリシーに変更が生じた場合は、必ず **clear ip bgp** コマンドを使用して、BGP ピアリング セッションをリセットする必要があります。Cisco IOS ソフトウェアは、BGP ピアリング セッションのリセットとして、次の 3 つのメカニズムをサポートしています。

- ハード リセット：ハード リセットは、TCP 接続を含む指定されたピアリング セッションを終了し、指定されたピアから到着したルートを削除します。
- ソフト リセット：ソフト リセットは、保存されたプレフィックス情報を使用し、既存のピアリング セッションを終了せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフトリセットは保存されたアップデート情報を使用するため、アップデート保存用のメモリを追加することで、ネットワークを中断することなく新しい BGP ポリシーを適用できます。ソフトリセットは、インバウンドとアウトバウンドのセッションに設定できます。
- ダイナミック インバウンド ソフト リセット：これは RFC 2918 に定義されているルート リフレッシュ機能で、サポートしているピアへのルート リフレッシュ要求を交換することにより、ローカル デバイスがインバウンド ルーティング テーブルを動的にリセットできるようにするものです。ルート リフレッシュ機能は、中断を伴わないポリシー変更についてはアップデート情報をローカルに保存しません。その代わり、サポートしているピアとの動的な交換に依存します。ルート リフレッシュは、最初にピア間の BGP 機能ネゴシエーションを通じてアドバタイズされる必要があります。すべての BGP ルータが、ルート リフレッシュ機能をサポートしていなければなりません。

BGP ルータがこの機能をサポートしているかどうかを確認するには、**show ip bgp neighbors** コマンドを使用します。ルータがルート リフレッシュ機能をサポートしている場合、次のメッセージが出力されます。

```
Received route refresh capability from peer.
```

BGP COMMUNITIES 属性

BGP コミュニティは、ネットワーク、自律システム、またはあらゆる物理的な境界に関係なく、共通プロパティを共有するルートのグループです。大規模ネットワークにおいて、プレフィックス リストやアクセス リストを使用して共通のルーティング ポリシーを適用するには、ネットワーキング デバイスごとに個別のピア文が必要になります。BGP COMMUNITIES 属性を使えば、共通のルーティング ポリシーを持つ BGP スピーカーに、コミュニティ タグに基づいてインバウンドやアウトバウンドのルート フィルタを実装でき、個別に permit 文や deny 文を羅列した長いリストを扱わずにすみます。COMMUNITIES 属性には複数のコミュニティを含めることができます。

ルートは複数のコミュニティに所属できます。ネットワーク管理者は、ルートが属するコミュニティを定義します。デフォルトでは、すべてのルートは一般的なインターネット コミュニティに属します。

番号付きのコミュニティに加えて、次の事前定義された（ウェルノウン）コミュニティがあります。

- no-export：このルートを外部 BGP ピアにアドバタイズしません。
- no-advertise：このルートをどのピアにもアドバタイズしない。
- internet：このルートをインターネットコミュニティにアドバタイズします。すべてのBGP対応ネットワーキング デバイスはこのコミュニティに属します。
- local-as：ローカル自律システムの外部にはこのルートを送信しません。
- gshut：ルートのコミュニティのグレースフル シャットダウンを実行します。

COMMUNITIES 属性はオプションです。そのため、コミュニティを認識しないネットワーキング デバイスは通過できません。コミュニティを認識するネットワーキング デバイスでも、コミュニティを扱うよう設定しなければ、COMMUNITIES 属性は無視されます。デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性をネイバーに送信するには、**neighbor send-community** コマンドを使用します。

拡張コミュニティ

拡張コミュニティ属性は、仮想ルーティング/転送（VRF）インスタンスおよびマルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）のルートの設定、フィルタリング、識別に使用されます。アクセスリストの標準ルールすべてが、拡張コミュニティ リストの設定に適用されます。正規表現は、拡張コミュニティ リスト番号の拡張範囲によってサポートされています。正規表現の設定オプションはすべてサポートされます。ルート ターゲット（RT）および Site of Origin（SoO）拡張コミュニティ属性は、拡張コミュニティ リストの標準範囲でサポートされます。

ルート ターゲット拡張コミュニティ属性

RT 拡張コミュニティ属性は、**ip extcommunity-list** コマンドの **rt** キーワードで設定されます。この属性は、configured route target とタグ付けされたルートを受け取る可能性があるサイトと VRF のセットとの識別に使用します。ルート付き route target 拡張コミュニティ属性により、対応するサイトから受信したトラフィックのルーティングに使用するサイト別のフォワーディング テーブルにルートを置くことが可能になります。

Site of Origin 拡張コミュニティ属性

SoO 拡張コミュニティ属性は、**ip extcommunity-list** コマンドの **soo** キーワードで設定されます。この属性は、プロバイダー エッジ（PE）ルータがルートを学習したサイトを一意に識別します。ある特定のサイトから学習したルートにはすべて、サイトが接続されている PE ルータの数にかかわらず、同一の SoO 拡張コミュニティ属性が割り当てられる必要があります。マルチホーミングされているサイトでは、この属性を設定することでルーティングにループが

発生するのを防止できます。SoO拡張コミュニティ属性はインターフェイス上で設定され、再配布によって BGP へ伝播されます。SoO 拡張コミュニティ属性は、VRF から学習したルートへ適用することができます。スタブ サイトやマルチホーミングされていないサイトには、SoO 拡張コミュニティ属性を設定しないでください。

IP 拡張コミュニティリスト コンフィギュレーション モード

名前付きおよび番号付きコミュニティ リストは、IP拡張コミュニティリスト コンフィギュレーション モードで設定することができます。IP 拡張コミュニティリスト コンフィギュレーション モードは、グローバル コンフィギュレーション モードで使用できる機能すべてをサポートしています。さらに、次のような操作も行えます。

- 拡張コミュニティ リスト エントリにシーケンス番号を設定する。
- 既存の拡張コミュニティ リスト エントリのシーケンス番号を再設定する。
- デフォルト値を使用するよう、拡張コミュニティ リストを設定する。

デフォルトのシーケンス番号

シーケンス番号が指定されていない場合、デフォルト動作が設定されている場合、および拡張コミュニティリストのシーケンス番号が開始番号や後続エントリ用増分の指定なく再割り当てされた場合、拡張コミュニティ リスト エントリは 10 番から開始され、後続のエントリでは 1 エントリにつき 10 ずつ増えていきます。

拡張コミュニティ リストのシーケンス番号再割り当て

拡張コミュニティ リスト エントリは、拡張コミュニティ リスト単位を基本としてシーケンス番号の割り当てと再割り当てが行われます。**resequence** コマンドを引数なしで使用すると、リスト内のすべてのエントリにデフォルトのシーケンス番号割り当てを行えます。**resequence** コマンドでは、最初のエントリ用のシーケンス番号や後続のエントリごとの数値の増減範囲を設定することもできます。設定できるシーケンス番号の範囲は、1 ～ 2147483647 です。

拡張コミュニティ リスト

拡張コミュニティ リストは、VRF インスタンスと MPLS VPN のルートを設定し、フィルタリングし、識別するために使用されます。名前付きまたは番号付きコミュニティ リストの設定には、**ip extcommunity-list** コマンドを使用します。アクセス リストの標準ルールすべてが、拡張コミュニティ リストの設定に適用されます。正規表現は、拡張コミュニティ リスト番号の拡張範囲によってサポートされています。

アドミニストレーティブ ディスタンス

アドミニストレーティブ ディスタンスは、異なるルーティング プロトコルのプリファレンスを測定する方法です。BGP にある **distance bgp** コマンドで、外部、内部、ローカルという 3 つのルート タイプのアドミニストレーティブ ディスタンスを、それぞれ設定することができま

す。他のプロトコル同様、BGP もアドミニストレーティブ ディスタンスが最小となるルートを優先します。

BGP ルート マップ ポリシー リスト

BGP ルート マップ ポリシー リストにより、ネットワーク オペレータはルート マップ match 句をグループ化して、ポリシー リストと呼ばれる名前付きリストにすることができます。ポリシー リスト機能はマクロに似ています。ルート マップでポリシー リストが参照されると、match 句がすべて評価され、ルート マップで直接設定された場合と同様に処理されます。この機能強化により、中規模から大規模のネットワークでの BGP ルーティング ポリシーの BGP 設定が単純になりました。ネットワーク オペレータが match 句のグループを持つポリシー リストを事前に設定しておき、さまざまなルート マップ内でそれらのポリシー リストを参照できるからです。複数のルートマップのエントリに繰り返し現れる一群の match 句を、ネットワーク オペレータがそれぞれ手動で再設定する必要がなくなりました。

ルート マップで設定されるポリシー リスト機能はマクロに似ており、次のような機能や特長を持っています。

- ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。
- 1 つのルートマップに 2 つ以上のポリシーリストを設定できます。ポリシーリストはルート マップ内で AND や OR を使用して評価されるように設定可能です。
- ポリシーリストは、同じルート マップ内にあってもポリシー リスト外で設定されている他の既存の match および set 文とも共存可能です。
- 1 つのルート マップ エントリ内で複数のポリシー リストがマッチングを行う場合、すべてのポリシー リストは受信属性だけでマッチングします。

ポリシー リストがサポートするのは match 句だけで、set 句はサポートしていません。ポリシー リストは、再配布を含めルート マップのアプリケーションすべてに設定でき、同一のルート マップ エントリ内でポリシー リストと別に設定される match および set 句と共存させることもできます。

（注） ポリシー リストは BGP だけでサポートされ、他の IP ルーティング プロトコルではサポートされません。

外部BGPを使用したサービス プロバイダーとの接続方法

インバウンド パス選択の変更

BGPを使用して、別の自律システムにあるパスの選択を変化させることができます。明らかにベスト ルート以外のパスを BGP に選ばせたい場合もあります。たとえば、中継トラフィックの一部が自律システムを通過するのを避けたい場合や、非常に遅い、または輻輳しているリンクを避けたい場合です。BGP では、次の BGP 属性のいずれかを使用して、インバウンド パスの選択を変化させることができます。

- AS-path
- Multi-Exit 識別子（MED）

インバウンド パス選択を変化させる場合、次の作業のいずれかを実行します。

AS_PATH 属性の変更によるインバウンド パス選択の変化

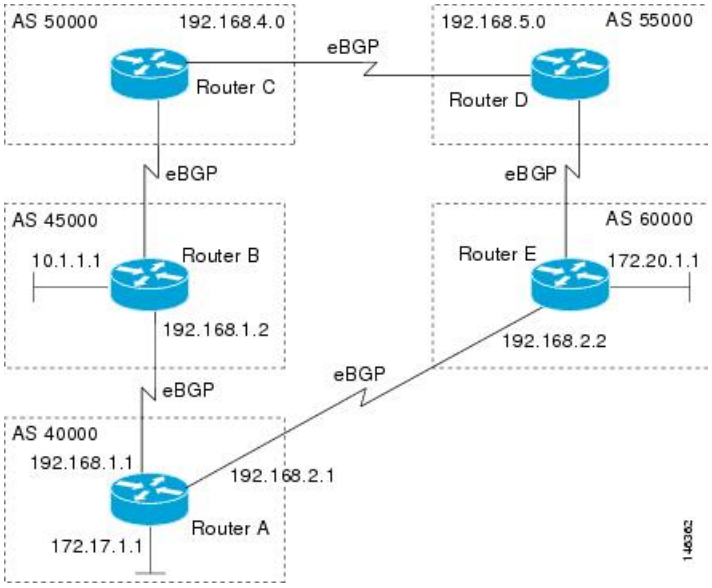
AS_PATH 属性を変更して 172.17.1.0 ネットワークへ向かうトラフィックのインバウンド パス選択を変化させるには、次の作業を実行します。設定は、下の図のルータ A で実行されます。asplain 形式の 4 バイト自律システム番号を使用した設定例については、「例：4 バイト AS 番号を使用したAS-path 属性の変更によるインバウンドパス選択の変化」を参照してください。

AS_PATH 属性の変更は、別の自律システムのパス選択を変化させるために BGP で使用可能な方法の 1 つです。たとえば、下の図において、ルータ A は自身のネットワーク 172.17.1.0 を、自律システム 45000 および自律システム 60000 にある BGP ピアにアドバタイズします。ルーティング情報が自律システム 50000 に伝播されるとき、自律システム 50000 内のルータは、2 つの異なるルートからのネットワーク 172.17.1.0 の到達可能性情報を持つことになります。1 番目のルートは、45000 と 40000 で構成される AS_PATH を備えた自律システム 45000 によるもので、2 番目のルートは、55000、60000、40000 の AS_PATH を備えた自律システム 55000 によるものです。他の BGP 属性がすべて同じだとすれば、自律システム 50000 内のルータ C はネットワーク 172.17.1.0 へのトラフィックのルートとして、自律システム 45000 を通るルートを選択します。通過した自律システムという点では最短ルートとなるからです。

自律システム 40000 は、自律システム 45000 を通して、自律システム 50000 から 172.17.1.0 ネットワークへのトラフィックすべてを受け取ることになります。しかし、自律システム 45000 と自律システム 40000 の間のリンクが非常に遅く輻輳している場合、**set as-path prepend** コマンドをルータ A で使用して、自律システム 45000 経由のルートが自律システム 60000 経由のパスよりも遠いように見せることで、172.17.1.0 ネットワークへのインバウンド パス選択を変化させることができます。下の図のルータ A の設定は、アウトバウンド BGP アップデートをルータ B に適用することで完了します。**set as-path prepend** コマンドの使用により、ルータ A からルータ B へのアウトバウンド BGP アップデートはすべて、ローカル自律システム番号 40000 を 2 回追加するよう変更された AS_PATH 属性を持つようになります。この設定の後、自律システム 50000 は 172.17.1.0 ネットワークについてのアップデートを、自律システム 45000 経由で受け取ることになります。新しい AS_PATH は 45000、40000、40000、40000 となり、これ

は自律システム 55000 からの AS-path（55000、60000、40000 で変更なし）よりも長くなります。自律システム 50000 内のネットワーキング デバイスは、172.17.1.0 ネットワーク内の宛先アドレスを持つパケットを転送するときに、自律システム 55000 経由のルートを優先するようになります。

図 *24 : AS_PATH* 属性変更のネットワーク トポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. **exit-address-family**
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **set as-path** {**tag** | **prepend** *as-path-string*}
13. **end**
14. **show running-config**

手順の詳細

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

	コマンドまたはアクション	目的
	`Device> enable`	
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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、192.168.1.2 のルータ B の BGP ピアが IPv4 マルチプロトコル BGP ネイバー テーブルに追加され、BGP アップデートを受け取ることになります。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • unicast キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例：	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	• 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.1.2 activate`	ルータ B 上の 192.168.1.2 にある BGP ネイバーのため、アドレス ファミリ IPv4 ユニキャスト用アドレス交換を有効にします。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 192.168.1.2 route-map PREPEND out`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、PREPEND という名前のルート マップが、ルータ B へのアウトバウンド ルートに適用されています。
ステップ 9	**exit-address-family** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 10	**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 11	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map PREPEND permit 10`	ルート マップを設定し、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。 • この例では、PREPEND という名前のルート マップが permit 句で作成されます。
ステップ 12	**set as-path** {**tag** | **prepend** *as-path-string*} 例： `Device(config-route-map)# set as-path prepend 40000 40000`	BGP ルートの自律システム パスを変更します。 • 任意の自律システム パス文字列を BGP ルートの前に付加するには、**prepend** キーワードを使用します。通常、ローカルな自律システム番号は複数回追加され、AS パス長が増します。 • この例では、2 つの自律システム エントリがルータ B へのアウトバウンド ルートの自律システム パスに追加されます。

	コマンドまたはアクション	目的
ステップ 13	**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、特権 EXEC モードに戻ります。
ステップ 14	**show running-config** 例： `Device# show running-config`	実行コンフィギュレーション ファイルを表示します。

例

ルータ A

次の **show running-config** コマンドからの出力の一部は、この作業で行った設定を示します。

```
Device# show running-config
.
.
.
router bgp 40000
 neighbor 192.168.1.2 remote-as 45000
 !
 address-family ipv4
 neighbor 192.168.1.2 activate
 neighbor 192.168.1.2 route-map PREPEND out
 no auto-summary
 no synchronization
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
!
route-map PREPEND permit 10
 set as-path prepend 40000 40000
.
.
.
```

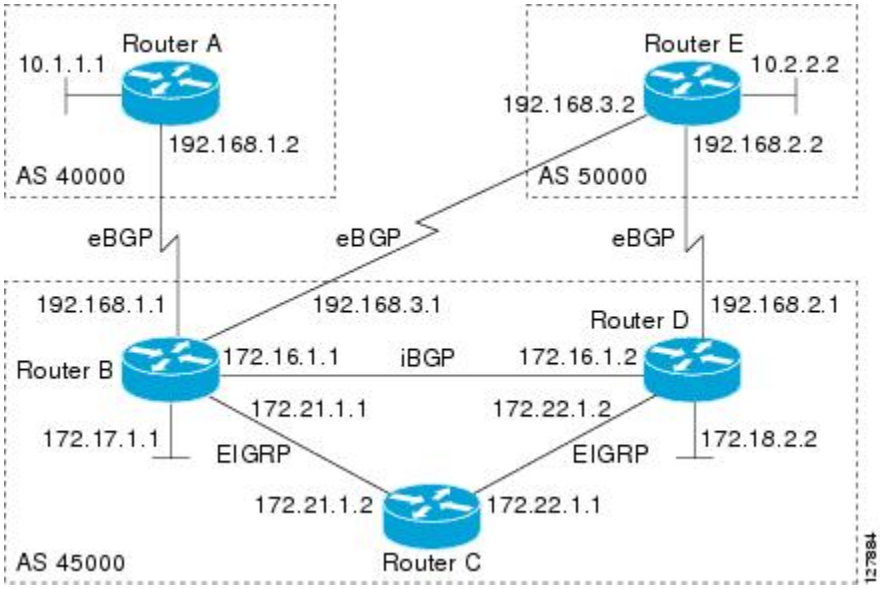
MED 属性の設定によるインバウンド パス選択の変化

Multi-Exit 識別子（MED）属性の設定は、別の自律システムへのパス選択を変化させるために BGP で使用可能な方法の 1 つです。MED 属性は、（外部ピアに）自律システムへの優先パスを示します。自律システムへのエントリ ポイントが複数ある場合、MED を使って別の自律システムに特定のエントリ ポイントを選択するよう働きかけることができます。低い値の MED メトリックの方が高い値の MED メトリックより優先されるソフトウェアでは、ルート マップを使用してメトリックが割り当てられます。

MED メトリック属性の設定によってインバウンド パス選択を変化させるには、次の作業を行います。下の図では、ルータ B とルータ D で設定を実行します。ルータ B はネットワーク

172.16.1.0 を自身の BGP ピアにアドバタイズし、ルータ E は自律システム 50000 にあります。シンプルなルート マップを使用して、ルータ B はアウトバウンド アップデートの MED メトリックを 50 に設定します。この作業がルータ D でも繰り返されますが、MED メトリックは 120 に設定されます。ルータ E がルータ B とルータ D の両方からアップデートを受け取ったとき、MED メトリックは BGP ルーティング テーブルに保存されます。ネットワーク 172.16.1.0 へパケットを転送する前に、ルータ E は同じ自律システム内の複数のピアから受信した属性を比較します（ルータ B とルータ D はどちらも自律システム 45000 にあります）。ルータ B の MED メトリックはルータ D の MED より小さいため、ルータ E はパケットをルータ B 経由で転送します。

図 *25 : MED* 属性設定のネットワーク トポロジ



別の自律システムのピアからの MED 属性を比較するには、**bgp always-compare-med** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. **exit**
9. **exit**
10. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
11. **set metric** *value*
12. **end**
13. ルータ D で手順 1 ～ 12 を繰り返します。

14. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Device(config-router-af)# network 172.16.1.0 mask 255.255.255.0`	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 192.168.3.2 route-map MED out`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、MED という名前のルート マップが、ルータ E にある BGP ピアへのアウトバウンド ルートに適用されます。
ステップ 8	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 9	**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	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map MED permit 10`	ルート マップを設定し、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。 • この例では、MED という名前のルート マップが作成されます。
ステップ 11	**set metric** *value* 例： `Device(config-route-map)# set metric 50`	MED メトリックの値を設定します。
ステップ 12	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 13	ルータ D で手順 1 ～ 12 を繰り返します。	-
ステップ 14	**show ip bgp** [*network*] [*network-mask*] 例：	（任意）BGP ルーティング テーブル内のエントリを表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp 172.17.1.0 255.255.255.0`	• 上の図で、ルータ B とルータ D の両方が MED 属性を設定しているとき、このコマンドをルータ E で実行します。 • この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力は、この作業が上の図のルータ B とルータ D の両方で実行された後に、ルータ E から取得されたものです。ネットワーク 172.16.1.0 への 2 つのルートのメトリック（MED）値に注目してください。ルータ D にあるピア 192.168.2.1 は、ネットワーク 172.16.1.0 へのパスとしてメトリック 120 を持ち、ルータ B の 192.168.3.1 はメトリック 50 になっています。ルータ B のピア 192.168.3.1 のエントリでは、ルータ E がネットワーク 172.16.1.0 を宛先とするパケットを送るのに、MED メトリックが低いことからルータ B 経由での送信を選ぶことを示すため、エントリの最後に best という語が付いています。

```
Device# show ip bgp 172.16.1.0

BGP routing table entry for 172.16.1.0/24, version 10
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1
  45000
    192.168.2.1 from 192.168.2.1 (192.168.2.1)
      Origin IGP, metric 120, localpref 100, valid, external
  45000
    192.168.3.1 from 192.168.3.1 (172.17.1.99)
      Origin IGP, metric 50, localpref 100, valid, external, best
```

アウトバウンド パス選択への影響

BGP を使用して、ローカルの自律システムからのアウトバウンド トラフィックに対するパス選択を変化させることができます。このセクションでは、アウトバウンドパスの選択を変化させるのに BGP が使用可能な 2 つの方法を説明します。

- Local_Pref 属性の使用
- BGP アウトバウンド ルート フィルタ（ORF）機能の使用

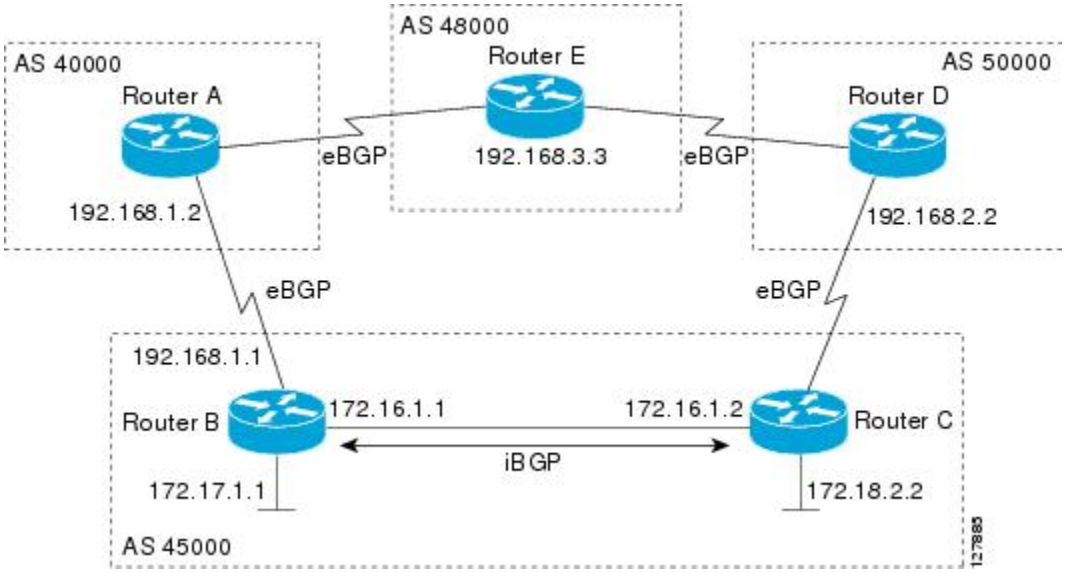
アウトバウンド パス選択を変化させる場合、次の作業のいずれかを実行します。

Local_Pref 属性を使用したアウトバウンド パス選択の変更

アウトバウンド パス選択を変化させる方法の 1 つが、BGP Local-Pref 属性の使用です。アウトバウンド パス選択を変化させるには、ローカル プリファレンス属性を使用してこの作業を実行します。同じ宛先への複数のパスがある場合、ローカルプリファレンス属性の値が最大であるものが、優先パスになります。

この作業で使用するネットワーク トポロジについては、下の図を参照してください。ルータ B とルータ C の両方が設定されています。自律システム 45000 は、ネットワーク 192.168.3.0 のアップデートを自律システム 40000 と自律システム 50000 から受信します。ルータ B は、自律システム 40000 へのアップデートすべてに対し、ローカルプリファレンスの値を 150 にするよう設定されています。ルータ C は、自律システム 50000 へのアップデートすべてに対し、ローカル プリファレンスの値を 200 にするよう設定されています。設定の後、ローカル プリファレンス情報が自律システム 45000 との間で交換されます。ルータ B とルータ C は、ネットワーク 192.168.3.0 のアップデートで自律システム 50000 からの方が高いプリファレンス値を持つことがわかるため、自律システム 45000 内で宛先ネットワークが 192.168.3.0 のトラフィックは、すべてルータ C 経由で送られます。

図 *26 :* アウトバウンド パス選択のネットワーク トポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
5. **bgp default local-preference** *value*
6. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
7. **network** *network-number* [**mask** *network-mask*][**route-map** *route-map-name*]
8. **neighbor** {*ip-address*| *peer-group-name*} **activate**
9. **end**

10. 手順 1 ～ 9 をルータ C で繰り返します。ただし、ピアの IP アドレスと自律システム番号は変更し、ローカル プリファレンスの値を 200 に設定します。
11. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**bgp default local-preference** *value* 例： `Router(config-router)# bgp default local-preference 150`	ローカル プリファレンスのデフォルト値を変更します。 • この例では、自律システム 40000 から自律システム 45000 へのアップデートすべてのローカル プリファレンスが 150 に変更されます。 • ローカル プリファレンスの値は、デフォルトでは 100 です。
ステップ 6	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファ

	コマンドまたはアクション	目的
		ミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 7	**network** *network-number* [**mask** *network-mask*][**route-map** *route-map-name*] 例： `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 8	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 192.168.1.2 activate`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 9	**end** 例： `Router(config-router-af)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	手順 1 ～ 9 をルータ C で繰り返します。ただし、ピアの IP アドレスと自律システム番号は変更し、ローカルプリファレンスの値を 200 に設定します。	--
ステップ 11	**show ip bgp** [*network*] [*network-mask*] 例： `Router# show ip bgp 192.168.3.0 255.255.255.0`	BGP ルーティング テーブル内のエントリを表示します。 • ルータ B とルータ C の両方でこのコマンドを入力し、Local_Pref の値を記録します。最大のプリファレンス値を持つルートが、ネットワーク 192.168.3.0 への優先ルートになります。

	コマンドまたはアクション	目的
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

アウトバウンド BGP ルート プレフィックスのフィルタリング

BGP プレフィックスベース アウトバウンド ルート フィルタリングを使用してアウトバウンド パス選択を変化させるには、次の作業を行います。

始める前に

プレフィックスベース ORF BGP の配信が受信可能になるには、ピアリング セッションが確立され、BGP ORF 機能が各参加ルータで有効になっている必要があります。

（注）
- BGP プレフィックスベース アウトバウンド ルート フィルタリングはマルチキャストをサポートしていません。
- アウトバウンド ルート フィルタリングに使用する IP アドレスは IP プレフィックス リストで定義されている必要があります。BGP 配信リストおよび IP アクセス リストはサポートしていません。
- アウトバウンド ルート フィルタリングはアドレス ファミリ単位ベースだけで設定され、ジェネラル セッションや BGP ルーティング プロセス下では設定できません。
- アウトバウンド ルート フィルタリングは、外部ピアリング セッションだけに設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
4. **router bgp** autonomous-system-*number*
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **ebgp-multihop** [*hop-count*]
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **neighbor** *ip-address* **capability orf prefix-list** [**send** | **receive** | **both**]
9. **neighbor** {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}
10. **end**
11. **clear ip bgp** {*ip-address* | *****} **in prefix-filter**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Router(config)# ip prefix-list FILTER seq 10 permit 192.168.1.0/24`	プレフィックスベース アウトバウンド ルート フィルタリング用にプレフィックス リストを作成します。 • アウトバウンド ルート フィルタリングは、プレフィックス長のマッチング、ワイルドカードベースのプレフィックス マッチング、アドレスファミリ単位ベースのアドレス プレフィックス マッチングをサポートします。 • アウトバウンド ルート フィルタを定義するためにプレフィックス リストが作成されます。アウトバウンド ルート フィルタリング機能が send モードまたは both モードでアドバタイズされるよう設定されているときは、フィルタの作成が必要です。ピアが receive モードだけでアドバタイズされるよう設定されている場合は不要です。 • この例では、アウトバウンド ルート フィルタリングのためにサブネット 192.168.1.0/24 を定義する、FILTER という名前のプレフィックス リストを作成します。
ステップ 4	**router bgp** autonomous-system-*number* 例： `Router(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.1.1.1 remote-as 200`	指定されたネイバーまたはピア グループとのピアリングを確立します。ORF 機能が交換できるようになるには、BGP ピアリングが確立されている必要があります。

	コマンドまたはアクション	目的
		• この例では、ネイバー 10.1.1.1 とのピアリングを確立します。
ステップ 6	**neighbor** *ip-address* **ebgp-multihop** [*hop-count*] 例： `Router(config-router)# neighbor 10.1.1.1 ebgp-multihop`	直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れるか、または開始します。
ステップ 7	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。 （注） アウトバウンド ルート フィルタリングは、アドレス ファミリ単位ベースで設定されます。
ステップ 8	**neighbor** *ip-address* **capability orf prefix-list** [**send** | **receive** | **both**] 例： `Router(config-router-af)# neighbor 10.1.1.1 capability orf prefix-list both`	ローカル ルータで ORF 機能を有効にし、*ip-address* 引数で指定された BGP ピアへの ORF 機能アドバタイズメントを有効にします。 • **send** キーワードは、ORF 送信機能をアドバタイズするようルータを設定します。 • **receive** キーワードは、ORF 受信機能をアドバタイズするようルータを設定します。 • **both** キーワードは、送受信機能をアドバタイズするようルータを設定します。 • アウトバウンドルートフィルタリングがイネーブルにされる前に、リモート ピアで送信と受

	コマンドまたはアクション	目的
		信いずれかの ORF 機能が設定されている必要があります。 • この例では、ネイバー 10.1.1.1 への送信と受信機能をアドバタイズするようルータを設定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**} 例： `Router(config-router-af)# neighbor 10.1.1.1 prefix-list FILTER in`	インバウンド プレフィックス リスト フィルタを適用し、BGP ネイバー情報を配信しないようにします。 • この例では、FILTER という名前のプレフィックス リストがネイバー 10.1.1.1 からの受信アドバタイズメントに適用され、サブネット 192.168.1.0/24 を配信しないようにしています。
ステップ 10	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 11	**clear ip bgp** {*ip-address* | *****} **in prefix-filter** 例： `Router# clear ip bgp 10.1.1.1 in prefix-filter`	BGP アウトバウンド ルート フィルタをクリアし、インバウンド ソフト リセットを開始します。 • 単一のネイバーまたはすべてのネイバーを指定できます。 （注） この機能が正しく動作するために、**clear ip bgp** コマンドでインバウンド ソフト リセットを開始する必要があります。

ISP との BGP ピアリングの設定

BGP はドメイン間ルーティング プロトコルとして開発されたもので、ISP への接続は BGP の主要機能の 1 つです。使用するネットワークのサイズやビジネスの目的により、ISP への接続にはさまざまな方法があります。1 つ以上の ISP へのマルチホーミングは、ISP への外部リンクの 1 つに障害が発生した場合のための冗長性を提供します。このセクションでは、プロバイダーへのマルチホーミングの手法を使用した接続に応用可能なオプション作業の一部を紹介します。規模の小さい企業では 1 つの ISP との接続だけを使用することがありますが、ISP へのバックアップ ルートが必要になります。規模の大きい企業では、2 つの ISP へのアクセスを確保して 1 つをバックアップとして使用したり、中継用自律システムを設定する必要が生じたりすることがあります。

1 つ以上の ISP へ接続するには、次のオプション作業のいずれかを行います。

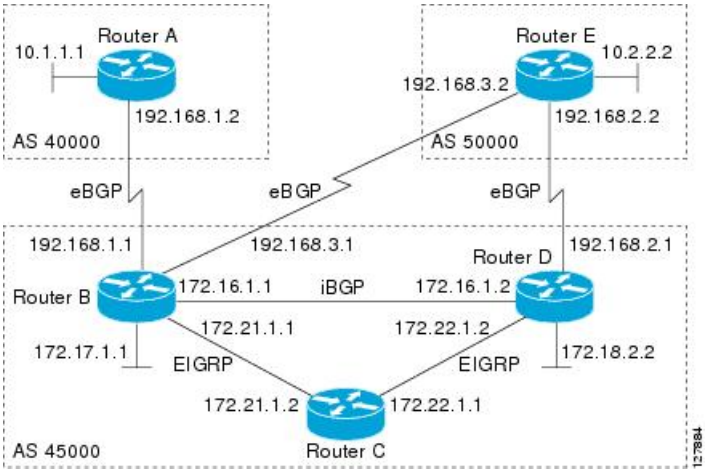
2 つの ISP とのマルチホーミングの設定

ネットワークを 2 つの ISP にアクセスさせるには、次の作業を行います。1 番目の ISP を優先ルート、2 番目の ISP はバックアップ ルートとします。下の図において、自律システム 45000 のルータ B は、自律システム 40000 と自律システム 50000 の 2 つの ISP に BGP ピアを持っています。この作業を行うことで、ルータ B は自律システム 40000 内にあるルータ A の BGP ピアへのルートを優先するよう設定されます。

このネイバーから学習したすべてのルートに、重みが割り当てられます。特定のネットワークへのルートが複数ある場合、重みが最大のルートが優先ルートとして選ばれます。

（注） **set weight** ルート マップ コンフィギュレーション コマンドで割り当てられた重みは、**neighbor weight** コマンドで割り当てられた重みを上書きします。

図 *27 : 2* つの *ISP* とのマルチホーミング



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*]
7. **neighbor** {*ip-address* | *peer-group-name*} **weight** *number*
8. **exit**
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
10. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
11. **neighbor** {*ip-address* | *peer-group-name*} **weight** *number*
12. **end**
13. **clear ip bgp** {* | *ip-address* | *peer-group-name*} [**soft** [**in** | **out**]]

14. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	**network** *network-number* [**mask** *network-mask*] 例： `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **weight** *number* 例： `Router(config-router-af)# neighbor 192.168.1.2 weight 150`	BGP ピア接続に重みを割り当てます。 • この例では、ルートの weight 属性が BGP ピア 192.168.1.2 から受け取る値は 150 に設定されています。
ステップ 8	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 10	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **weight** *number* 例： `Router(config-router-af)# neighbor 192.168.3.2 weight 100`	BGP ピア接続に重みを割り当てます。 • この例では、ルートの weight 属性が BGP ピア 192.168.3.2 から受け取る値は 100 に設定されています。
ステップ 12	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 13	**clear ip bgp** {***** | *ip-address* | *peer-group-name*} [**soft** [**in** | **out**]] 例： `Router# clear ip bgp *`	（任意）BGP アウトバウンドルート フィルタをクリアし、アウトバウンド ソフト リセットを開始します。単一のネイバーまたはすべてのネイバーを指定できます。
ステップ 14	**show ip bgp** [*network*] [*network-mask*] 例： `Router# show ip bgp`	BGP ルーティング テーブル内のエントリを表示します。 • BGP ピアへのそれぞれのルートの weight 属性を見るには、このコマンドをルータ B に入力します。weight 属性が最大のルートが、ネットワーク 172.17.1.0 への優先ルートになります。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の例は、ルートに weight 属性が割り当てられた、ルータ B の BGP ルーティング テーブルを示しています。192.168.1.2（ 上の図のルータ A）を通るルートは最大の weight 属性を持っているため、ネットワーク 10.3.0.0 への優先ルートとなり、ネットワーク 10.3.0.0 にはルータ A とルータ E を介してアクセスできます。何らかの理由により、このルート（ルータ B 経由）で障害が発生した場合は、ネットワーク 10.3.0.0 に到達するために 192.168.3.2（ルータ E）を通るルートが使用されます。これにより、ルータ B に到達するための冗長性が提供されます。

```
BGP table version is 8, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop            Metric    LocPrf   Weight  Path

*> 10.1.1.0/24         192.168.1.2           0             150      40000 i
*> 10.2.2.0/24         192.168.3.2           0             100      50000 i

*> 10.3.0.0/16         192.168.1.2           0             150      40000 i
*                      192.168.3.2           0             100      50000 i

*> 172.17.1.0/24       0.0.0.0               0             32768         i
```

単一 ISP とのマルチホーミング

ネットワークを単一の ISP との 2 つの接続のうち 1 つにアクセスさせるには、次の作業を行います。1 番目の接続を優先ルート、2 番目の接続をバックアップ ルートとします。上の図において、自律システム 50000 のルータ E には、単一自律システムである自律システム 45000 内に 2 つの BGP ピアがあります。この作業を行うことで、自律システム 50000 は自律システム 45000 からどのルートも学習せず、BGP を使用して自身のルートを送信するようになります。この作業は、上の図のルータ E で設定し、単一 ISP へのマルチホーミングに関する 3 つの機能をカバーします。

- アウトバウンド トラフィック：ルータ E は、ルータ B をプライマリ リンク、ルータ D をバックアップ リンクとして、デフォルト ルートとトラフィックを自律システム 45000 に転送します。ルータ B とルータ D にはスタティック ルートが設定され、ルータ B へのリンクのディスタンスの方が低く設定されています。
- インバウンド トラフィック：自律システム 45000 からのインバウンド トラフィックは、リンクに障害が生じたためにトラフィックをルータ D からバックアップ ルートで送る場合を除き、ルータ B から送信されるよう設定されます。この状態にするため、MED メトリックを使用したアウトバウンド フィルタが設定されています。
- 中継トラフィックの防止：自律システム 50000 のルータ E には、受信 BGP ルーティング アップデートをすべてブロックし、自律システム 50000 が自律システム 45000 の ISP からの中継トラフィックを受信しないよう、ルート マップが設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. ステップ 7 で指定されたネイバーに別のルート マップを適用するには、ステップ 7 を繰り返します。
9. **exit**
10. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
11. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]

12. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
13. ステップ 10 で指定されたネイバーに別のルート マップを適用するには、ステップ 10 を繰り返します。
14. **exit**
15. **exit**
16. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
17. 別のスタティック ルートを確立するには、ステップ 14 を繰り返します。
18. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
19. **set metric** *value*
20. **exit**
21. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
22. **set metric** *value*
23. **exit**
24. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
25. **end**
26. **show ip route** [*ip-address*] [*mask*] [**longer-prefixes**]
27. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.2.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ルータ D にある BGP ピアが BGP ルーティング テーブルに追加されます。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] 例： `Router(config-router-af)# network 10.2.2.0 mask 255.255.255.0`	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。

ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
	例：
	`Router(config-router-af)# neighbor 192.168.2.1 route-map BLOCK in`
	例：
	`Router(config-router-af)# neighbor 192.168.2.1 route-map SETMETRIC1 out`
		着信ルートまたは発信ルートにルート マップを適用します。
		• 1 番目の例では、BLOCK という名前のルート マップがルータ E のインバウンド ルートに適用されます。
		• 2 番目の例では、SETMETRIC1 という名前のルート マップがルータ D のアウトバウンド ルートに適用されます。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。

ステップ 8	ステップ 7 で指定されたネイバーに別のルート マップを適用するには、ステップ 7 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 9	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 10	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.3.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ルータ D にある BGP ピアが BGP ルーティング テーブルに追加されます。
ステップ 11	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

ステップ 12	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
	例：
	`Router(config-router-af)# neighbor 192.168.3.1 route-map BLOCK in`
	例：
	`Router(config-router-af)# neighbor 192.168.3.1 route-map SETMETRIC2 out`
		着信ルートまたは発信ルートにルート マップを適用します。
		• 1 番目の例では、BLOCK という名前のルート マップがルータ E のインバウンド ルートに適用されます。
		• 2 番目の例では、SETMETRIC2 という名前のルート マップがルータ D のアウトバウンド ルートに適用されます。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。

	コマンドまたはアクション	目的
ステップ 13	ステップ 10 で指定されたネイバーに別のルートマップを適用するには、ステップ 10 を繰り返します。	--
ステップ 14	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 15	**exit** 例： `Router(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 16	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 50`
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 50`
	例：
	`and`
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.3.1 40`
		スタティック ルートを確立します。
		• 1 番目の例では、BGP ピア 192.168.2.1 へのスタティック ルートが確立され、アドミニストレーティブ ディスタンスとして 50 が設定されます。
		• 2 番目の例では、BGP ピア 192.168.3.1 へのスタティック ルートが確立され、アドミニストレーティブ ディスタンスとして 40 が設定されます。アドミニストレーティブ ディスタンスが小さいことで、ルータ B を経由するこのルートが優先ルートになります。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。

ステップ 17	別のスタティック ルートを確立するには、ステップ 14 を繰り返します。	--
ステップ 18	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map SETMETRIC1 permit 10`	ルート マップを設定し、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。 • この例では、SETMETRIC1 という名前のルート マップが作成されます。
ステップ 19	**set metric** *value* 例： `Router(config-route-map)# set metric 100`	MED メトリックの値を設定します。

	コマンドまたはアクション	目的
ステップ 20	**exit** 例： `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 21	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map SETMETRIC2 permit 10`	ルート マップを設定し、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。 • この例では、SETMETRIC2 という名前のルート マップが作成されます。
ステップ 22	**set metric** *value* 例： `Router(config-route-map)# set metric 50`	MED メトリックの値を設定します。
ステップ 23	**exit** 例： `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 24	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map BLOCK deny 10`	ルート マップを設定し、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。 • この例では、自律システム 45000 からの受信ルートをすべてブロックするために、BLOCK という名前のルート マップが作成されます。
ステップ 25	**end** 例： `Router(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 26	**show ip route** [*ip-address*] [*mask*] [**longer-prefixes**] 例： `Router# show ip route`	（任意）ルーティング テーブルからのルート情報を表示します。 • 上の図のルータ B とルータ D がルータ E から MED メトリックを含んだアップデート情報を受信した後に、このコマンドをルータ E で使用します。 • この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 27	**show ip bgp** [*network*] [*network-mask*] 例： `Router# show ip bgp 172.17.1.0 255.255.255.0`	（任意）BGP ルーティング テーブル内のエントリを表示します。 • 上の図のルータ B とルータ D がルータ E から MED メトリックを含んだアップデート情報を受信した後に、このコマンドをルータ E で使用します。 • この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の例は、この設定作業が完了し、ルータ B とルータ D が MED メトリックを含んだアップデート情報を受信した後に、ルータ E で **show ip route** コマンドを入力したときの出力を示します。ラスト リゾート ゲートウェイがルータ B へのルートである 192.168.3.1 に設定されていることに注意してください。

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.3.1 to network 0.0.0.0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.2.2.0 is directly connected, Ethernet0/0
C    192.168.2.0/24 is directly connected, Serial3/0
C    192.168.3.0/24 is directly connected, Serial2/0
S*   0.0.0.0/0 [40/0] via 192.168.3.1
```

次の例は、この設定作業が完了し、ルータ B とルータ D がルーティング アップデートを受信した後に、ルータ E で **show ip bgp** コマンドを入力したときの出力を示します。ルート マップ BLOCK は自律システム 45000 から入ってくるルートをすべて拒否しているため、表示される唯一のネットワークはローカル ネットワークです。

```
Router# show ip bgp

BGP table version is 2, local router ID is 10.2.2.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24      0.0.0.0                  0         32768 i
```

次の例は、ルータ E でこの設定作業が完了し、ルータ B がルーティング アップデートを受信した後に、ルータ B で **show ip bgp** コマンドを入力したときの出力を示します。ネットワーク 10.2.2.0 のメトリックが 50 であることに注意してください。

```
Router# show ip bgp

BGP table version is 7, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 10.2.2.0/24      192.168.3.2             50             0 50000 i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

次の例は、ルータ E でこの設定作業が完了し、ルータ D がルーティング アップデートを受信した後に、ルータ D で **show ip bgp** コマンドを入力したときの出力を示します。ネットワーク 10.2.2.0 のメトリックが 100 であることに注意してください。

```
Router# show ip bgp

BGP table version is 3, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24      192.168.2.2            100             0 50000 i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
```

マルチホーミングのフル インターネット ルーティング テーブル受信設定

アウトバウンドルートをフィルタリングしながら、他の自律システム内の他のルータとのネイバー関係を作成するようネットワークを設定するには、次の作業を実行します。この作業では、フル インターネット ルーティング テーブルはネイバー自律システム内のサービス プロバイダーから受信しますが、ローカルで生成されたルートだけがサービスプロバイダーにアドバタイズされることになります。この作業は、上の図のルータ B で設定され、ローカルで生成されたルートだけを許可するアクセスリストと、ローカルで生成されたルートだけが他の自律システムへアウトバウンドでアドバタイズされるようにしたルート マップを使用します。

（注） 2 つの ISP からのフル インターネット ルーティング テーブルを受信すると、小さいルータの場合メモリを使いきってしまう可能性があることに注意が必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]

6. **network** *network-number* [**mask** *network-mask*]
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. **exit**
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
10. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
11. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
12. **exit**
13. **exit**
14. **ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression*
15. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
16. **match as-path** *path-list-number*
17. **end**
18. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファ

	コマンドまたはアクション	目的
		ミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**network** *network-number* [**mask** *network-mask*] 例： `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Router(config-router-af)# neighbor 192.168.1.2 route-map localonly out`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、localonly という名前のルート マップが、ルータ A へのアウトバウンド ルートに適用されています。
ステップ 8	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 10	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファ

	コマンドまたはアクション	目的
		ミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Router(config-router-af)# neighbor 192.168.3.2 route-map localonly out`	着信ルートまたは発信ルートにルート マップを適用します。 • この例では、localonly という名前のルートマップが、ルータ E へのアウトバウンド ルートに適用されています。
ステップ 12	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 13	**exit** 例： `Router(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 14	**ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression* 例： `Router(config)# ip as-path access-list 10 permit ^$`	BGP-related アクセス リストを定義します。 • この例では、アクセス リスト番号 10 が、ローカルで生成された BGP ルートだけを許可するよう定義されています。
ステップ 15	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map localonly permit 10`	ルート マップを設定し、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。 • この例では、localonly という名前のルートマップが作成されます。
ステップ 16	**match as-path** *path-list-number* 例： `Router(config-route-map)# match as-path 10`	BGP 自律システム パス アクセス リストを照合します。 • この例では、match 句にステップ 12 で作成された BGP 自律システム パス アクセス リストが使用されます。

	コマンドまたはアクション	目的
ステップ 17	**end** 例： `Router(config-route-map)# end`	ルートマップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 18	**show ip bgp** [*network*] [*network-mask*] 例： `Router# show ip bgp`	BGP ルーティング テーブル内のエントリを表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業設定が完了した後の、上の図のルータ B の BGP ルーティング テーブルの例を示します。ルーティング テーブルには、自律システム 40000 と 50000 のネットワークについての情報が含まれることに注意してください。

```
BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

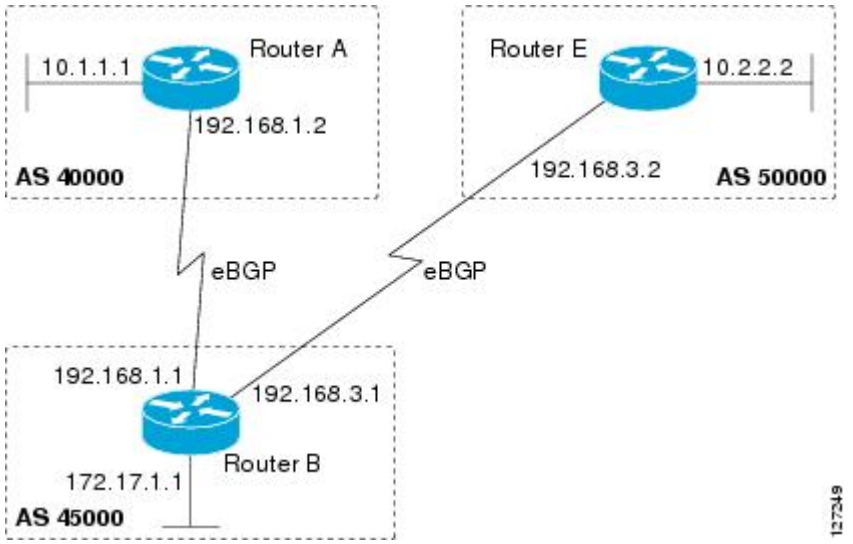
BGP ポリシーの設定

このセクションの作業は、BGP ネットワーク内でトラフィックをフィルタリングする BGP ポリシーの設定に役立ちます。次に示すオプション作業は、BGPネットワークでトラフィックをフィルタリングするさまざまな方法の一部を示すものです。

プレフィックス リストによる BGP プレフィックスのフィルタリング

プレフィックス リストを使用して BGP ルート情報をフィルタリングするには、次の作業を実行します。この設定作業は、下の図においてルータ A とルータ E の両方が BGP ピアとしてセットアップされた状況で、ルータ B で実行します。アウトバウンドにするため、プレフィックス リストをネットワーク 10.2.2.0/24 からのルートだけを許可するよう設定します。実質的に、ルータ E から受信した情報のうち、ルータ A に転送される情報がこれにより制限されます。プレフィックス リスト情報を表示するための手順、およびヒット カウントをリセットするための手順も含まれます。

図 *28 : BGP* ポリシー設定作業の *BGP* トポロジ



（注） **neighbor prefix-list** コマンドと **neighbor distribute-list** コマンドは、BGP ピアに同時には使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. すべての BGP ピアにステップ 5 を繰り返します。
6. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
7. **network** *network-number* [**mask** *network-mask*]
8. **aggregate-address** *address mask* [**as-set**]
9. **neighbor** *ip-address* **prefix-list** *list-name* {**in** | **out**}
10. **exit**
11. **exit**
12. **ip prefix-list** *list-name* [**seq** *seq-number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] [**eq** *eq-value*]
13. **end**
14. **show ip prefix-list** [**detail** | **summary**] [*prefix-list-name* [**seq** *seq-number* | *network/length*[**longer** | **first-match**]]]
15. **clear ip prefix-list** {* | *ip-address* | *peer-group-name*} **out**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定した自律システムのネイバーの IP アドレスをローカル ルータの BGP ネイバーテーブルに追加します。
ステップ 5	すべての BGP ピアにステップ 5 を繰り返します。	--
ステップ 6	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 7	**network** *network-number* [**mask** *network-mask*] 例： `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。
ステップ 8	**aggregate-address** *address mask* [**as-set**] 例： `Router(config-router-af)# aggregate-address 172.0.0.0 255.0.0.0`	BGP ルーティング テーブルに集約エントリを作成します。 • 指定されたルートは、BGP テーブル内に存在する必要があります。 • 指定された範囲に含まれる、より詳しい BGP ルートがある場合は、キーワードを指定せずに **aggregate-address** コマンドを使用して、集約エントリを作成します。 （注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 9	**neighbor** *ip-address* **prefix-list** *list-name* {**in** | **out**} 例： `Router(config-router-af)# neighbor 192.168.1.2 prefix-list super172 out`	プレフィックス リストで指定された BGP ネイバー情報を配布します。 • この例では、super172 と呼ばれるプレフィックス リストがルータ A の発信ルートに設定されます。
ステップ 10	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 11	**exit** 例： `Router(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 12	**ip prefix-list** *list-name* [**seq** *seq-number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] [**eq** *eq-value*] 例：	BGP 関連のプレフィックス リストを定義し、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。

	コマンドまたはアクション	目的
	`Router(config)# ip prefix-list super172 permit 172.0.0.0/8`	• この例では、転送されるルートとして 172.0.0.0/8 だけを許可する、super172 と呼ばれるプレフィックス リストが定義されます。 • すべてのプレフィックス リストの末尾には明示的な拒否があるため、他のルートはすべて拒否されます。
ステップ 13	**end** 例： `Router(config-access-list)# end`	アクセス リスト 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。
ステップ 14	**show ip prefix-list** [**detail** | **summary**] [*prefix-list-name* [**seq** *seq-number* | *network*/*length*[**longer** | **first-match**]]] 例： `Router# show ip prefix-list detail super172`	プレフィックス リストについての情報を表示します。 • この例では、super172 という名前のプレフィックス リストの詳細が、ヒット カウントを含めて表示されます。ヒット カウントとは、エントリがルートに一致した回数のことです。
ステップ 15	**clear ip prefix-list** {* | *ip-address* | *peer-group-name*} **out** 例： `Router# clear ip prefix-list super172 out`	プレフィックス リスト エントリのヒット カウントをリセットします。 • この例では、super172 と呼ばれるプレフィックス リストのヒット カウントがリセットされます。

例

次に示す **show ip prefix-list** コマンドからの出力では、super172 という名前のプレフィックス リストの詳細が、ヒット カウントを含めて表示されます。**clear ip prefix-list** コマンドが入力されてヒット カウントがリセットされ、さらに再度 **show ip prefix-list** コマンドが入力されて、0 にリセットされたヒット カウントが表示されます。

```
Router# show ip prefix-list detail super172

ip prefix-list super172:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 4
   seq 5 permit 172.0.0.0/8 (hit count: 1, refcount: 1)

Router# clear ip prefix-list super172

Router# show ip prefix-list detail super172

ip prefix-list super172:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 4
   seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
```

AS-Path フィルタを使用した BGP プレフィックスのフィルタ処理

フィルタ ルート情報への AS-path 属性の値をベースにしたアクセス リスト付きの AS-path フィルタを使用して BGP プレフィックスをフィルタリングするには、次の作業を実行します。上の図では、AS-path アクセス リストがルータ B で設定されます。アクセス リストの 1 行目では、AS-path 50000 に一致するものがすべて拒否され、2 行目では他のパスすべてが許可されています。ルータは **neighbor filter-list** コマンドを使用して、AS-path アクセス リストをアウトバウンド フィルタとして指定します。フィルタが有効化された後、トラフィックはルータ A とルータ C の両方で受信されますが、自律システム 50000（ルータ C）で生成されたアップデートがルータ B によりルータ A に転送されることはありません。ルータ C からのアップデートのうち、別の自律システムで生成されたものがあった場合、その中には自律システム 50000 だけでなく別の自律システム番号も含まれているため、アップデートは転送されることになり、AS-path アクセス リストとは一致しないことになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression*
4. AS-path アクセス リストで要求されているすべてのエントリについて、手順 3 を繰り返します。
5. **router bgp** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. すべての BGP ピアに手順 6 を繰り返します。
8. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
9. **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}
10. **end**
11. **show ip bgp regexp** *as-regular-expression*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 as-path access-list** *access-list-number* {**deny**	**permit**} *as-regular-expression* 例：	BGP 関連のアクセス リストを定義し、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。

	コマンドまたはアクション	目的
	Device(config)# ip as-path access-list 100 deny ^50000$ **例**： Device(config)# ip as-path access-list 100 permit .*	• 1 番目の例では、アクセス リスト番号 100 は 50000 で始まり 50000 で終わる AS-path はすべて拒否するように定義されています。 • 2 番目の例では、AS-path アクセス リストの 1 番目の例での基準に一致しないルートは、すべて許可されます。ピリオドとアスタリスク記号は AS-path 内のすべての文字が一致することを示しているため、ルータ B はそれらアップデートをルータ A に転送することになります。 （注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。
ステップ 4	AS-path アクセス リストで要求されているすべてのエントリについて、手順 3 を繰り返します。	-
ステップ 5	**router bgp** *autonomous-system-number* **例**： Device(config)# router bgp 45000	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例**： Device(config-router)# neighbor 192.168.1.2 remote-as 40000	指定した自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。
ステップ 7	すべての BGP ピアに手順 6 を繰り返します。	-
ステップ 8	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] **例**： Device(config-router)# address-family ipv4 unicast	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。

	コマンドまたはアクション	目的
		• **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**} 例： `Device(config-router-af)# neighbor 192.168.1.2 filter-list 100 out`	プレフィックス リストで指定された BGP ネイバー情報を配布します。 • この例では、アクセス リスト番号 100 が、ルータ A への発信ルートに設定されます。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ip bgp regexp** *as-regular-expression* 例： `Device# show ip bgp regexp ^50000$`	正規表現に一致するルートを表示します。 • 正規表現の確認にこのコマンドを使用できます。 • この例では、「50000 で始まり 50000 で終わる」表現に一致するパスすべてが表示されます。

例

次の、**show ip bgp regexp** コマンドからの出力は、AS-path が 50000 で始まり 50000 で終わるという正規表現に一致する自律システム パスを表示します。

```
Device# show ip bgp regexp ^50000$

BGP table version is 9, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24      192.168.3.2              0           150 50000 i
```

4バイト自律システム番号を使用したAS-pathフィルタによるBGPプレフィックスのフィルタリング

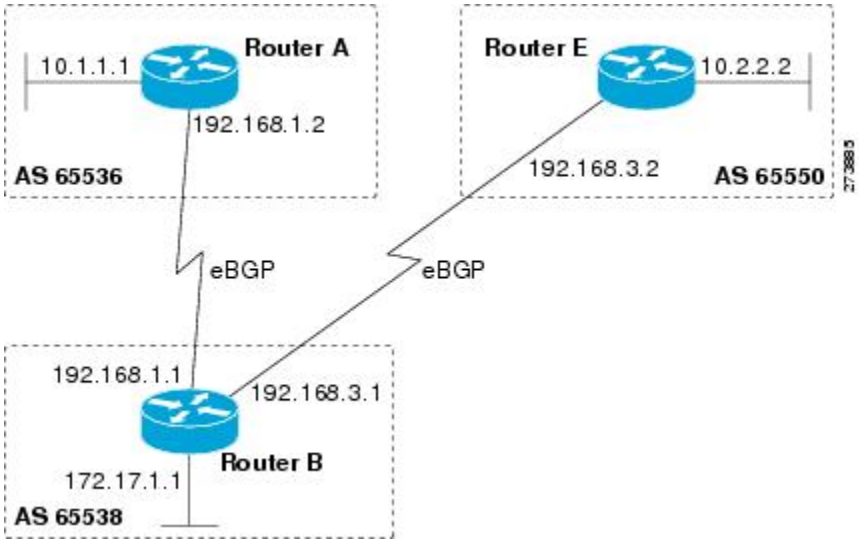
Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースで、BGP は 4 オクテット（4 バイト）自律システム番号をサポートするようになりました。この作業にある 4 バイト自律システム番号は、デフォルトの asplain（10 進数値）形式に

フォーマットされています。たとえば、下の図にあるルータ B の自律システム番号は 65538 です。4 バイト自律システム番号の詳細については、「BGP 自律システム番号の形式」の項を参照してください。

4 バイト自律システム番号とルート情報フィルタ用の AS-path 属性の値に基づくアクセス リストを使用して AS-path フィルタで BGP プレフィックスをフィルタリングするには、次の作業を実行します。下の図では、AS-path アクセス リストがルータ B で設定されます。アクセス リストの 1 行目では、AS パス 65550 に一致するものがすべて拒否され、2 行目では他のパスすべてが許可されています。ルータは **neighbor filter-list** コマンドを使用して、AS-path アクセス リストをアウトバウンド フィルタとして指定します。フィルタ処理が有効化された後、トラフィックはルータ A とルータ E の両方で受信されますが、自律システム 65550（ルータ E）で生成されたアップデートがルータ B によりルータ A に転送されることはありません。ルータ E からのアップデートのうち、別の自律システムで生成されたものがあった場合、その中には自律システム 65550 だけでなく別の自律システム番号も含まれているため、アップデートは転送されることになり、AS-path アクセス リストとは一致しないことになります。

（注） Cisco IOS Release 12.0(22)S、12.2(15)T、12.2(18)S、およびそれ以降のリリースでは、**ip as-path access-list** コマンドを使用して設定できる自律システム アクセス リストの上限値が、199 から 500 に増加しました。

図 *29 : 4* バイト自律システム番号を使用した *AS-path* フィルタによる *BGP* プレフィックス フィルタリングの *BGP* トポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*

5. すべての BGP ピアにステップ 4 を繰り返します。
6. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
7. **network** *network-number* [**mask** *network-mask*]
8. **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number*{**in** | **out**}
9. **exit**
10. **exit**
11. **ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression*
12. AS-path アクセス リストで要求されているすべてのエントリについて、手順 11 を繰り返します。
13. **end**
14. **show ip bgp regexp** *as-regular-expression*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 65538`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.1.2 remote-as 65536`	指定した自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの BGP ネイバー テーブルに追加します。 • この例では、ルータ A でのネイバーの IP アドレスが追加されます。
ステップ 5	すべての BGP ピアにステップ 4 を繰り返します。	--
ステップ 6	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファ

	コマンドまたはアクション	目的
		ミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 7	**network** *network-number* [**mask** *network-mask*] 例： `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。 （注） この例では、一部の構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number*{**in** | **out**} 例： `Router(config-router-af)# neighbor 192.168.1.2 filter-list 99 out`	プレフィックス リストで指定された BGP ネイバー情報を配布します。 • この例では、アクセス リスト番号 99 が、ルータ A への発信ルートに設定されます。
ステップ 9	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Router(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 11	**ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression* 例：	BGP 関連のアクセス リストを定義し、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。

	コマンドまたはアクション	目的

	`Router(config)# ip as-path access-list 99 deny ^65550$`
	例：
	and
	例：
	`Router(config)# ip as-path access-list 99 permit .*`
		• 1 番目の例では、アクセス リスト番号 99 は 65550 で始まり 65550 で終わる AS-path はすべて拒否するように定義されています。
		• 2 番目の例では、AS-path アクセス リストの 1 番目の例での基準に一致しないルートは、すべて許可されます。ピリオドとアスタリスク記号は AS-path 内のすべての文字が一致することを示しているため、ルータ B はそれらアップデートをルータ A に転送することになります。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。

ステップ 12	AS-path アクセス リストで要求されているすべてのエントリについて、手順 11 を繰り返します。	--
ステップ 13	**end** 例： `Router(config-access-list)# end`	アクセス リスト 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 14	**show ip bgp regexp** *as-regular-expression* 例： `Router# show ip bgp regexp ^65550$`	正規表現に一致するルートを表示します。 • 正規表現の確認にこのコマンドを使用できます。 • この例では、「65550 で始まり 65550 で終わる」表現に一致するパスすべてが表示されます。

例

次の、**show ip bgp regexp** コマンドからの出力は、AS-path が 65550 で始まり 65550 で終わるという正規表現に一致する自律システム パスを表示します。

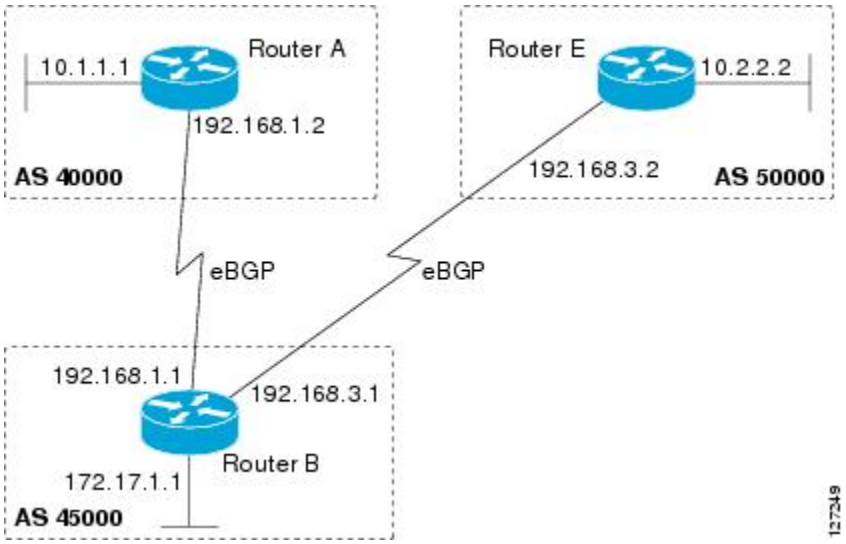
```
RouterB# show ip bgp regexp ^65550$
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24      192.168.3.2              0             0 65550 i
```

コミュニティ リストを使用したトラフィック フィルタリング

BGP コミュニティ リストを作成し、ルート マップ内でそのコミュニティ リストを参照し、そのルートマップをネイバーに適用することによってトラフィックをフィルタ処理するには、次の作業を実行します。

この作業では、受信ルートを制御するために、ルート マップとコミュニティ リストを使用して下の図のルータ B を設定します。

図 *30 :* コミュニティ リストが設定されているトポロジ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in** | **out**}
7. **exit**
8. **exit**
9. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
10. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
11. **set weight** *weight*
12. **exit**
13. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
14. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
15. **set community** *community-number*
16. **exit**

17. **ip community-list** {*standard-list-number* | **standard** *list-name* {**deny** | **permit**} [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]} | {*expanded-list-number* | **expanded** *list-name* {**deny** | **permit**} *regular-expression*}
18. ステップ 17 を繰り返して、必要なコミュニティ リストすべてを作成します。
19. **exit**
20. **show ip community-list** [*standard-list-number* | *expanded-list-number* | *community-list-name*] [**exact-match**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	ネイバーの IP アドレスまたはピア グループ名を、指定した自律システムのローカル ルータの BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。

	コマンドまたはアクション	目的
		• **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 192.168.3.2 route-map 2000 in`	インバウンドまたはアウトバウンドのルートにルート マップを適用します。 • この例では、2000 と呼ばれるルートマップが、192.168.3.2 の BGP ピアからのインバウンド ルートに適用されます。
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 8	**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 9	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map 2000 permit 10`	ルート マップを作成し、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。 • この例では、2000 と呼ばれるルート マップが定義されます。
ステップ 10	**match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]} 例： `Device(config-route-map)# match community 1`	BGP コミュニティ リストのコミュニティとのマッチングを行います。 • この例では、ルートのコミュニティ属性はコミュニティ リスト 1 のコミュニティと一致しています。
ステップ 11	**set weight** *weight* 例： `Device(config-route-map)# set weight 30`	コミュニティ リストに一致する BGP ルートの重み（weight）を設定します。 • この例では、コミュニティ リスト 1 に一致するすべてのルートの重みが 30 に設定されます。
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 モードを終了して、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 13	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map 3000 permit 10`	ルート マップを作成し、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。 • この例では、3000 と呼ばれるルート マップが定義されます。
ステップ 14	**match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]} 例： `Device(config-route-map)# match community 2`	BGP コミュニティ リストのコミュニティとのマッチングを行います。 • この例では、ルートの COMMUNITIES 属性はコミュニティ リスト 2 のコミュニティと一致しています。
ステップ 15	**set community** *community-number* 例： `Device(config-route-map)# set community 99`	BGP コミュニティ属性を設定します。 • この例では、コミュニティ リスト 2 に一致するすべてのルートが、99 に設定された COMMUNITIES 属性を持つことになります。
ステップ 16	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 17	**ip community-list** {*standard-list-number* | **standard** *list-name* {**deny** | **permit**} [*community-number*] [*AA*:*NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]} | {*expanded-list-number* | **expanded** *list-name* {**deny** | **permit**} *regular-expression*}
	例：
	`Device(config)# ip community-list 1 permit 100`
	例：
	`Device(config)# ip community-list 2 permit internet`
		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。
		• 1 番目の例では、コミュニティ リスト 1 は COMMUNITIES 属性が 100 のルートを許可しています。ルータ E のルートはすべて COMMUNITIES 属性が 100 であるため、重みは 30 に設定されます。
		• 2 番目の例では、コミュニティ リスト 2 は **internet** コミュニティを指定することで、効果的にすべてのルートを許可しています。コミュニティ リスト 1 に一致しなかったルートはどれも、コミュニティ リスト 2 でチェックされます。すべてのルートが許可されますが、ルート属性には変化が加えられません。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。

	コマンドまたはアクション	目的
ステップ 18	ステップ 17 を繰り返して、必要なコミュニティ リストすべてを作成します。	-
ステップ 19	**exit** 例： `Device(config)# exit`	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 モードを開始します。
ステップ 20	**show ip community-list** [*standard-list-number* | *expanded-list-number* | *community-list-name*] [**exact-match**] 例： `Device# show ip community-list 1`	設定された BGP コミュニティ リスト エントリを表示します。

例

次の出力例は、コミュニティ リスト 1 が作成されたことを確認し、コミュニティ属性が 100 のルートがコミュニティ リスト 1 で許可されていることを示しています。

```
Device# show ip community-list 1

Community standard list 1
     permit 100
```

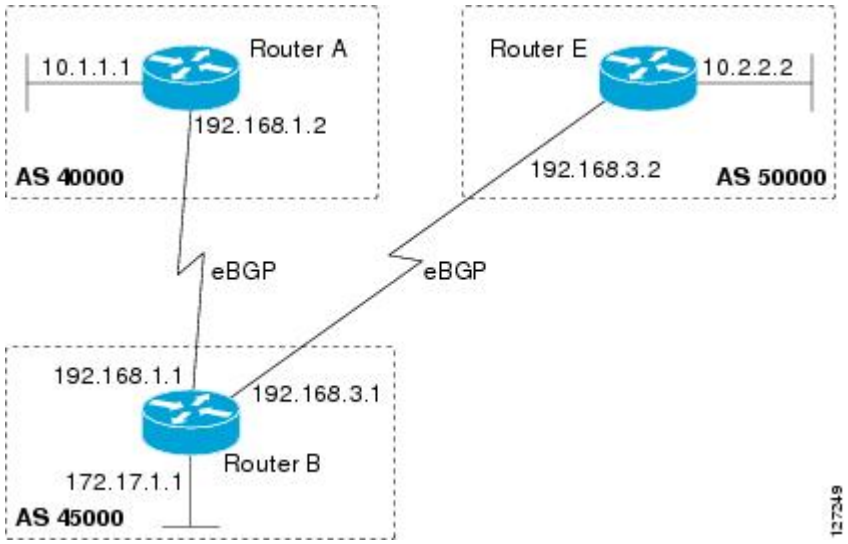
次の出力例は、コミュニティ リスト 2 が作成されたことを確認し、コミュニティ リスト 2 が **internet** キーワードを指定して実質的にすべてのルートを許可していることを示しています。

```
Device# show ip community-list 2

Community standard list 2
     permit internet
```

拡張コミュニティ リストを使用したトラフィック フィルタリング

拡張 BGP コミュニティ リストを作成してアウトバウンド ルートを制御することによりトラフィックをフィルタリングするには、次の作業を実行します。

図 *31* : コミュニティ リストが設定されているトポロジ



この作業において、上の図のルータ B は、拡張名前付きコミュニティ リストを使用して設定され、192.168.1.2 の BGP ピアが自律システム 50000 からの、または 50000 経由のどのパスについてのアドバタイズメントも送られないよう指定されます。IP 拡張コミュニティリスト コンフィギュレーション モードが使用され、エントリのシーケンス番号再割り当て機能が示されます。

（注） 拡張コミュニティ リストのエントリにはすべて、コンフィギュレーション モードにかかわらずデフォルトでシーケンス番号が適用されます。拡張コミュニティ リスト エントリのシーケンス番号の明示的な割り当てと再割り当ては、IP 拡張コミュニティリスト コンフィギュレーション モードだけで設定でき、グローバル コンフィギュレーション モードでは設定できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** {*expanded-list-number* | **expanded** *list-name* | *standard-list-number* | **standard** *list-name*}
4. [*sequence-number*] {**deny** [*regular-expression*] | **exit** | **permit** [*regular-expression*]}
5. 拡張コミュニティ リスト内のすべての必要な許可や拒否エントリについて、ステップ 4 を繰り返します。
6. **resequence** [*starting-sequence*] [*sequence-increment*]
7. **exit**
8. **router bgp** *autonomous-system-number*
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
10. 必要な BGP ピアすべてについて、前の手順を繰り返します。

11. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
12. **network** *network-number* [**mask** *network-mask*]
13. **end**
14. **show ip extcommunity-list** [*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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 extcommunity-list** {*expanded-list-number* | **expanded** *list-name* | *standard-list-number* | **standard** *list-name*} 例： `Device(config)# ip extcommunity-list expanded DENY50000`	IP 拡張コミュニティリスト コンフィギュレーション モードを開始し、拡張コミュニティ リストの作成や設定を行います。 • この例では、拡張コミュニティ リスト DENY50000 が作成されます。

ステップ 4	[*sequence-number*] {**deny** [*regular-expression*] | **exit** | **permit** [*regular-expression*]}
	例：
	`Device(config-extcomm-list)# 10 deny _50000_`
	例：
	`Device(config-extcomm-list)# 20 deny ^50000 .*`
		拡張コミュニティ リスト エントリを設定します。
		• 1 番目の例では、自律システム 50000 からのパスについてのアドバタイズメントを拒否するよう、シーケンス番号 10 の拡張コミュニティ リスト エントリが設定されます。
		• 2 番目の例では、自律システム 50000 を経由するパスについてのアドバタイズメントを拒否するよう、シーケンス番号20の拡張コミュニティ リスト エントリが設定されます。
		（注） 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 5	拡張コミュニティ リスト内のすべての必要な許可や拒否エントリについて、ステップ 4 を繰り返します。	-
ステップ 6	**resequence** [*starting-sequence*] [*sequence-increment*] 例： `Device(config-extcomm-list)# resequence 50 100`	拡張コミュニティ リスト エントリのシーケンス番号を再割り当てします。 • この例では、最初の拡張コミュニティ リスト エントリを 50 に、続くエントリは 100 ずつ増えるように設定されます。そのため、2番目の拡張コミュニティ リスト エントリは 150 になります。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 7	**exit** 例： `Device(config-extcomm-list)# exit`	拡張コミュニティリスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	ネイバーの IP アドレスまたはピア グループ名を、指定した自律システムのローカル ルータの BGP ネイバー テーブルに追加します。
ステップ 10	必要な BGP ピアすべてについて、前の手順を繰り返します。	-
ステップ 11	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファ

	コマンドまたはアクション	目的
		ミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 （注） **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーションモードコマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 12	**network** *network-number* [**mask** *network-mask*] 例： `Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）この自律システムにローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 • 外部プロトコルの場合、**network** コマンドはアドバタイズされるネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 13	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show ip extcommunity-list** [*list-name*] 例： `Device# show ip extcommunity-list DENY50000`	設定された拡張BGP コミュニティ リスト エントリを表示します。

例

次の出力例は、BGP 拡張コミュニティ リスト DENY50000 が作成されたことを確認するもので、出力は自律システム 50000 についてのアドバタイズメントを拒否するエントリのシーケンス番号が、10 と 20 から再割り当てによって 50 と 150 になったことを示しています。

```
Device# show ip extcommunity-list DENY50000

Expanded extended community-list DENY50000
     50 deny _50000_
     150 deny ^50000 .*
```

BGP ルート マップ ポリシー リストを使用したトラフィック フィルタリング

BGP ポリシー リストを作成してルート マップ内で参照するには、次の作業を実行します。

ポリシー リストは、match 句だけを含んだルート マップのようなものです。ポリシー リストに伴う match 句セマンティックやルート マップ機能の変更はありません。match 句はポリシー リスト内で permit と deny 文により設定されます。ルート マップはこれを評価して各 match 句を処理し、設定に基づいてルートの許可や拒否を行います。ルート マップ機能での AND および OR セマンティックは、match 句の扱いについてポリシー リストと同様です。

ポリシー リストにより、中規模以上のネットワークでの BGP ルーティング ポリシー設定を簡素化できます。ネットワーク オペレータは、ルート マップ内で一群の match 句を持つ事前に設定されたポリシー リストを参照することで、BGP ルーティング ポリシーへの一般的な変更を簡単に適用することができます。複数のルート マップのエントリに繰り返し現れる一群の match 句を、ネットワーク オペレータがそれぞれ手動で再設定する必要がなくなりました。

自律システム パスとルータの MED が一致するトラフィックをフィルタリングする BGP ポリシー リストを作成し、それからポリシー リストを参照するルート マップを作成するには、次の作業を実行します。

始める前に

ネットワークで BGP ルーティングが設定され、BGP ネイバーが確立されている必要があります。

（注）

- BGP ルート マップ ポリシー リストは、ポリシー リスト内での IPv6 の match 句の設定をサポートしていません。
- ポリシー リストは、Cisco IOS Release 12.0(22)S および 12.2(15)T よりも前のバージョンの Cisco IOS ソフトウェアではサポートされていません。古いバージョンの Cisco IOS ソフトウェアを実行中のルータをリロードすると、ルーティング ポリシーの設定の一部が失われることがあります。
- ポリシー リストがサポートするのは match 句だけで、set 句はサポートしていません。ただし、ポリシー リストは、ポリシー リストとは別に設定された match および set 句と、同一のルート マップ エントリ内で共存することができます。
- ポリシー リストは BGP だけでサポートされます。他の IP ルーティング プロトコルではサポートされません。この制限が再配布を含めたルートマップの通常動作を妨げることはありません。ポリシー リスト機能は BGP の中で透過的に動作し、他の IP ルーティング プロトコルからは見ることができないからです。
- ポリシー リストがサポートするのは match 句だけで、set 句はサポートしていません。ただし、ポリシー リストは、ポリシー リストとは別に設定された match および set 句と、同一のルート マップ エントリ内で共存することができます。1 番目のルート マップの例では AND セマンティックを設定し、2 番目のルート マップ設定例はセマンティックを設定しています。このセクションの例はいずれも、ポリシー リストと個別の match および set 句サンプル ルート マップ設定とを、同じ設定の中で参照するルート マップのサンプルとなっています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip policy-list** *policy-list-name* {**permit** | **deny**}
4. **match as-path** *as-number*
5. **match metric** *metric*
6. **exit**
7. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
8. **match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*]
9. **match policy-list** *policy-list-name*
10. **set community** *community-number* [**additive**] [*well-known-community*] | **none**}
11. **set local-preference** *preference-value*
12. **end**
13. **show ip policy-list** [*policy-list-name*]
14. **show route-map** [*route-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip policy-list** *policy-list-name* {**permit** | **deny**} 例： `Router(config)# ip policy-list POLICY-LIST-NAME-1 permit`	ポリシー リスト コンフィギュレーション モードを開始し、続く match 句で許容されるルートを許可する BGP ポリシー リストを作成します。
ステップ 4	**match as-path** *as-number* 例： `Router(config-policy-list)# match as-path 500`	指定した自律システム パスからのルートを許可する match 句を作成します。
ステップ 5	**match metric** *metric* 例： `Router(config-policy-list)# match metric 10`	指定したメトリックのルートを許可する match 句を作成します。
ステップ 6	**exit** 例： `Router(config-policy-list)# exit`	ポリシー リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map MAP-NAME-1 permit 10`	ルート マップを作成し、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 8	**match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*] 例： `Router(config-route-map)# match ip address 1`	指定した *access-list-number* または *access-list-name* 引数に一致するルートを許可する match 句を作成します。
ステップ 9	**match policy-list** *policy-list-name* 例：	指定したポリシー リストに一致する句を作成します。

	コマンドまたはアクション	目的
	`Router(config-route-map)# match policy-list POLICY-LIST-NAME-1`	• ポリシー リスト内の match 句すべてが評価され、処理されます。このコマンドで、複数のポリシー リストを参照できます。 • このコマンドはまた、標準の match 句と同様に AND や OR セマンティックをサポートします。
ステップ 10	**set community** *community-number* [**additive**] [*well-known-community*] | **none**} 例： `Router(config-route-map)# set community 10:1`	指定したコミュニティを設定または削除する句を作成します。
ステップ 11	**set local-preference** *preference-value* 例： `Router(config-route-map)# set local-preference 140`	指定したローカル プリファレンス値を設定する句を作成します。
ステップ 12	**end** 例： `Router(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 13	**show ip policy-list** [*policy-list-name*] 例： `Router# show ip policy-list POLICY-LIST-NAME-1`	設定されたポリシー リストとポリシー リスト エントリについての情報を表示します。
ステップ 14	**show route-map** [*route-map-name*] 例： `Router# show route-map`	ローカルで設定されたルート マップとルート マップ エントリを表示します。

例

次の出力例は、ポリシーリストが作成されたことを確認し、ポリシーリスト名と設定された match 句を表示しています。

```
Router# show ip policy-list
 POLICY-LIST-NAME-1

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
    as-path (as-path filter): 1
```

（注） ポリシー リスト名は、**show ip policy-list** コマンドが入力されたときに指定できます。このオプションは、このコマンドの出力をフィルタリングして、1 つのポリシー リストを確認するときに便利です。

次の **show route-map** コマンドの出力例は、ルート マップが作成され、ポリシー リストが参照されたことを確認します。このコマンドの出力は、ルート マップ名と、設定されたルート マップで参照されたポリシー リストとを表示します。

```
Router# show route-map

route-map ROUTE-MAP-NAME-1, deny, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME-1, permit, sequence 10
  Match clauses:
    IP Policy lists:
        POLICY-LIST-NAME-1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
7. **exit**
8. **exit**
9. **route-map** *map-name* {**permit** | **deny**} [*sequence-number*]
10. **match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*]
11. **set community** { { [*community-number*] [*well-known-community*] [**additive**]} | **none**}
12. **continue** [*sequence-number*]
13. **end**
14. **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	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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 50000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 10.0.0.1 route-map ROUTE-MAP-NAME in`	インバウンド ルート マップを指定されたネイバーから受信したルートに適用します。もしくは、アウトバウンド ルート マップを指定されたネイバーへアドバタイズされたルートへ適用します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 8	**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 9	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME permit 10`	ルート マップ コンフィギュレーション モードを開始し、ルート マップを作成または設定します。
ステップ 10	**match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*] 例： `Device(config-route-map)# match ip address 1`	ポリシー ルーティングとルート フィルタリングが発生する条件を指定する **match** コマンドを設定します。 • 複数の **match** コマンドを設定できます。**match** コマンドが設定された場合、continue 文は一致が出現した場合にのみ実行されます。**match** コマンドが設定されない場合、set および continue 句は実行されます。 （注） この作業で使用する **match** コマンドおよび **set** コマンドは、**continue** コマンドの動作を記述するための例です。具体的な **match** コマンドおよび **set** コマンドのリストについては、『*Cisco IOS IP Routing: BGP Command Reference*』の **continue** コマンドを参照してください。
ステップ 11	**set community** { { [*community-number*] [*well-known-community*] [**additive**]} | **none**} 例： `Device(config-route-map)# set community 10:1`	**set** コマンドを設定して、**match** コマンドで適用された条件が満たされた場合のルーティング アクションを指定します。 • 複数の **set** コマンドを設定できます。 • この例では、指定した aa:nn 形式のコミュニティ番号をセットする句が作成されます。
ステップ 12	**continue** [*sequence-number*] 例：	一致が出現した後も match 文の評価と実行を継続するよう、ルート マップを設定します。

	コマンドまたはアクション	目的
	`Device(config-route-map)# continue`	• シーケンス番号が指定された場合、continue 句は指定されたシーケンス番号のルート マップへ移動します。 • シーケンス番号が指定されない場合、continue 句はその次のシーケンス番号のルート マップへ移動します。この動作は、「黙示的継続」と呼ばれます。
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show route-map** [*map-name*] 例： `Device# show route-map`	（任意）ローカルで設定されたルート マップを表示します。出力をフィルタリングするためのルート マップ名は、このコマンドの構文内で指定できます。

例

次に、**show route-map** コマンドを使用して continue 句の設定を確認する方法の出力例を示します。設定されたルート マップが、match、set、および continue 句を含め、出力に表示されます。

```
Device# show route-map

route-map MARKETING, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 40
  Match clauses:
    community (community-list filter): 10:1
```

```
  Set clauses:
    local-preference 104
  Policy routing matches: 0 packets, 0 bytes
route-map MKTG-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

外部BGPを使用したサービス プロバイダーとの接続の設定例

例：インバウンド パス選択の変化

次に、ルート マップを使用してネイバーからの受信データを変更する方法の例を示します。10.222.1.1 から受信した、自律システム アクセス リスト 200 で設定されたフィルタ パラメータに一致するルートはどれも、その weight は 200 に、ローカル プリファレンスは 250 に設定され、それが受け入れられることになります。

```
router bgp 100
!
 neighbor 10.222.1.1 route-map FIX-WEIGHT in
 neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map FIX-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight 200
```

次の例では、FINANCE という名前のルート マップが、自律システム 690 で生成されたパスすべてを、MED メトリック属性 127 でマークしています。2 番目の permit 句は、自律システム パス リスト 1 に一致しないルートを引き続きネイバー 10.1.1.1 へ送るために必要です。

```
router bgp 65000
 neighbor 10.1.1.1 route-map FINANCE out
!
ip as-path access-list 1 permit ^690_
ip as-path access-list 2 permit .*
!
route-map FINANCE permit 10
 match as-path 1
 set metric 127
!
route-map FINANCE permit 20
 match as-path 2
```

インバウンド ルート マップはプレフィックスベースのマッチングを行って、アップデートのさまざまなパラメータを設定できます。自律システム パスとコミュニティ リスト マッチングに加え、インバウンド プレフィックス マッチングが利用できます。次に、SET-LOCAL-PREF

というルート マップ コンフィギュレーション コマンドでどのようにインバウンド プレフィックス 172.20.0.0/16 のローカル プリファレンスを 120 に設定するかを例に示します。

```
!
router bgp 65100
 network 10.108.0.0
 neighbor 10.108.1.1 remote-as 65200
 neighbor 10.108.1.1 route-map SET-LOCAL-PREF in
!
route-map SET-LOCAL-PREF permit 10
 match ip address 2
 set local-preference 120
!
route-map SET-LOCAL-PREF permit 20
!
access-list 2 permit 172.20.0.0 0.0.255.255
access-list 2 deny any
```

例：4 バイト AS 番号を使用した AS-path 属性の変更によるインバウンド パス選択の変化

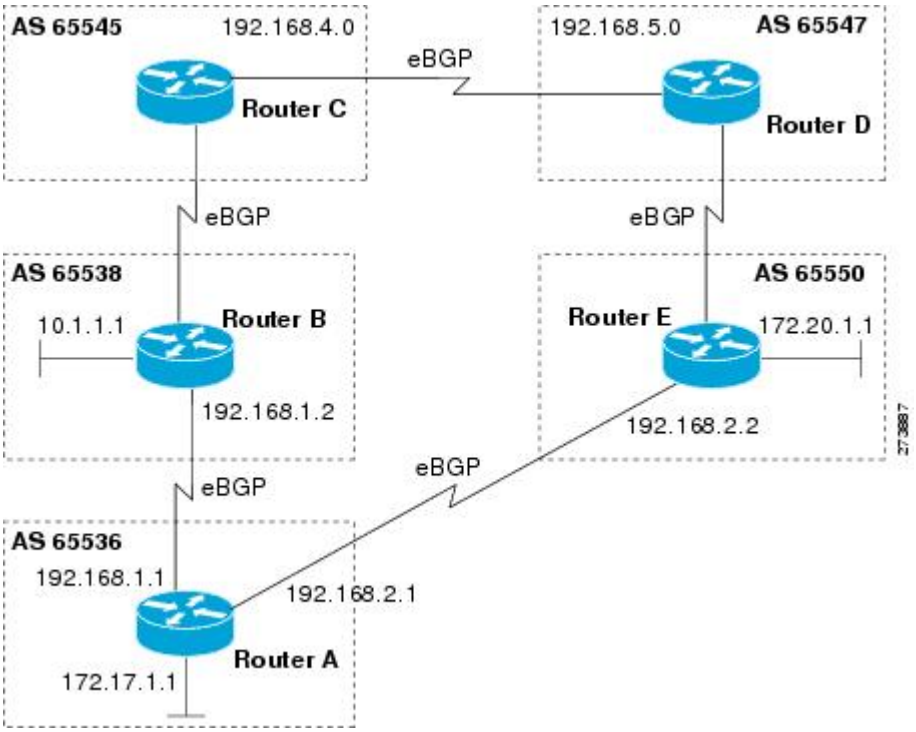
この例は、AS-path 属性の変更によって 172.17.1.0 宛てトラフィックのインバウンド パス選択を変化させるために BGP を設定する方法を示します。Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースで、BGP は 4 オクテット（4 バイト）自律システム番号をサポートするようになりました。この例にある 4 バイト自律システム番号は、デフォルトの asplain（10 進数値）形式にフォーマットされています。たとえば、下の図にあるルータ B の自律システム番号は 65538 です。4 バイト自律システム番号の詳細については、「BGP 自律システム番号の形式」の項を参照してください。

AS-path 属性の変更は、別の自律システムのパス選択を変化させるために BGP で使用可能な方法の 1 つです。たとえば、下の図において、ルータ A は自身のネットワーク 172.17.1.0 を、自律システム 65538 および自律システム 65550 にある BGP ピアにアドバタイズします。ルーティング情報が自律システム 65545 に伝播されるとき、自律システム 65545 内のルータは、2 つの異なるルートからのネットワーク 172.17.1.0 の到達可能性情報を持つことになります。1 番目のルートは、65538 と 65536 で構成される AS-path を備えた自律システム 65538 によるものです。2 番目のルートは自律システム 65547 を経由するもので、AS-path は 65547、65550、65536 です。他の BGP 属性がすべて同じだとすれば、自律システム 65545 内のルータ C はネットワーク 172.17.1.0 へのトラフィックのルートとして、自律システム 65538 を通るルートを選択します。通過した自律システムという点では最短ルートとなるからです。

自律システム 65536 は自律システム 65545 のネットワーク 172.17.1.0 へのトラフィックすべてを自律システム 65538 のルータ B 経由で受信するようになります。しかし、自律システム 65538 と自律システム 65536 の間のリンクが非常に遅く輻輳している場合、**set as-path prepend** コマンドをルータ A で使用して、自律システム 65538 経由のルートが自律システム 65550 経由のパスよりも遠いように見せることで、172.17.1.0 ネットワークへのインバウンド パス選択を変化させることができます。下の図のルータ A の設定は、アウトバウンド BGP アップデートをルータ B に適用することで完了します。**set as-path prepend** コマンドの使用により、ルータ A からルータ B へのアウトバウンド BGP アップデートはすべて、ローカル自律システム番号 65536 を 2 回追加するよう変更された AS-path 属性を持つようになります。この設定の後、自律シス

テム 65545 は 172.17.1.0 ネットワークについてのアップデートを、自律システム 65538 経由で受け取ることになります。新しい AS-path は 65538、65536、65536、65536 となり、これは自律システム 65547 からの AS-path（65547、65550、65536 で変更なし）よりも長くなります。自律システム 65545 内のネットワーキング デバイスは、172.17.1.0 ネットワーク内の宛先アドレスを持つパケットを転送するときに、自律システム 65547 経由のルートを優先するようになります。

図 *32 : AS-path* 属性変更のネットワーク トポロジ



この例の設定は、上の図のルータ A で実行されます。

```
router bgp 65536
 address-family ipv4 unicast
  network 172.17.1.0 mask 255.255.255.0
  neighbor 192.168.1.2 remote-as 65538
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 route-map PREPEND out
  exit-address-family
 exit
route-map PREPEND permit 10
set as-path prepend 65536 65536
```

例：プレフィックス リストによる BGP プレフィックスのフィルタ処理

ここでは、次の例について説明します。

例：シングル プレフィックス リストを使用した BGP プレフィックスのフィルタ処理

次に、プレフィックス リストでデフォルト ルート 0.0.0.0/0 を拒否する例を示します。

```
ip prefix-list abc deny 0.0.0.0/0
```

次に、プレフィックス リストでプレフィックス 10.0.0.0/8 に一致するルートを許可する例を示します。

```
ip prefix-list abc permit 10.0.0.0/8
```

次の例に、プレフィックス長が /8 ～ /24 のプレフィックスだけを受け入れるように BGP プロセスを設定する方法を示します。

```
router bgp 40000
 network 10.20.20.0
 distribute-list prefix max24 in
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

次に、プレフィックス 10.1.1.0/24 がルーティング テーブルに存在する場合に、条件付きでデフォルト ルート（0.0.0.0/0）を RIP に生成する設定例を示します。

```
ip prefix-list cond permit 10.1.1.0/24
!
route-map default-condition permit 10
 match ip address prefix-list cond
!
router rip
 default-information originate route-map default-condition
```

次の例に、プレフィックスの長さによるフィルタリングに加え、192.168.1.1 からのルーティング アップデートだけを受け入れるよう BGP を設定する方法を示します。

```
router bgp 40000
 distribute-list prefix max24 gateway allowlist in
!
ip prefix-list allowlist seq 5 permit 192.168.1.1/32
!
```

次に、name1 を使用してプレフィックスへの受信アップデートをフィルタ処理し、アップデートされているプレフィックスのゲートウェイ（ネクスト ホップ）をプレフィックス リスト name2 へマッチングするよう、ギガビット イーサネット インターフェイス 0/0/0 上で BGP プロセスに指示する例を示します。

```
router bgp 103
 distribute-list prefix name1 gateway name2 in gigabitethernet 0/0/0
```

例：プレフィックスのグループを使用した BGP プレフィックスのフィルタ処理

次に、ネットワーク 192/8 でプレフィックス長が 24 以下のルートを許可するよう BGP を設定する例を示します。

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

次に、192/8 でプレフィックス長が 25 より大きいルートを拒否するよう BGP を設定する例を示します。

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

次に、すべてのアドレス空間でプレフィックス長が 8 より大きく 24 より小さいルートを許可するよう BGP を設定する例を示します。

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次に、すべてのアドレス空間でプレフィックス長が 25 より大きいルートを拒否するよう BGP を設定する例を示します。

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

次に、ネットワーク 10/8 のルートをすべて拒否するよう BGP を設定する例を示します。これは、クラス A ネットワーク 10.0.0.0/8 内のルートのマスクが 32 ビット以下である場合、そのルートが拒否されるためです。

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

次に、192.168.1.0/24 でマスクが 25 より大きいルートを拒否するよう BGP を設定する例を示します。

```
ip prefix-list abc deny 192.168.1.0/24 ge 25
```

次に、すべてのルートを許可するよう BGP を設定する例を示します。

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

例：プレフィックス リスト エントリの追加と削除

プレフィックス リストの初期設定が次のようになっている場合、プレフィックス リスト内のエントリを個別に追加、削除できます。

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 192.168.0.0/15
```

次に、プレフィックス リストからエントリを削除して 192.168.0.0 を許可しないようにし、10.0.0.0/8 を許可する新しいエントリを追加する例を示します。

```
no ip prefix-list abc permit 192.168.0.0/15
ip prefix-list abc permit 10.0.0.0/8
```

新しい設定は次のようになります。

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 10.0.0.0/8
```

例：COMMUNITIES 属性を使用したトラフィックのフィルタ処理

この項では、BGP COMMUNITIES 属性とルート マップを使用した 2 つの例を示します。

1 番目の例では、*set-community* というルート マップを設定し、ネイバー 172.16.232.50 のアウトバウンド アップデートに適用します。アクセス リスト 1 を渡すルートには、well-known COMMUNITIES 属性値 **no-export** を指定します。残りのルートは通常どおりアドバタイズされます。**no-export** コミュニティ値は、自律システム 200 内の BGP スピーカーがそれらのルートのアドバタイズメントを行うのを自動的に防止します。

```
router bgp 100
 neighbor 172.16.232.50 remote-as 200
 neighbor 172.16.232.50 send-community
 neighbor 172.16.232.50 route-map set-community out
!
route-map set-community permit 10
 match address 1
 set community no-export
!
route-map set-community permit 20
 match address 2
```

2 番目の例では、*set-community* というルート マップを設定し、ネイバー 172.16.232.90 のアウトバウンド アップデートに適用します。自律システム 70 で生成されるルートはすべて、COMMUNITIES 属性値 200 200 を自身の既存のコミュニティに追加します。他のルートはすべて、通常と同じようにアドバタイズされます。

```
route-map bgp 200
 neighbor 172.16.232.90 remote-as 100
 neighbor 172.16.232.90 send-community
 neighbor 172.16.232.90 route-map set-community out
!
route-map set-community permit 10
 match as-path 1
 set community 200 200 additive
!
route-map set-community permit 20
!
ip as-path access-list 1 permit 70$
ip as-path access-list 2 permit .*
```

例：AS-Path フィルタを使用したトラフィックのフィルタ処理

次に、ネイバーによる BGP パス フィルタリングの例を示します。自律システム パス access list 2 を通過するルートだけが 192.168.12.10 に送られます。同様に、access list 3 を通過するルートだけが 192.168.12.10 から受け入れられます。

```
router bgp 200
 neighbor 192.168.12.10 remote-as 100
 neighbor 192.168.12.10 filter-list 1 out
 neighbor 192.168.12.10 filter-list 2 in
 exit
ip as-path access-list 1 permit _109_
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
```

```
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

例：4バイト自律システム番号を使用したAS-pathフィルタによるトラフィックのフィルタ処理

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次の例は Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースで使用できるもので、4 バイト自律システム番号を asplain 形式で使用し、ネイバーによる BGP パス フィルタリングを行います。自律システム パス access list 2 を通過するルートだけが 192.168.3.2 に送られます。

```
ip as-path access-list 2 permit ^65536$
router bgp 65538
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 65550
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 filter-list 2 in
  end
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次の例は Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースで使用できるもので、4 バイト自律システム番号を asdot 形式で使用し、ネイバーによる BGP パス フィルタリングを行います。自律システム パス access list 2 を通過するルートだけが 192.168.3.2 に送られます。

（注） Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、この例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して、asdot をデフォルトの表示形式として設定した場合だけです。

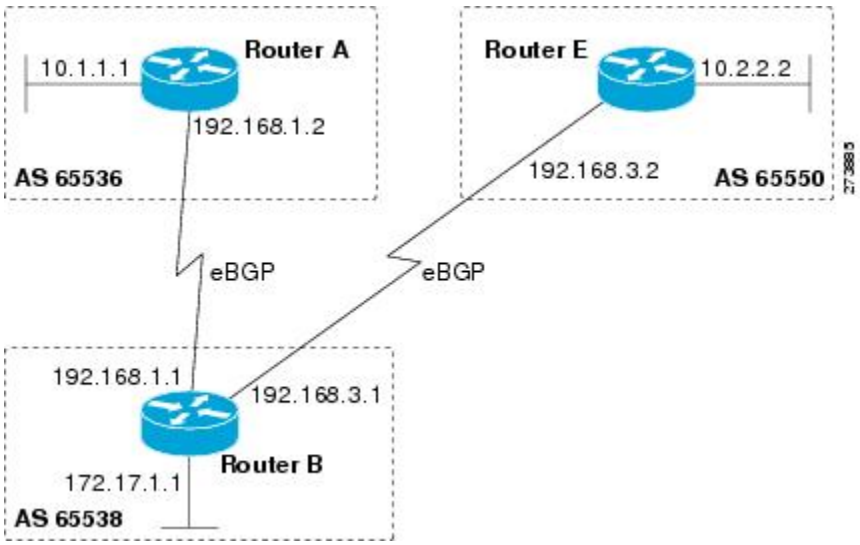
```
ip as-path access-list 2 permit ^1\.0$
router bgp 1.2
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.3.2 filter-list 2 in
  end
```

例：4 バイト自律システム番号と拡張コミュニティ リストを使用したトラフィックのフィルタ処理

Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)SXI1、およびそれ以降のリリースにおける asplain デフォルト形式

次に、アウトバウンド ルートを制御するために拡張 BGP コミュニティ リストを作成することによるトラフィック フィルタリングの例を示します。Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、拡張 BGP コミュニティはデフォルトで asplain の正規表現中の 4 バイト自律システム番号をサポートしています。拡張コミュニティ リストは、VRF インスタンスと MPLS VPN のルートを設定し、フィルタリングし、識別するために使用されます。名前付きまたは番号付きコミュニティ リストの設定には、**ip extcommunity-list** コマンドを使用します。アクセス リストの標準ルールすべてが、拡張コミュニティ リストの設定に適用されます。正規表現は、拡張コミュニティ リスト番号の拡張範囲によってサポートされています。

図 *33 : asplain* 形式の *4* バイト自律システム番号と拡張コミュニティ リストを使用したトラフィック フィルタリングの *BGP* トポロジ



（注） 拡張コミュニティ リストのエントリにはすべて、コンフィギュレーション モードにかかわらずデフォルトでシーケンス番号が適用されます。拡張コミュニティ リスト エントリのシーケンス番号の明示的な割り当てと再割り当ては、IP 拡張コミュニティリスト コンフィギュレーション モードだけで設定でき、グローバル コンフィギュレーション モードでは設定できません。

この例では、上の図は、拡張名前付きコミュニティ リストを使用して設定され、192.168.1.2 の BGP ピアが 4 バイト自律システム 65550 からの、または 65550 経由のどのパスについてのアド

バタイズメントも送られないよう指定されます。IP拡張コミュニティリストコンフィギュレーション モードが使用され、エントリのシーケンス番号再割り当て機能が示されます。

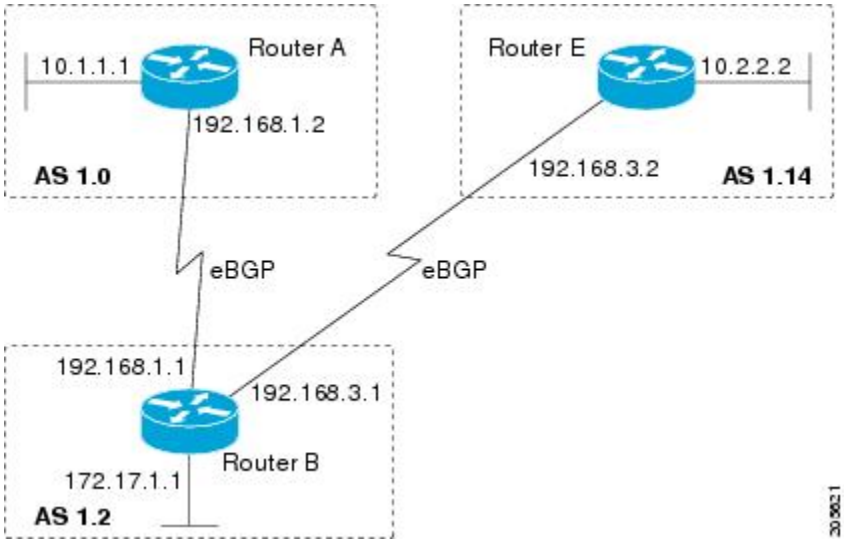
```
ip extcommunity-list expanded DENY65550
 10 deny _65550_
 20 deny ^65550 .*
 resequence 50 100
 exit
router bgp 65538
 network 172.17.1.0 mask 255.255.255.0
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 65550
  neighbor 192.168.1.2 remote-as 65536
  neighbor 192.168.3.2 activate
  neighbor 192.168.1.2 activate
  end
show ip extcommunity-list DENY65550
```

Cisco IOS Release 12.0(32)S12 および 12.4(24)T における asdot デフォルト形式

次に、アウトバウンド ルートを制御するために拡張 BGP コミュニティ リストを作成することによるトラフィック フィルタリングの例を示します。Cisco IOS Release 12.0(32)S12、12.4(24)T、およびそれ以降のリリースでは、拡張 BGP コミュニティは正規表現中の 4 バイト自律システム番号を asdot 形式だけでサポートします。拡張コミュニティ リストは、VRF インスタンスと MPLS VPN のルートを設定し、フィルタリングし、識別するために使用されます。名前付きまたは番号付きコミュニティ リストの設定には、**ip extcommunity-list** コマンドを使用します。アクセス リストの標準ルールすべてが、拡張コミュニティ リストの設定に適用されます。正規表現は、拡張コミュニティ リスト番号の拡張範囲によってサポートされています。

（注） Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースでは、この例が正常に動作するのは、**bgp asnotation dot** コマンドを使用して、asdot をデフォルトの表示形式として設定した場合だけです。

図 *34 : asdot* 形式の *4* バイト自律システム番号と拡張コミュニティ リストを使用したトラフィック フィルタリングの *BGP* トポロジ



（注） 拡張コミュニティ リストのエントリにはすべて、コンフィギュレーション モードにかかわらずデフォルトでシーケンス番号が適用されます。拡張コミュニティ リスト エントリのシーケンス番号の明示的な割り当てと再割り当ては、IP 拡張コミュニティリスト コンフィギュレーション モードだけで設定でき、グローバル コンフィギュレーション モードでは設定できません。

この例では、上の図は、拡張名前付きコミュニティ リストを使用して設定され、192.168.1.2 の BGP ピアが 4 バイト自律システム 65550 からの、または 65550 経由のどのパスについてのアドバタイズメントも送られないよう指定されます。IP 拡張コミュニティリスト コンフィギュレーション モードが使用され、エントリのシーケンス番号再割り当て機能が示されます。

```
ip extcommunity-list expanded DENY114
 10 deny _1\.14_
 20 deny ^1\.14 .*
 resequence 50 100
 exit
router bgp 1.2
 network 172.17.1.0 mask 255.255.255.0
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.1.2 remote-as 1.0
  neighbor 192.168.3.2 activate
  neighbor 192.168.1.2 activate
  end
show ip extcommunity-list DENY114
```

例：BGP ルート マップを使用したトラフィックのフィルタ処理

次に、アクセス リスト 1 に一致している場合、ネイバー 10.1.1.1 からのユニキャストおよびマルチキャスト ルートを受け入れるように、アドレス ファミリを使用して BGP を設定する例を示します。

```
route-map filter-some-multicast
 match ip address 1
 exit
router bgp 65538
 neighbor 10.1.1.1 remote-as 65537
 address-family ipv4 unicast
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 route-map filter-some-multicast in
  exit
 exit
router bgp 65538
 neighbor 10.1.1.1 remote-as 65537
 address-family ipv4 multicast
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 route-map filter-some-multicast in
  end
```

次の作業

- BGP の拡張機能を設定する場合は、「BGP の拡張機能の設定」モジュールに進んでください。
- BGP ネイバー セッション オプションを設定する場合は、「BGP ネイバー セッション オプションの設定」モジュールに進んでください。
- 内部 BGP 機能を設定する場合は、「内部 BGP 機能の設定」モジュールに進んでください。

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』
BGP 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、コマンド履歴、使用上の注意事項、および例	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概要	「Cisco BGP 概要」モジュール
BGP 基本作業の設定	「基本 BGP ネットワークの設定」モジュール

関連項目	マニュアル タイトル
BGP の基礎と説明	『*Large-Scale IP Network Solutions*』Khalid Raza、Mark Turner（Cisco Press, 2000）
拡張可能なネットワークへの BGP の実装と制御	『*Building Scalable Cisco Networks*』Catherine Paquet、Diane Teare（Cisco Press, 2001）
ドメイン間ルーティングの基本	『*Internet Routing Architectures*』Bassam Halabi（Cisco Press, 1997）

標準

標準	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB のリンク
CISCO-BGP4-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

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』

RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4684	『*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*』
RFC 4893	『*BGP Support for Four-Octet AS Number Space*』
RFC 5291	『*Outbound Route Filtering Capability for BGP-4*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

外部BGPを使用したサービス プロバイダーとの接続の機能情報

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

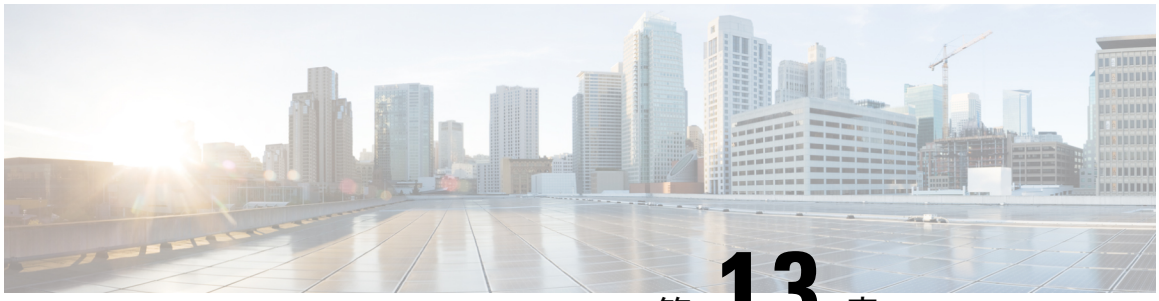
けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *28 :* 外部 *BGP* を使用したサービス プロバイダーとの接続の機能情報

機能名	リリース	機能の設定情報
BGPがサポートする番号付き AS-path アクセス リストの数が 500 に増加	12.0(22)S 12.2(15)T 12.2(18)S 12.2(18)SXD 12.2(27)SBC 15.0(1)S	BGP がサポートする番号付き AS-path アクセス リストの数が 500 に増加したことにより、**ip as-path access-list** コマンドを使用して設定できる自律システム アクセス リストの最大数が 199 から 500 に増加しました。
BGP名前付きコミュニティ リスト	12.2(8)T 12.2(14)S 15.0(1)S	BGP名前付きコミュニティ リスト機能により、名前付きコミュニティリストと呼ばれる新しいタイプのコミュニティリストが導入されます。BGP名前付きコミュニティリスト機能により、ネットワーク オペレータはコミュニティリストに意味がわかりやすい名前を割り当てることができるようになり、設定可能なコミュニティリストの数も増加しました。名前付きコミュニティリストは、正規表現や番号付きコミュニティリストによって設定可能です。番号付きコミュニティのルールは、名前付きコミュニティリストに設定可能なコミュニティ属性数の上限がないことを除き、すべて名前付きコミュニティリストにも適用されます。

機能名	リリース	機能の設定情報
BGP ルートマップ ポリシー リストのサポート	12.0(22)S 12.2(15)T 12.2(18)S 12.2(18)SXD 12.2(27)SBC 15.0(1)S	BGP ルート マップ ポリシー リスト サポート機能により、BGP ルートマップに新しい機能性が追加されます。ネットワーク オペレータはこの機能を使用して、ルートマップの match 句をポリシー リストと呼ばれる名前付きリストにグループ化できます。ポリシー リスト機能はマクロに似ています。ルートマップでポリシー リストが参照されると、match 句がすべて評価され、ルートマップで直接設定された場合と同様に処理されます。この機能強化により、中規模から大規模のネットワークでの BGP ルーティング ポリシーの BGP 設定が単純になりました。ネットワーク オペレータが match 句のグループを持つポリシー リストを事前に設定しておき、さまざまなルートマップ内でそれらのポリシー リストを参照できるからです。複数のルートマップのエントリに繰り返し現れる一群の match 句を、ネットワーク オペレータがそれぞれ手動で再設定する必要がなくなりました。
名前付き拡張コミュニティ リストに対する BGP サポート	12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.3(11)T 15.0(1)S	名前付き拡張コミュニティ リストに対する BGP サポート機能により、既存の数字形式に加え、名前を使用しても拡張コミュニティ リストを設定できるようになりました。
拡張コミュニティ リストのシーケンス エントリに対する BGP サポート	12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.3(11)T 15.0(1)S	拡張コミュニティ リスト内のシーケンスされたエントリに対する BGP サポート機能により、BGP 拡張コミュニティ リスト内の個別のエントリに自動シーケンスが導入されます。この機能により、既存の拡張コミュニティ リスト全体を削除することなく、拡張コミュニティ リスト エントリの削除やシーケンス再割り当てを行うことも可能になりました。
BGP 4 プレフィックス フィルタおよびインバウンド ルート マップ	Cisco IOS XE 3.1.0SG	



第 13 章

BGP ルート マップ継続

BGP ルート マップ継続機能により、continue 句が BGP ルート マップ コンフィギュレーションに導入されます。continue 句によって、ポリシー設定とルート フィルタリングのプログラム性は高まり、正常な match および set 句によってエントリが実行された後に追加のエントリを実行する機能が導入されます。continue 句によって、ネットワーク オペレータはポリシー定義をさらにモジュール化して設定できるようになり、特定のポリシー設定を同じルートマップ内で繰り返す必要がなくなりました。

- 機能情報の確認 （391 ページ）
- BGP ルート マップ継続に関する情報 （392 ページ）
- BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理の方法 （393 ページ）
- BGP ルート マップ継続の設定例 （397 ページ）
- その他の参考資料 （399 ページ）
- BGP ルート マップ継続の機能情報 （399 ページ）

機能情報の確認

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

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

BGP ルート マップ継続に関する情報

continue 句を使用した BGP ルート マップ

BGPルートマップ コンフィギュレーションでは、continue句によって、ポリシー設定とルート フィルタリングのプログラム性が高まり、正常な match および set 句によってエントリが実行された後に追加のエントリを実行する機能が導入されました。continue 句によって、ポリシー定義をさらにモジュール化して設定できるようになり、特定のポリシー設定を同じルートマップ内で繰り返す必要がなくなります。continue 句の導入以前は、ルートマップの設定はリニア的であり、ルート マップのフローを制御することがまったくできませんでした。

continue 句を使用しないルート マップの動作

ルート マップは一致が出現するまで match 句を評価します。一致が出現すると、ルート マップは match 句の評価を停止し、設定された順序で set 句の実行を開始します。一致が出現しない場合、ルート マップはマッチングに「失敗」し、ルート マップの次のシーケンス番号を評価します。これをすべての設定されたルート マップ エントリが評価されるか、一致が出現するまで続けます。各ルートマップは、エントリを識別するシーケンス番号でタグ付けされています。ルートマップエントリは、シーケンス番号が最小のものから評価が始まり、最大のシーケンス番号を持つもので終わります。ルートマップに set 句だけが含まれる場合、set 句は自動的に実行され、ルート マップは他のルート マップ エントリを評価しません。

continue 句を使用したルート マップの動作

continue 句を設定すると、ルート マップは一致が出現した後も、指定されたルート マップ エントリで match 句の評価と実行を続けます。continue 句は、シーケンス番号を指定することで特定のルート マップ エントリに移動する（ジャンプする）よう設定できます。シーケンス番号が指定されていない場合、continue句は次のシーケンス番号へ移動します。この動作は、「黙示的継続」と呼ばれます。match 句がある場合、continue 句は一致が出現した場合にだけ実行されます。一致が出現しなかった場合、continue 句は無視されます。

continue 句を使用した match 動作

match 句がルート マップ エントリに存在しないのに continue 句が存在する場合、continue 句は自動的に実行され、指定されたルート マップ エントリへ移動します。ルート マップ エントリに match 句が存在する場合、continue 句は一致が出現した場合にだけ実行されます。一致が出現し、かつ continue 句が存在する場合、ルート マップは set 句を実行し、それから指定されたルート マップ エントリへ移動します。その次のルート マップ エントリに continue が含まれている場合、ルート マップは一致が出現すればその continue 句を実行します。continue 句がその次のルート マップ エントリに存在しない場合、ルート マップは通常どおり評価されます。continue句がその次のルートマップエントリに存在するが一致が出現しない場合、ルートマップは継続せずに「失敗」し、その次のシーケンス番号が存在すればそこへ移動します。

（注） ルート マップ内の match community 句のコミュニティ リスト数が 1 行で 256 文字を超える場合は、新しい行で複数の match community 文の不揮発性生成（NVGEN）を行う必要があります。

continue 句を使用した Set 動作

set 句は、match 句の評価中は残しておかれ、ルート マップ評価が完了した後に実行されます。set 句は、設定された順番に評価され、処理されます。ルート マップに match 句が存在しない場合を除き、set 句は一致が出現した後にだけ実行されます。continue 文は、設定された set アクションが実行された後にだけ、指定のルート マップ エントリへと進みます。set アクションが最初のルート マップで発生し、それから後続のルート マップ エントリにおいて再び同じ set アクションが異なる値で発生した場合、同じ **set** コマンドで設定された set アクションは、**set** コマンドが複数の値を許可する場合を除き、最後の set アクションによってそれ以前のものが上書きされます。たとえば、**set as-path prepend** コマンドは複数の自律システム番号の設定を許可しています。

（注） ルート マップ エントリに match 句が含まれない場合、continue 句は一致の出現なしで実行できます。

（注） ルートマップはリニア動作であり、入れ子動作ではありません。あるルートがいったんcontinue コマンド句を伴ったルート マップ許可エントリで一致すると、ルート マップ末尾の黙示的拒否により処理されません。例については、「例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理」の項を参照してください。

BGPルートマップでのcontinue句の使用によるトラフィックのフィルタ処理の方法

BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング

BGP ルート マップで continue 句を使用してトラフィックのフィルタリングを行うには、次の作業を実行します。

（注） continue 句ではより大きな値のエントリ（シーケンス番号が自身より大きいルート マップ エントリ）にだけ移動できます。小さな値のルート マップ エントリには移動できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** {*ip-address*| *peer-group-name*} **route-map** *map-name* {**in** | **out**}
6. **exit**
7. **route-map** *map-name* {**permit** | **deny**} [*sequence-number*]
8. **match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*]
9. **set community** *community-number* [**additive**] [*well-known-community*] | **none**}
10. **continue** [*sequence-number*]
11. **end**
12. **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	**enable** 例： `Device> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** {*ip-address*| *peer-group-name*} **route-map** *map-name* {**in**	**out**} 例： `Device(config-router)# neighbor 10.0.0.1 route-map ROUTE-MAP-NAME in`	インバウンド ルート マップを指定されたネイバーから受信したルートに適用します。もしくは、アウトバウンド ルート マップを指定されたネイバーへアドバタイズされたルートへ適用します。

	コマンドまたはアクション	目的
ステップ 6	**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 7	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME permit 10`	ルート マップ コンフィギュレーション モードを開始し、ルート マップを作成または設定します。
ステップ 8	**match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*] 例： `Device(config-route-map)# match ip address 1`	ポリシー ルーティングとルート フィルタリングが発生する条件を指定する **match** コマンドを設定します。 • 複数の **match** コマンドを設定できます。**match** コマンドが設定された場合、continue 文が実行されるには一致の発生が必要になります。**match** コマンドが設定されない場合、set および continue 句は実行されます。 （注） この作業で使用する **match** コマンドおよび **set** コマンドは、**continue** コマンドの動作を記述するための例です。具体的な **match** コマンドおよび **set** コマンドのリストについては、『*Cisco IOS IP Routing: BGP Command Reference*』の **continue** コマンドを参照してください。
ステップ 9	**set community** *community-number* [**additive**] [*well-known-community*] | **none**} 例： `Device(config-route-map)# set community 10:1`	**set** コマンドを設定して、**match** コマンドで適用された条件が満たされた場合のルーティング アクションを指定します。 • 複数の **set** コマンドを設定できます。 • この例では、指定したコミュニティをセットする句が作成されます。
ステップ 10	**continue** [*sequence-number*] 例： `Device(config-route-map)# continue`	一致が出現した後も match 文の評価と実行を継続するよう、ルート マップを設定します。 • シーケンス番号が指定された場合、continue 句は指定されたシーケンス番号のルート マップへ移動します。

	コマンドまたはアクション	目的
		• シーケンス番号が指定されない場合、continue 句はその次のシーケンス番号のルート マップへ移動します。この動作は、「黙示的継続」と呼ばれます。 （注） アウトバウンド ルート マップの continue 句は、Cisco IOS XE Release 2.1 以降のリリースだけでサポートされています。
ステップ 11	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 12	**show route-map** [*map-name*] 例： `Device# show route-map`	（任意）ローカルで設定されたルート マップを表示します。出力をフィルタリングするためのルート マップ名は、このコマンドの構文内で指定できます。

例

次に、**show route-map** コマンドを使用して continue 句の設定を確認する方法の出力例を示します。設定されたルート マップが、match、set、および continue 句を含め、出力に表示されます。

```
Device# show route-map

route-map MARKETING, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 40
  Match clauses:
    community (community-list filter): 10:1
```

```
  Set clauses:
    local-preference 104
  Policy routing matches: 0 packets, 0 bytes
route-map MKTG-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

BGP ルート マップ継続の設定例

例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理

次に、ルート マップ シーケンスでの continue 句設定の例を示します。

（注） アウトバウンド ルート マップの continue 句は、Cisco IOS Release 12.0(31)S、12.2(33)SB、12.2(33)SRB、12.2(33)SXI、12.4(4)T、およびそれ以降のリリースだけでサポートされています。

ルート マップ エントリ 10 にある 1 番目の continue 句は、一致が出現した場合にルート マップがエントリ 30 に移動することを示します。一致が出現しなければ、ルート マップは「失敗」してエントリ 20 へ移動します。ルート マップ エントリ 20 で一致が出現すると、set アクションが実行され、ルート マップはそれ以上どのルート マップ エントリも評価しません。最初に一致した **match ip address** 句だけをサポートします。

ルート マップ エントリ 20 で一致が出現しない場合、ルート マップはマッチングに失敗してルート マップ エントリ 30 へ移動します。このシーケンスには match 句が含まれていないため、set 句は自動的に実行され、**continue** 句にはシーケンス番号が指定されていないため、その次のルート マップ エントリへ移動することになります。

一致が出現しない場合、ルート マップはマッチングに失敗してエントリ 30 へ移動し、set 句を実行します。**continue** 句にはシーケンス番号が指定されていないため、ルート マップ エントリ 40 が評価されることになります。

後続の **continue** 句エントリで、同じ **set** コマンドが繰り返される場合、2 種類の動作が考えられます。値の加算や累積を設定する **set** コマンド（**set community additive**、**set extended community additive**、**set as-path prepend** など）では、後続のエントリによって後続の値が加算されます。次に、この動作の例を示します。match 句の各セットの後に、as-path に自律システム番号を追加するため **set as-path prepend** コマンドが設定されています。一致が出現すると、ルート マップは match 句の評価を停止し、設定された順序で set 句の実行を開始します。一致が何度出現するかに応じて、as-path には 1 つ、2 つ、または 3 つの自律システム番号がプリペンドされます。

```
route-map ROUTE-MAP-NAME permit 10
```

```
 match ip address 1
 match metric 10
 set as-path prepend 10
 continue 30
 !
route-map ROUTE-MAP-NAME permit 20
 match ip address 2
 match metric 20
 set as-path prepend 10 10
 !
route-map ROUTE-MAP-NAME permit 30
 set as-path prepend 10 10 10
 continue
 !
route-map ROUTE-MAP-NAME permit 40
 match community 10:1
 set local-preference 104
```

この例では、同じ **set** コマンドが後続の **continue** 句エントリで繰り返されますが、動作は 1 番目の例と異なります。絶対値を設定する **set** コマンドの場合、最後のインスタンスの値がそれ以前の値を上書きします。次に、この動作の例を示します。シーケンス 20 の set 句の値が、シーケンス 10 の set 句の値を上書きします。ネットワーク 172.16/16 からのプレフィックスのネクスト ホップは 10.2.2.2 に設定され、10.1.1.1 にはなりません。

```
ip prefix-list 1 permit 172.16.0.0/16
ip prefix-list 2 permit 192.168.1.0/24
route-map RED permit 10
 match ip address prefix-list 1
 set ip next hop 10.1.1.1
 continue 20
 exit
route-map RED permit 20
 match ip address prefix-list 2
 set ip next hop 10.2.2.2
 end
```

（注） ルートマップはリニア動作であり、入れ子動作ではありません。あるルートがいったん continue コマンド句を伴ったルート マップ許可エントリで一致すると、ルート マップ末尾の黙示的拒否により処理されません。次に、この場合の例を示します。

次の例では、ルートの as-path が 10、20、または 30 に一致する場合、ルートは許可され、continue 句は明示的 deny 句をジャンプして IP アドレス プレフィックス リストのマッチング処理へ移動します。一致が出現すると、ルート メトリックが 100 に設定されます。as-path が 10、20、または 30 に一致せず、かつコミュニティ番号が 30 に一致するルートだけが拒否されます。他のルータを拒否するには、明示的 deny 文を設定する必要があります。

```
route-map test permit 10
 match as-path 10 20 30
 continue 30
 exit
route-map test deny 20
 match community 30
 exit
route-map test permit 30
 match ip address prefix-list 1
```

```
set metric 100
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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

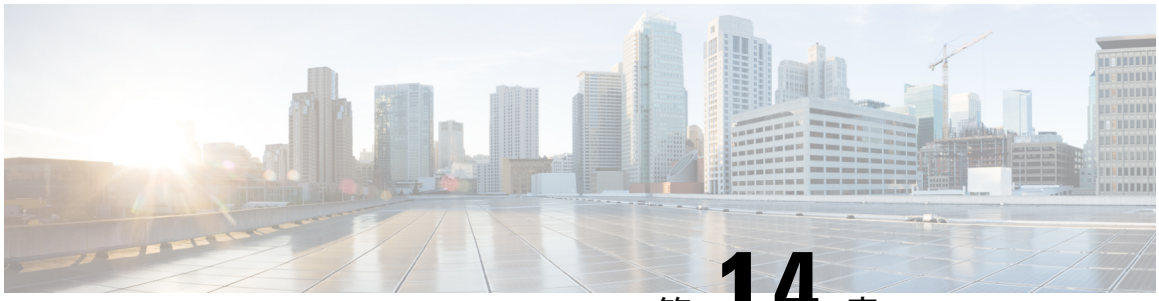
BGP ルート マップ継続の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *29 : BGP* ルート マップ継続の機能情報

機能名	リリース	機能情報
BGP ルート マップ継続		BGP ルート マップ継続機能により、continue 句が BGP ルート マップ コンフィギュレーションに導入されます。continue 句によって、ポリシー設定とルート フィルタリングのプログラム性は高まり、正常な match および set 句によってエントリが実行された後に追加のエントリを実行する機能が導入されます。continue 句によって、ネットワーク オペレータはポリシー定義をさらにモジュール化して設定できるようになり、特定のポリシー設定を同じルート マップ内で繰り返す必要がなくなりました。



第 14 章

アウトバウンドポリシーに対するBGPルート マップ継続のサポート

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポート機能により、continue 句のアウトバウンド ルート マップへの適用がサポートされます。

- 機能情報の確認 （401 ページ）
- アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートに関する情報 （402 ページ）
- BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理の方法 （403 ページ）
- アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートの設定例 （407 ページ）
- その他の参考資料 （409 ページ）
- アウトバウンドポリシーに対するBGPルートマップ継続のサポートの機能情報 （410ページ）

機能情報の確認

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

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

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートに関する情報

continue 句を使用した BGP ルート マップ

ルート マップのシスコでの実装に続いて、continue 句が BGP ルート マップ コンフィギュレーションに導入されました。continue 句により、プログラム可能なポリシー設定およびルート フィルタリングが実現されます。continue 句を使用すると、正常な match および set 句によってエントリが実行された後に追加のエントリを実行できます。continue 句によって、ポリシー定義をさらにモジュール化して設定できるようになり、特定のポリシー設定を同じルートマップ内で繰り返す必要がなくなります。continue 句の導入以前は、ルートマップの設定はリニア的であり、ルート マップのフローを制御することがまったくできませんでした。

continue 句を使用しないルート マップの動作

ルート マップは一致が出現するまで match 句を評価します。一致が出現すると、ルート マップは match 句の評価を停止し、設定された順序で set 句の実行を開始します。一致が出現しない場合、ルート マップはマッチングに「失敗」し、ルート マップの次のシーケンス番号を評価します。これをすべての設定されたルート マップ エントリが評価されるか、一致が出現するまで続けます。各ルートマップは、エントリを識別するシーケンス番号でタグ付けされています。ルートマップエントリは、シーケンス番号が最小のものから評価が始まり、最大のシーケンス番号を持つもので終わります。ルートマップに set 句だけが含まれる場合、set 句は自動的に実行され、ルート マップは他のルート マップ エントリを評価しません。

continue 句を使用したルート マップの動作

continue 句を設定すると、ルート マップは一致が出現した後も、指定されたルート マップ エントリで match 句の評価と実行を続けます。continue 句は、シーケンス番号を指定することで特定のルート マップ エントリに移動する（ジャンプする）よう設定できます。シーケンス番号が指定されていない場合、continue 句は次のシーケンス番号へ移動します。この動作は、「黙示的継続」と呼ばれます。match 句がある場合、continue 句は一致が出現した場合にだけ実行されます。一致が出現しなかった場合、continue 句は無視されます。

continue 句を使用した match 動作

match 句がルート マップ エントリに存在しないのに continue 句が存在する場合、continue 句は自動的に実行され、指定されたルート マップ エントリへ移動します。ルート マップ エントリに match 句が存在する場合、continue 句は一致が出現した場合にだけ実行されます。一致が出現し、かつ continue 句が存在する場合、ルート マップは set 句を実行し、それから指定されたルート マップ エントリへ移動します。その次のルート マップ エントリに continue が含まれている場合、ルート マップは一致が出現すればその continue 句を実行します。continue 句がその次のルート マップ エントリに存在しない場合、ルート マップは通常どおり評価されます。

continue 句がその次のルートマップエントリに存在するが一致が出現しない場合、ルートマップは継続せずに「失敗」し、その次のシーケンス番号が存在すればそこへ移動します。

（注） ルートマップ内の match community 句のコミュニティ リスト数が 1 行で 256 文字を超える場合は、新しい行で複数の match community 文の不揮発性生成（NVGEN）を行う必要があります。

continue 句を使用した Set 動作

set 句は、match 句の評価中は残しておかれ、ルートマップ評価が完了した後に実行されます。set 句は、設定された順番に評価され、処理されます。ルート マップに match 句が存在しない場合を除き、set 句は一致が出現した後にだけ実行されます。continue 文は、設定された set アクションが実行された後にだけ、指定のルート マップ エントリへと進みます。set アクションが最初のルートマップで発生し、それから後続のルートマップエントリにおいて再び同じ set アクションが異なる値で発生した場合、同じ **set** コマンドで設定された set アクションは、**set** コマンドが複数の値を許可する場合を除き、最後の set アクションによってそれ以前のものが上書きされます。たとえば、**set as-path prepend** コマンドは複数の自律システム番号の設定を許可しています。

（注） ルート マップ エントリに match 句が含まれない場合、continue 句は一致の出現なしで実行できます。

（注） ルートマップはリニア動作であり、入れ子動作ではありません。あるルートがいったんcontinue コマンド句を伴ったルート マップ許可エントリで一致すると、ルート マップ末尾の黙示的拒否により処理されません。例については、「例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理」の項を参照してください。

BGPルートマップでのcontinue句の使用によるトラフィックのフィルタ処理の方法

BGP ルート マップでの continue 句の使用によるトラフィック フィルタリング

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
7. **exit**
8. **exit**
9. **route-map** *map-name* {**permit** | **deny**} [*sequence-number*]
10. **match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*]
11. **set community** { { [*community-number*] [*well-known-community*] [**additive**]} | **none**}
12. **continue** [*sequence-number*]
13. **end**
14. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャスト アドレス ファミ

	コマンドまたはアクション	目的
		リのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} 例： `Device(config-router-af)# neighbor 10.0.0.1 route-map ROUTE-MAP-NAME in`	インバウンド ルート マップを指定されたネイバーから受信したルートに適用します。もしくは、アウトバウンド ルート マップを指定されたネイバーへアドバタイズされたルートへ適用します。
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 8	**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 9	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME permit 10`	ルート マップ コンフィギュレーション モードを開始し、ルート マップを作成または設定します。
ステップ 10	**match ip address** {*access-list-number* | *access-list-name*} [*... access-list-number* | *... access-list-name*] 例： `Device(config-route-map)# match ip address 1`	ポリシー ルーティングとルート フィルタリングが発生する条件を指定する **match** コマンドを設定します。 • 複数の **match** コマンドを設定できます。**match** コマンドが設定された場合、continue 文は一致が出現した場合にのみ実行されます。**match** コマンドが設定されない場合、set および continue 句は実行されます。

	コマンドまたはアクション	目的
		（注） この作業で使用する **match** コマンドおよび **set** コマンドは、**continue** コマンドの動作を記述するための例です。具体的な **match** コマンドおよび **set** コマンドのリストについては、『*Cisco IOS IP Routing: BGP Command Reference*』の **continue** コマンドを参照してください。
ステップ 11	**set community** { { [*community-number*] [*well-known-community*] [**additive**]} | **none**} 例： `Device(config-route-map)# set community 10:1`	**set** コマンドを設定して、**match** コマンドで適用された条件が満たされた場合のルーティング アクションを指定します。 • 複数の **set** コマンドを設定できます。 • この例では、指定した aa:nn 形式のコミュニティ番号をセットする句が作成されます。
ステップ 12	**continue** [*sequence-number*] 例： `Device(config-route-map)# continue`	一致が出現した後も match 文の評価と実行を継続するよう、ルート マップを設定します。 • シーケンス番号が指定された場合、continue 句は指定されたシーケンス番号のルート マップへ移動します。 • シーケンス番号が指定されない場合、continue 句はその次のシーケンス番号のルート マップへ移動します。この動作は、「黙示的継続」と呼ばれます。
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show route-map** [*map-name*] 例： `Device# show route-map`	（任意）ローカルで設定されたルート マップを表示します。出力をフィルタリングするためのルート マップ名は、このコマンドの構文内で指定できます。

例

次に、**show route-map** コマンドを使用して continue 句の設定を確認する方法の出力例を示します。設定されたルート マップが、match、set、および continue 句を含め、出力に表示されます。

```
Device# show route-map

route-map MARKETING, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
  Set clauses:
    as-path prepend 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
    metric 20
  Set clauses:
    as-path prepend 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 30
  Match clauses:
  Continue: to next entry 40
  Set clauses:
    as-path prepend 10 10 10
  Policy routing matches: 0 packets, 0 bytes
route-map MARKETING, permit, sequence 40
  Match clauses:
    community (community-list filter): 10:1
  Set clauses:
    local-preference 104
  Policy routing matches: 0 packets, 0 bytes
route-map MKTG-POLICY-MAP, permit, sequence 10
  Match clauses:
  Set clauses:
    community 655370
  Policy routing matches: 0 packets, 0 bytes
```

アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートの設定例

例：BGP ルート マップでの continue 句の使用によるトラフィックのフィルタ処理

次に、ルート マップ シーケンスでの continue 句設定の例を示します。

ルート マップ エントリ 10 にある 1 番目の continue 句は、一致が出現した場合にルート マップがエントリ 30 に移動することを示します。一致が出現しなければ、ルート マップは「失敗」してエントリ 20 へ移動します。ルート マップ エントリ 20 で一致が出現すると、set アクションが実行され、ルート マップはそれ以上どのルート マップ エントリも評価しません。最初に一致した IP アドレスだけをサポートします。

ルート マップ エントリ 20 で一致が出現しない場合、ルート マップはマッチングに失敗してルート マップ エントリ 30 へ移動します。このシーケンスには match 句が含まれていないた

め、set 句は自動的に実行され、continue 句にはシーケンス番号が指定されていないため、その次のルート マップ エントリへ移動することになります。

一致が出現しない場合、ルート マップはマッチングに失敗してエントリ 30 へ移動し、set 句を実行します。continue 句にはシーケンス番号が指定されていないため、ルート マップ エントリ 40 が評価されることになります。

後続の continue 句エントリで、同じ **set** コマンドが繰り返される場合、2 種類の動作が考えられます。値の加算や累積を設定する **set** コマンド（**set community additive**、**set extended community additive**、**set as-path prepend** など）では、後続のエントリによって後続の値が加算されます。次に、この動作の例を示します。match 句の各セットの後に、as-path に自律システム番号を追加するため **set as-path prepend** コマンドが設定されています。一致が出現すると、ルート マップは match 句の評価を停止し、設定された順序で set 句の実行を開始します。一致数に応じて、as-path には 1 つ、2 つ、または 3 つの自律システム番号が前に付加されます。

```
route-map ROUTE-MAP-NAME permit 10
 match ip address 1
 match metric 10
 set as-path prepend 10
 continue 30
 !
route-map ROUTE-MAP-NAME permit 20
 match ip address 2
 match metric 20
 set as-path prepend 10 10
 !
route-map ROUTE-MAP-NAME permit 30
 set as-path prepend 10 10 10
 continue
 !
route-map ROUTE-MAP-NAME permit 40
 match community 10:1
 set local-preference 104
```

この例では、同じ **set** コマンドが後続の continue 句エントリで繰り返されますが、動作は 1 番目の例と異なります。絶対値を設定する **set** コマンドの場合、最後のインスタンスの値がそれ以前の値を上書きします。次に、この動作の例を示します。シーケンス 20 の set 句の値が、シーケンス 10 の set 句の値を上書きします。ネットワーク 172.16/16 からのプレフィックスのネクスト ホップは 10.2.2.2 に設定され、10.1.1.1 にはなりません。

```
ip prefix-list 1 permit 172.16.0.0/16
ip prefix-list 2 permit 192.168.1.0/24
route-map RED permit 10
 match ip address prefix-list 1
 set ip next hop 10.1.1.1
 continue 20
 exit
route-map RED permit 20
 match ip address prefix-list 2
 set ip next hop 10.2.2.2
 end
```

（注） ルートマップはリニア動作であり、入れ子動作ではありません。あるルートがいったんcontinueコマンド句を伴ったルート マップ許可エントリで一致すると、ルート マップ末尾にある暗黙の deny により処理されません。次に、この場合の例を示します。

次の例では、ルートの AS-path が 10、20、または 30 に一致する場合、ルートは許可され、continue 句は明示的 deny 句をジャンプして **match ip address prefix-list** コマンドの処理に移動します。一致が出現すると、ルート メトリックが 100 に設定されます。AS-path が 10、20、または 30 に一致せず、かつコミュニティ番号が 30 に一致するルートだけが拒否されます。他のルータを拒否するには、明示的 deny 文を設定する必要があります。

```
route-map test permit 10
 match as-path 10 20 30
 continue 30
 exit
route-map test deny 20
 match community 30
 exit
route-map test permit 30
 match ip address prefix-list 1
 set metric 100
 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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

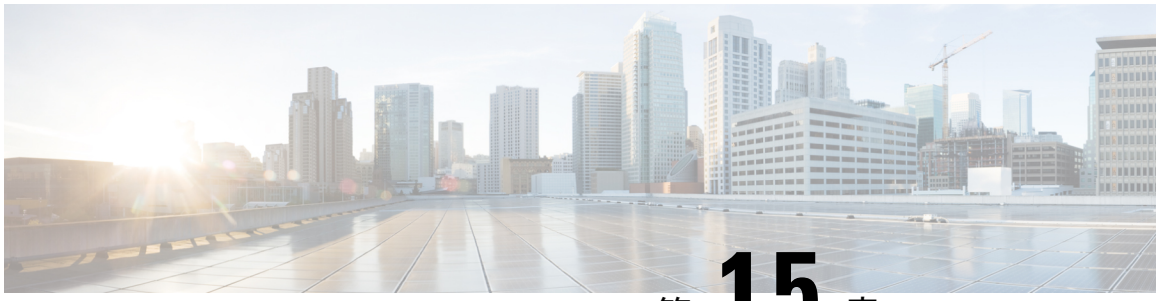
アウトバウンド ポリシーに対する BGP ルート マップ継続のサポートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *30 :* アウトバウンド ポリシーに対する *BGP* ルート マップ継続のサポートの機能情報

機能名	リリース	機能情報
アウトバウンド ポリシーに対する BGP ルート マップ継続のサポート		アウトバウンド ポリシーに対する BGP ルート マップ継続のサポート機能により、continue 句のアウトバウンド ルート マップへの適用がサポートされます。



第 15 章

BGP の AS パスからプライベート AS 番号の削除

プライベート自律システム番号（ASN）は、グローバルに一意な AS 番号を保護するために、ISP およびお客様のネットワークで使用されます。プライベート AS 番号は一意でないため、グローバル インターネットへのアクセスには使用できません。AS 番号はルーティング アップデートの eBGP AS パスに表示されます。プライベート ASN を使用している場合にグローバル インターネットにアクセスするには、AS パスからプライベート ASN を削除する必要があります。

- 機能情報の確認 （411 ページ）
- AS パスからプライベート ASN の削除および交換の制約事項 （412 ページ）
- AS パスからプライベート ASN の削除および交換に関する情報 （412 ページ）
- AS パスからプライベート ASN を削除および交換する方法 （414 ページ）
- AS パスからプライベート ASN を削除および交換する設定例 （417 ページ）
- その他の参考資料 （421 ページ）
- AS パスからプライベート ASN の削除および交換の機能情報 （422 ページ）

機能情報の確認

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

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

AS パスからプライベート ASN の削除および交換の制約事項

- この機能は、eBGP ネイバーのみに適用されます。
- この機能は、パブリック AS のみのルータに適用されます。この制約事項を回避するには、ネイバー単位で **neighbor local-as** コマンドを適用し、ローカル AS 番号をパブリック AS 番号として指定することです。

AS パスからプライベート ASN の削除および交換に関する情報

パブリックおよびプライベート AS 番号

パブリックな AS 番号は、InterNIC によって割り当てられ、グローバルに一意です。範囲は 1 ～ 64511 です。プライベート AS 番号は、グローバルに一意な AS 番号（有効な範囲は 64512 ～ 65535）を保護するために使用されます。プライベート AS 番号はグローバル BGP ルーティング テーブルにリークできません。プライベート AS 番号は一意ではなく、BGP のベスト パスの計算には一意の AS 番号が必要であるからです。そのため、ルートが BGP ピアに伝播される前に、AS パスからプライベート AS 番号を削除する必要がある可能性があります。

AS パスからプライベート ASN の削除および交換の利点

外部 BGP では、グローバルなインターネットへのルーティングで、グローバルに一意な AS 番号を使用する必要があります。プライベート AS 番号（これは一意でない）を使用すると、グローバルなインターネットにアクセスできません。この機能を使用すると、プライベート AS に属するルータがグローバルなインターネットにアクセスできます。ネットワーク管理者は、発信アップデート メッセージに含まれる AS パスからプライベート AS を削除するようにルータを設定します。場合によっては、これらの番号をローカル ルータの ASN で置き換えて、AS パス長が変化しないようにします。

AS パスからプライベート ASN の削除に関する過去の制約事項

AS パスからプライベート AS 番号を削除する機能は、以前から利用できました。Cisco IOS XE Release 3.1S 以前は、この機能には次の制約事項がありました。

- AS パスがプライベートとパブリックの両方の AS 番号に含まれる場合、**neighbor remove-private-as** コマンドでプライベート AS 番号が削除されませんでした。

- AS パスにコンフェデレーション セグメントが含まれている場合、自律パスのコンフェデレーション部分の後にプライベート AS 番号が続く場合に限って、**neighbor remove-private-as** コマンドでプライベート AS 番号が削除されていました。
- AS パスに eBGP ネイバーの AS 番号が含まれている場合、プライベート AS 番号は削除されませんでした。

AS パスからプライベート ASN の削除の拡張機能

AS パスからプライベート ASN の削除および交換機能は、次のように拡張されました。

- **neighbor remove-private-as** コマンドでは、AS パスにパブリックとプライベートの両方の ASN が含まれる場合でも、AS パスからプライベート AS 番号が削除されます。
- **neighbor remove-private-as** コマンドでは、AS パスにプライベート AS 番号のみが含まれる場合でも、AS パスからプライベート AS 番号が削除されます。このコマンドは eBGP ピアのみに適用され、その場合、eBGP ピアではローカル ルータの AS 番号が AS パスに付加されるため、長さ 0 の AS パスにはなることはありません。
- **neighbor remove-private-as** コマンドでは、AS パスでコンフェデレーション セグメントの前にプライベート ASN が出現する場合でも、プライベート AS 番号が削除されます。
- **replace-as** キーワードを使用して、パスから削除されるプライベート AS 番号をローカル AS 番号と交換できるため、AS パスの長さは同じままに保つことができます。
- この機能は、アドレス ファミリごとにネイバーに適用できます（アドレス ファミリ コンフィギュレーション モード）。そのため、この機能をあるアドレス ファミリのネイバーには適用して、別のアドレス ファミリでは適用しないようにすることで、機能が設定されているアドレス ファミリのみのアウトバウンド側のアップデート メッセージに影響を与えることができます。
- この機能は、ピア グループ テンプレート モードで適用できます。
- この機能を設定すると、**show ip bgp update-group** および **show ip bgp neighbor** コマンドの出力で、プライベート AS 番号が削除または交換されたことが示されます。

AS パスからプライベート ASN を削除および交換する方法

AS パスのプライベート ASN の削除および置換（Cisco IOS XE Release 3.1S 以降）

eBGP ネイバーのアウトバウンド側で AS パスからプライベート AS 番号を削除するには、次の作業を実行します。また、プライベート AS 番号をローカル ルータの AS 番号に置き換える場合は、手順 17 で **all replace-as** キーワードを指定します。

この作業例は、下の図のシナリオにおけるルータ 2 の設定を反映しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **exit**
12. **router bgp** *autonomous-system-number*
13. **network** *network-number*
14. **network** *network-number*
15. **neighbor** {*ip-address* | *ipv6-address*[**%**]| *peer-group-name*} **remote-as** *autonomous-system-number*
16. **neighbor** {*ip-address* | *ipv6-address*[**%**]| *peer-group-name*} **remote-as** *autonomous-system-number*
17. **neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** [**all** [**replace-as**]]
18. **end**
19. **show ip bgp update-group**
20. **show ip bgp neighbors**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイスを設定します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.30.1.1 255.255.0.0`	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	**exit** 例： `Router(config-if)# exit`	次に高次のコンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* 例： `Router(config)# interface serial 0/0`	インターフェイスを設定します。
ステップ 7	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.0.2 255.255.255.0`	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。
ステップ 8	**exit** 例： `Router(config-if)# exit`	次に高次の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** *type number* 例： `Router(config)# interface serial 1/0`	インターフェイスを設定します。
ステップ 10	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 192.168.0.1 255.255.255.0`	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。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `Router(config-if)# exit`	次に高次のコンフィギュレーション モードに戻ります。
ステップ 12	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP インスタンスを指定します。
ステップ 13	**network** *network-number* 例： `Router(config-router)# network 172.30.0.0`	ネットワークが BGP によってアドバタイズされるように指定します。
ステップ 14	**network** *network-number* 例： `Router(config-router)# network 192.168.0.0`	ネットワークが BGP によってアドバタイズされるように指定します。
ステップ 15	**neighbor** {*ip-address* | *ipv6-address*[**%**]| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 172.16.0.1 remote-as 65000`	エントリをルーティング テーブルに追加します。 • この例では、ルータ 3 をプライベート AS 65000 の eBGP ネイバーとして設定します。
ステップ 16	**neighbor** {*ip-address* | *ipv6-address*[**%**]| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.0.2 remote-as 1`	エントリをルーティング テーブルに追加します。 • この例では、ルータ 1 をパブリック AS 1 の eBGP ネイバーとして設定します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** [**all** [**replace-as**]] 例： `Router(config-router)# neighbor 192.168.0.2 remove-private-as all replace-as`	発信更新の AS パスからプライベート AS 番号を削除します。 • この例では、発信 eBGP 更新の AS パスからプライベート AS 番号を削除し、ローカル ルータのパブリック AS 番号である 5 で置き換えます。
ステップ 18	**end** 例： `Router(config-router)# end`	現在の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 19	**show ip bgp update-group** 例： `Router# show ip bgp update-group`	（任意）BGP 更新グループの情報を表示します。
ステップ 20	**show ip bgp neighbors** 例： `Router# show ip bgp neighbors`	（任意）BGP ネイバーに関する情報を表示します。

AS パスからプライベート ASN を削除および交換する設定例

プライベート ASN の削除の例（Cisco IOS XE Release 3.1S）

次の例では、ルータ A が **neighbor remove-private-as** コマンドで設定されています。このコマンドは、172.30.0.7 のネイバーに送信される更新でプライベート AS 番号が削除されます。その後の **show** コマンドで、ホスト 1.1.1.1 へのルートに関する情報を要求します。出力には、AS パス 1001 65200 65201 65201 1002 1003 1003 に プライベート AS 番号 65200、65201、65201 が含まれています。

これらのプライベート AS 番号が AS パスから削除されたことを確認するには、ルータ B の **show** コマンドでもホスト 1.1.1.1 へのルートに関する情報を要求します。短い AS パス 100 1001 1002 1003 1003 が出力されますが、プライベート AS 番号 65200、65201、および 65201 が除外されています。パスの先頭に付加された 100 は、ルータ B 自身の AS 番号です。

ルータ A

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 19.0.101.1 remote-as 1001
 neighbor 172.30.0.7 remote-as 200
 neighbor 172.30.0.7 remove-private-as all
 no auto-summary

RouterA# show ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1           2
  1001 65200 65201 65201 1002 1003 1003
    19.0.101.1 from 19.0.101.1 (19.0.101.1)
      Origin IGP, localpref 100, valid, external, best RouterA#
```

ルータ B（すべてのプライベート ASN を削除済み）

```
RouterB# show ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 3
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  100 1001 1002 1003 1003
    172.30.0.6 from 172.30.0.6 (19.1.0.1)
      Origin IGP, localpref 100, valid, external, best RouterB#
```

プライベート ASN の削除および置換の例（Cisco IOS XE Release 3.1S）

次の例では、ルータ A がピア 172.30.0.7 にプレフィックスを送信すると、AS パスのすべてのプライベート ASN がルータ自身の ASN である 100 で置き換えられます。

ルータ A

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 172.16.101.1 remote-as 1001
 neighbor 172.16.101.1 update-source Loopback0
 neighbor 172.30.0.7 remote-as 200
 neighbor 172.30.0.7 remove-private-as all replace-as
 no auto-summary
```

ルータ A は、ピア 172.16.101.1 から 1.1.1.1 を受信しますが、次の出力に示すように、その AS パス リストにはプライベート ASN（65200、65201、および 65201）があります。

```
RouterA# show ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 2
Paths: (1 available, best #1, table default)
   Advertised to update-groups:
      1           2
   1001 65200 65201 65201 1002 1003 1003
     172.16.101.1 from 172.16.101.1 (172.16.101.1)
       Origin IGP, localpref 100, valid, external, best RouterA#
```

ルータ A は **neighbor 172.30.0.7 remove-private-as all replace-as** で設定されるため、ルータ A はすべてのプライベート ASN が 100 で置き換えられたプレフィックス 1.1.1.1 を送信します。

ルータ B

```
RouterB# show ip bgp 1.1.1.1
BGP routing table entry for 1.1.1.1/32, version 3
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   100 1001 100 100 100 1002 1003 1003
     172.30.0.6 from 172.30.0.6 (192.168.1.2)
       Origin IGP, localpref 100, valid, external, best RouterB#
```

ルータ B

```
router bgp 200
 bgp log-neighbor-changes
```

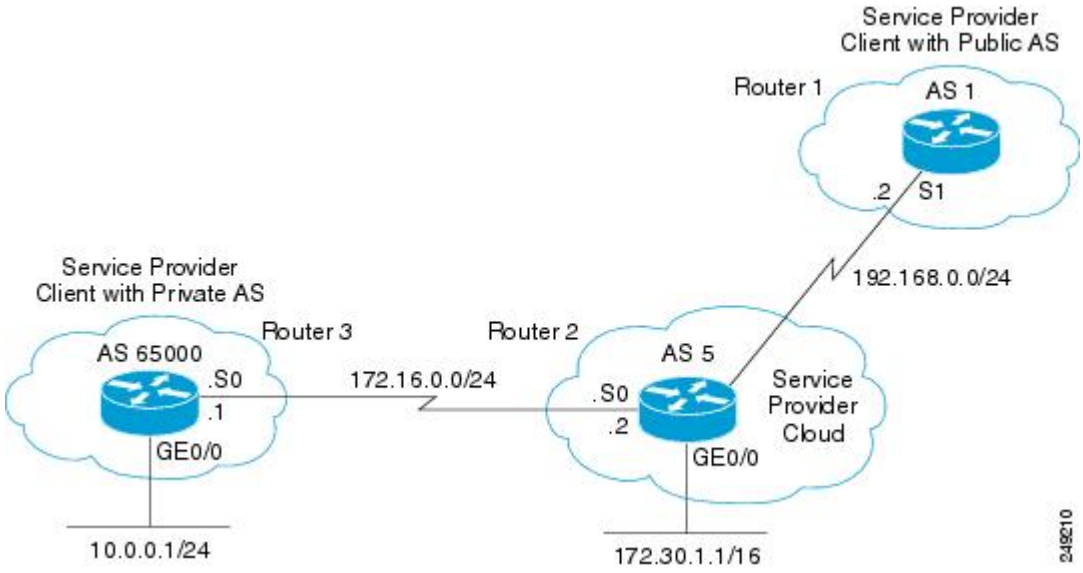
```
neighbor 172.30.0.6 remote-as 100
no auto-summary
```

プライベート ASN の置換の例（Cisco IOS XE Release 2S）

この例では、ルータ 3 でプライベート ASN 65000 を使用します。ルータ 1 およびルータ 2 は、それぞれパブリック ASN AS 1 および AS 5 を使用します。

下の図に、サービス プロバイダーに属しているルータ 2、およびそのクライアントであるルータ 1 およびルータ 3 を示します。

図 *35* : プライベート *AS* 番号の削除



この例では、サービス プロバイダーに属しているルータ 2 で、次のようにプライベート AS 番号を削除します。

1. ルータ 3 は、AS パス属性 65000 のネットワーク 10.0.0.0/24 をルータ 2 にアドバタイズします。
2. ルータ 2 は、ルータ 3 から更新を受け取り、ルーティング テーブルにネクスト ホップ 172.16.0.1（ルータ 3 のシリアル インターフェイス S0）でネットワーク 10.0.0.0/24 に関するエントリを作成します。
3. ルータ 2（サービス プロバイダー デバイス）は、**neighbor 192.168.0.2 remove-private-as** コマンドで設定されると、プライベート AS 番号を削除して自身の AS 番号を 10.0.0.0/24 ネットワークの AS パス属性として新しい更新パケットを構成し、パケットをルータ 1 に送信します。
4. ルータ 1 は、ネットワーク 10.0.0.0/24 の eBGP 更新を受信し、ルーティング テーブルにネクスト ホップ 192.168.0.1（ルータ 2 のシリアル インターフェイス S1）でエントリを作成します。ルータ 1 で認識されるこのネットワークの AS パス属性は、AS 5（ルータ 2）で

す。つまりプライベート AS 番号がインターネットの BGP テーブルに入ることはありません。

ルータ 3、ルータ 2、およびルータ 1 の設定は次のとおりです。

ルータ 3

```
interface gigabitethernet 0/0
 ip address 10.0.0.1 255.255.255.0
!
interface Serial 0
 ip address 172.16.0.1 255.255.255.0
!
router bgp 65000
 network 10.0.0.0 mask 255.255.255.0
 neighbor 172.16.0.2 remote-as 5
!---Configures Router 2 as an eBGP neighbor in public AS 5.
!
end
```

ルータ 2

```
interface gigabitethernet 0/0
 ip address 172.30.1.1 255.255.0.0
!
interface Serial 0
 ip address 172.16.0.2 255.255.255.0
!
interface Serial 1
 ip address 192.168.0.1 255.255.255.0
!
router bgp 5
 network 172.30.0.0
 network 192.168.0.0
 neighbor 172.16.0.1 remote-as 65000
!---Configures Router 3 as an eBGP neighbor in private AS 65000.
 neighbor 192.168.0.2 remote-as 1
!---Configures Router 1 as an eBGP neighbor in public AS 1.
 neighbor 192.168.0.2 remove-private-as
!---Removes the private AS numbers from outgoing eBGP updates.
!
end
```

ルータ 1

```
version 12.2
!
!
interface Serial 0
 ip address 192.168.0.2 255.255.255.0
!
router bgp 1
 neighbor 192.168.0.1 remote-as 5
!---Configures Router 2 as an eBGP neighbor in public AS 5.
!
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 Commands List, All Releases』
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』

標準

標準	タイトル
なし	--

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	リンク
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

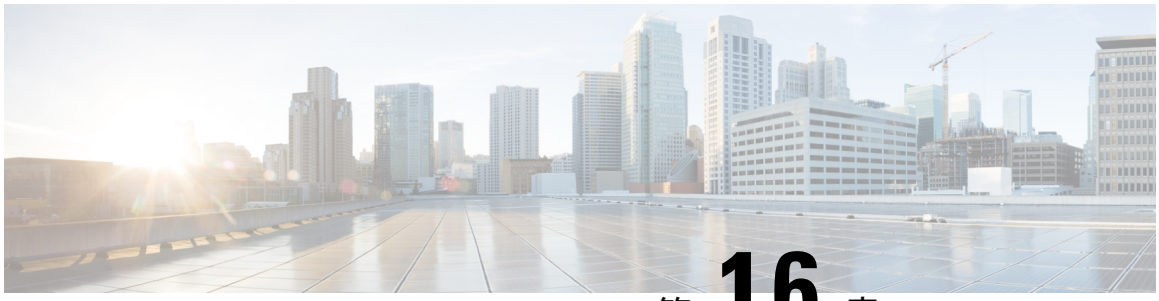
AS パスからプライベート ASN の削除および交換の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *31 : BGP* - プライベート *AS* の削除および置換の機能情報

機能名	リリース	機能情報
BGP - プライベート AS フィルタの削除および置換	Cisco IOS XE Release 3.1S	プライベート自律システム（AS）番号は、グローバルに一意な AS 番号を保護するために、ISP およびお客様のネットワークで使用されます。プライベート AS 番号は一意でないため、この番号を使用してグローバルなインターネットにアクセスすることはできません。AS 番号は、ルーティング テーブルで eBGP AS パスに出現します。プライベート AS 番号を使用している場合にグローバルなインターネットにアクセスするには、AS パスからプライベート AS 番号を削除することが必要です。 次のコマンドが変更されました。 • **neighbor remove-private-as**



第 16 章

BGP ネイバーセッションオプションの設定

このモジュールでは、ボーダー ゲートウェイ プロトコル（BGP）ネイバー ピア セッションに関するさまざまなオプションを設定する設定作業について説明します。BGP は、組織間のループのないルーティングを提供するよう設計されたドメイン間ルーティング プロトコルです。このモジュールでは、BGP ネイバー セッション コマンドを使用して以下を設定する作業について説明します。

- 自律システムの移行に役立つオプション
- TTL セキュリティ チェック（CPU 使用率に基づく攻撃から外部 BGP（eBGP）ピアリング セッションを保護する簡単なセキュリティ メカニズム）

- 機能情報の確認 （425 ページ）
- BGP ネイバー セッション オプションの設定に関する情報 （426 ページ）
- BGP ネイバー セッションのオプションの設定方法 （430 ページ）
- BGP ネイバー セッション オプションの設定例 （451 ページ）
- 次の作業 （453 ページ）
- その他の参考資料 （454 ページ）
- BGP ネイバー セッションのオプション設定の機能情報 （455 ページ）

機能情報の確認

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

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

BGPネイバーセッションオプションの設定に関する情報

BGP ネイバー セッション

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。BGP 対応ルータは、別の BGP 対応デバイスを自動的には検出しません。ネットワーク管理者は、通常、BGP 対応ルータ間の関係を手動で設定します。

BGP ネイバー デバイスは、別の BGP 対応デバイスへのアクティブな伝送制御プロトコル（TCP）接続がある BGP 対応ルータです。BGP デバイス間の関係は、多くの場合、ネイバーではなくピアと呼ばれます。これは、ネイバーは、複数の BGP デバイスがその間で他のルータを経由せず直接接続する概念を意味する場合があるためです。BGP ネイバーまたはピア セッションの設定には BGP ネイバー セッションのコマンドが使用されるため、このモジュールでは「ピア」ではなく「ネイバー」という用語を使用します。

高速ピアリング セッションの非アクティブ化に対する BGP サポート

BGP ホールド タイマー

デフォルトでは、BGP ホールド タイマーは、シスコ ソフトウェアで 180 秒ごとに実行するように設定されます。このタイマー値は、デフォルトとして設定され、BGP ルーティング プロセスを別のルーティング プロトコルを持つピアリング セッションが原因になっている可能性がある不安定な状態から保護します。BGP デバイスは、通常、大きなルーティング テーブルを持っているため、頻繁にセッションをリセットすることは好ましくありません。

BGP の高速ピアリング セッションの非アクティブ化

BGP の高速ピアリング セッションを無効にすると、BGP コンバージェンスおよび BGP ネイバーの隣接変更に対する応答時間が向上します。この機能は、イベントによって引き起こされ、ネイバーごとに設定されます。この機能をイネーブルにすると、BGP は指定したネイバーでピアリング セッションをモニタします。隣接変更が検出され、終了したピアリング セッションがデフォルトのまたは設定した BGP スキャン間隔中に無効にされます。

BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング

Cisco IOS Release 12.4(4)T、12.2(31)SB、12.2(33)SRB、およびこれら以降のリリースでは、BGP の選択的アドレス トラッキング機能により、BGP の高速セッションの非アクティブ化とともにルート マップの使用が導入されました。**route-map** キーワードおよび *map-name* 引数は、**neighbor fall-over** BGP ネイバー セッション コマンドとともに使用され、BGP ピアへのルートが変更されたときに、この BGP ネイバーのあるピアリング セッションをリセットする必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、 deny 文

が返された場合、ピア セッションがリセットされます。このルート マップはセッションの確立には使用されません。

（注） **neighbor fall-over** コマンドは、Cisco IOS Release 15.0(1)SY ではサポートされていません。**bgp nexthop** コマンドの **route-map** と *map-name* というキーワードと引数のペアは、Cisco IOS Release 15.0(1)SY ではサポートされていません。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

BGP IPv6 ネイバーの BFD サポート

Cisco IOS Release 15.1(2)S 以降では、双方向フォワーディング検出（BFD）を IPv6 アドレスがある BGP ネイバーの高速転送パス障害を追跡するために使用できます。BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。BFD は転送パス障害後の BGP の再コンバージェンス時間を短縮します。

BGP ネイバー セッションの TTL セキュリティ チェック

TTL セキュリティ チェックに対する BGP サポート

TTL セキュリティ チェック機能は、BGP に実装されると簡単なセキュリティ メカニズムを導入し、eBGP ネイバー セッションを CPU 利用率に基づく攻撃から防御します。この種の攻撃は、偽造の送信元と宛先の IP アドレスを含む大量の IP パケットでネットワークをあふれさせてネットワークを無効にしようとする典型的なブルートフォースのサービス妨害（DoS）攻撃です。

TTL セキュリティ チェック機能は、受信 IP パケットの TTL フィールドの値を各 eBGP ネイバーセッションにローカルで設定されているホップ カウントと比較して、eBGP ネイバーセッションを防御します。着信 IP パケットの TTL フィールドの値が、ローカルで設定された値以上の場合、この IP パケットは受け入れられ、通常どおり処理されます。IP パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージ プロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。

IP パケット ヘッダーの TTL フィールドを偽造することは可能ですが、信頼できるピアが属するネットワークが損なわれていない限り、信頼できるピアの TTL カウントと一致するように TTL カウントを正確に偽造することは不可能です。

TTL セキュリティ チェック機能は、直接接続されているネイバー セッションとマルチホップ eBGP ネイバーセッションの両方をサポートします。BGP ネイバーセッションは、無効な TTL

値を含む着信パケットには影響されません。BGP ネイバー セッションは開いたままで、ルータがサイレントに無効なパケットを廃棄します。ただし、それでも BGP セッションは、セッション タイマーが期限切れになる前にキープアライブ パケットを受信しないと期限切れになることがあります。

BGP ネイバー セッションの TTL セキュリティ チェック

TTL セキュリティ チェックに対する BGP サポート機能は、**neighbor ttl-security** コマンドを使用してルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで設定されます。この機能が有効な場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能を有効にすると、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。*hop-count* 引数は、2 つのピアを区切るホップの最大数を設定するために使用されます。TTL 値は、設定されたホップ カウントからルータによって決定されます。この引数の値は、1 ～ 254 の数値です。

マルチホップ BGP ネイバー セッションに対する TTL セキュリティ チェックのサポート

TTL セキュリティ チェックに対する BGP サポート機能は、直接接続されているネイバー セッションとマルチホップ ネイバー セッションの両方をサポートします。この機能がマルチホップ ネイバー セッションに設定されている場合、**neighbor ebgp-multihop** ルータ コンフィギュレーション コマンドは設定できず、ネイバー セッションを確立する必要はありません。これらのコマンドは、二者択一で、マルチホップ ネイバー セッションを確立するには 1 つのコマンドだけが必要です。両方のコマンドを同じピアリング セッションに設定しようとすると、コンソールにエラー メッセージが表示されます。

この機能を既存のマルチホップ セッションに設定するには、まず既存のネイバー セッションを **no neighbor ebgp-multihop** コマンドで無効にする必要があります。マルチホップ ネイバー セッションは、この機能を **neighbor ttl-security** コマンドで有効にすると復元されます。

この機能は、参加している各ルータで設定する必要があります。この機能の効果を最大化するには、ローカル ネットワークと外部ネットワークの間のホップ カウントが一致するように *hop-count* 引数を厳密に設定する必要があります。ただし、この機能をマルチホップ ネイバー セッションに設定する場合は、パスの種類を考慮する必要もあります。

TTL セキュリティ チェックに対する BGP サポートの利点

TTL セキュリティ チェックに対する BGP サポート機能は、eBGP ネイバー セッションを CPU 利用率に基づく攻撃から防御する、効果的で容易に導入できるソリューションを提供します。この機能が有効な場合、ホストがローカル BGP ネットワークまたはリモート BGP ネットワークのメンバでない場合、あるいはホストがローカル BGP ネットワークとリモート BGP ネットワークの間のネットワーク セグメントに直接接続されていない場合、ホストは BGP セッションを攻撃できません。このソリューションは、BGP 自律システムへの DoS 攻撃の効果を大幅に軽減します。

セッションごとの TCP の PMTUD に対する BGP サポート

パス MTU 検出

IP プロトコル ファミリは、広範な伝送リンクを使用できるように設計されました。最大 IP パケット長は、65000 バイトです。ほとんどの伝送リンクは、最大伝送単位（MTU）と呼ばれる、より小さい最大パケット長の制限が適用されます。この制限は、伝送リンクの種類によって異なります。IP の設計は、発信リンクに対する必要に応じて中間ルータで IP パケットをフラグメント化することにより、リンク パケット長の制限を受け入れます。IP パケットの最後の宛先は、必要に応じて、フラグメント化されたパケットの再組み立てを行います。

すべての TCP セッションは、単一のパケットで転送可能なバイト数に関する制限によってバインドされます。この制限は、最大セグメントサイズ（MSS）と呼ばれます。TCP は、パケットを IP レイヤに渡す前に、送信キューでパケットをチャンクに分割します。小さい MSS は、宛先デバイスへのパスにある IP デバイスで断片化されない場合がありますが、小さいパケットは、パケットを転送するために必要な帯域幅の量を増加します。最大 TCP パケット長は、TCP セットアップ プロセス中に、送信元デバイスのアウトバウンドインターフェイスの MTU と宛先デバイスによって知らされる MSS の両方によって決まります。

パス MTU 検出（PMTUD）は、最適の TCP パケット長を検出するソリューションとして開発されました。PMTUD は、最適化（RFC 1191 で詳述）で、ここで送信元から宛先へのパスで断片化されない TCP 接続が最長パケットの送信を試行します。PMTUD は、この作業を IP パケットでフラグ Don't Fragment（DF）を使用して行います。このフラグは、パケットが長すぎるため、これをリンクを超えて送信できない中間ルータの動作を変えるためのものです。通常、このフラグはオフで、ルータはパケットをフラグメント化し、このフラグメントを送信する必要があります。ルータが、DF ビットが設定された状態で IP データグラムをパケットのサイズよりも小さい MTU を持つリンクに転送しようとすると、ルータは、パケットをドロップし、ICMP 宛先到着不能メッセージを「断片化が必要です。DF が設定されています」ということを示すコードとともにこの IP データグラムの送信元に返します。送信元のデバイスは、ICMP メッセージを受信すると、送信 MSS を低くし、TCP がセグメントを再送信するときに、より小さいセグメント サイズを使用します。

BGP ネイバー セッションの TCP の PMTUD

TCP の PMTUD は、すべての BGP ネイバー セッションに対してデフォルトで有効にされますが、1 つまたはすべての BGP ネイバー セッションに対して TCP の PMTUD を無効にする必要がある場合があります。PMTUD は、大きい伝送リンク（たとえば、Packet over Sonet リンク）では適切に動作しますが、不適切に設定された TCP 実装やファイアウォールでは、TCP 接続のパケット転送を遅くしたり停止したりする場合があります。この種の状況では、TCP の PMTUD を無効にする必要がある場合があります。

シスコ ソフトウェアでは、設定オプションが導入され TCP の PMTUD を単一の BGP ネイバー セッションまたはすべての BGP セッションに対して無効、または再度有効にできます。TCP の PMTUD をすべての BGP ネイバーに対してグローバルに無効にするには、**no bgp transport path-mtu-discovery** 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。単一のネイバーに対して TCP の PMTUD を無効にするには、**no neighbor transport path-mtu-discovery** コマンドをルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレー

ション モードで使用します。詳細については、「すべての BGP セッションに対する TCP の PMTUD のグローバルな無効化」の項または「単一の BGP ネイバーに対する TCP の PMTUD の無効化」の項を参照してください。

BGP ネイバー セッションのオプションの設定方法

高速セッションの非アクティブ化の設定

この項の作業は、BGP ネクストホップアドレストラッキングの設定方法を示しています。BGP ネクストホップアドレストラッキングによって、RIB でのネクストホップの変更に対する BGP の応答時間が大幅に改善されます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP ネイバー セッションが不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。ルートのダンプニングの詳細については、「内部 BGP 機能の設定」モジュールを参照してください。

BGP ネイバー の高速セッションの非アクティブ化の設定

BGP ネイバーを持つピアリング セッションを確立し、このピアリング セッションを高速セッションの非アクティブ化に設定して、このピアリングセッションが無効にされた場合のネットワーク コンバージェンス時間を向上するには、次の作業を実行します。

BGP ネイバーの高速セッションの非アクティブ化を有効にすると、BGP コンバージェンス時間が大幅に向上します。ただし、不安定な IGP ピアにより、引き続き BGP ネイバー セッションが不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. 次のいずれかのコマンドを入力します。
   - **address-family ipv4** [**unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
   - **address-family ipv6** [**unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **fall-over**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	次のいずれかのコマンドを入力します。 • **address-family ipv4** [**unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] • **address-family ipv6** [**unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast vrf blue`	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、IPv6アドレッシングを有効にします。この手順は、VRFアドレス ファミリの高速セッションの非アクティブ化を設定する場合に実行します。 （注） 手順 4 は、VRF で高速セッションの非アクティブ化を設定する場合にのみ必要です。VRF で高速セッションの非アクティブ化を設定しない場合は、この手順をスキップし、アドレスファミリ コンフィギュレーション モード（config-router-af）ではなく、ルータ BGP モード（config-router）で以下のコマンドを実行してください。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 10.0.0.1 remote-as 50000`	BGP ネイバーを持つピアリング セッションを確立します。
ステップ 6	**neighbor** *ip-address* **fall-over** 例： `Device(config-router-af)# neighbor 10.0.0.1 fall-over`	高速セッションを無効にするようにBGP ピアリングを設定します。 • BGPは、セッションが無効になると、このピアで学習したすべてのルートを削除します。
ステップ 7	**end** 例：	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# end`	

高速セッションの非アクティブ化の選択的アドレス トラッキングの設定

高速セッションの非アクティブ化の選択的アドレス トラッキングを設定するには、次の作業を実行します。**neighbor fall-over** コマンドのオプションの **route-map** キーワードおよび *map-name* 引数を使用して、BGP ピアへのルートが変更されたときに BGP ネイバーを持つピアリング セッションを非アクティブ化（リセット）する必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、deny 文が返された場合、ピア セッションがリセットされます。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **fall-over** [**route-map** *map-name*]
6. **exit**
7. **ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network* / *length* | **permit** *network* / *length*} [**ge** *ge-value*] [**le** *le-value*]
8. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
9. **match ip address prefix-list** *prefix-list-name* [*prefix-list-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **fall-over** [**route-map** *map-name*] 例： `Device(config-router)# neighbor 192.168.1.2 fall-over route-map CHECK-NBR`	BGP へのルートが変更されるときにルート マップを適用します。 • この例では、ネイバー 192.168.1.2 へのルートが変更されるときに、CHECK-NBR という名前のルート マップが適用されます。
ステップ 6	**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 7	**ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network / length* | **permit** *network / length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28`	BGP ネクストホップ ルート フィルタリングのプレフィックス リストを作成します。 • 選択的ネクストホップ ルート フィルタリングは、アドレス ファミリごとにプレフィックス長のマッチングまたは送信元プロトコルのマッチングをサポートします。 • この例では、マスク長が 28 以上の場合だけルートを許可する FILTER28 という名前のプレフィックス リストが作成されます。
ステップ 8	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map CHECK-NBR permit 10`	ルート マップを設定し、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。 • この例では、CHECK-NBR という名前のルート マップが作成されます。次の **match** コマンドで IP アドレスの一致がある場合、その IP アドレスは許可されます。

	コマンドまたはアクション	目的
ステップ 9	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] 例： `Device(config-route-map)# match ip address prefix-list FILTER28`	指定されたプレフィックス リスト内の IP アドレスのマッチングを行います。 • プレフィックスリストの名前を指定するには、*prefix-list-name* 引数を使用します。省略記号は、複数のプレフィックス リストを指定できることを意味します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 10	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

次の作業

ピア ポリシー テンプレートの作成後、ピア ポリシー テンプレートのコンフィギュレーションを、別のピア ポリシー テンプレートに継承、または適用することができます。ピア ポリシーの継承の詳細については、「inherit peer-policy コマンドを使用したピア ポリシーテンプレートの継承の設定」の項または「neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定」の項を参照してください。

BGP IPv6 ネイバーの BFD の設定

Cisco IOS Release 15.1(2)S 以降では、双方向フォワーディング検出（BFD）を IPv6 アドレスがある BGP ネイバーに使用できます。

BFD ネイバーがアップ状態であることが確認されると、**show bgp ipv6 unicast neighbors** コマンドは、高速フォールオーバーを検出するためにBFDを使用することを、指定されたネイバーに示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 cef**
5. **interface** *type number*
6. **ipv6 address** *ipv6-address* / *prefix-length*
7. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

8. **no shutdown**
9. **exit**
10. **router bgp** *autonomous-system-number*
11. **no bgp default ipv4-unicast**
12. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
13. **neighbor** *ipv6-address* **remote-as** *autonomous-system-number*
14. **neighbor** *ipv6-address* **fall-over bfd**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 4	**ipv6 cef** 例： `Device(config)# ipv6 cef`	IPv6 のシスコ エクスプレス フォワーディングを有効にします。
ステップ 5	**interface** *type number* 例： `Device(config)# interface fastethernet 0/1`	インターフェイス タイプと番号を設定します。
ステップ 6	**ipv6 address** *ipv6-address* / *prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1:1::1/64`	IPv6 アドレスを設定し、インターフェイスで IPv6 処理を有効にします。
ステップ 7	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value* 例：	インターフェイスのベースライン BFD セッション 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
	`Device(config-if)# bfd interval 500 min_rx 500 multiplier 3`	
ステップ 8	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスを再起動します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 10	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 11	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	ピアリング セッションを確立するためのデフォルトの IPv4 ユニキャスト アドレス ファミリを無効にします。 • グローバル スコープでこのコマンドを設定することを推奨します。
ステップ 12	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] 例： `Device(config-router)# address-family ipv6`	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、IPv6 アドレッシングを有効にします。
ステップ 13	**neighbor** *ipv6-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 2001:DB8:2:1::4 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv6 BGP ネイバー テーブルに追加します。
ステップ 14	**neighbor** *ipv6-address* **fall-over bfd** 例： `Device(config-router-af)# neighbor 2001:DB8:2:1::4 fall-over bfd`	BGP が BFD を使用して IPv6 ネイバーのピアリング セッションをモニタできるようにします。
ステップ 15	**end** 例：	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# end`	

BGP ネイバー セッションの TTL セキュリティ チェックの設定

IP パケット ヘッダーの TTL 値が BGP ネイバー セッション用に設定された TTL 値以上の場合のみ BGP がセッションを確立または維持できるようにするには、次の作業を実行します。

始める前に

- TTL セキュリティ チェックに対する BGP サポート機能の効果を最大化するために、参加している各ルータでこの機能を設定することを推奨します。この機能を有効にすると、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。

（注）
- TTL セキュリティ チェックに対する BGP サポート機能がマルチホップ ネイバー セッション用に設定されている場合、**neighbor ebgp-multihop** コマンドは必要なく、この機能を設定する前にこのコマンドを無効にする必要があります。
- 大きい直径のマルチホップ ピアリングでは、TTL セキュリティ チェックに対する BGP サポート機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影響を受けたネイバー セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。
- この機能は、ローカル ネットワークおよびリモート ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、ローカル ネットワークとリモート ネットワークの間のネットワーク セグメント上のピアも含まれます。

手順の概要

1. **enable**
2. **trace** [*protocol*] *destination*
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **neighbor** *ip-address* **ttl-security hops** *hop-count*
6. **end**
7. **show running-config**
8. **show ip bgp neighbors** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**trace** [*protocol*] *destination* 例： `Device# trace ip 10.1.1.1`	パケットが宛先に移動中、実際に通過する指定されたプロトコルのルートを検出します。 • **trace** コマンドを入力して、指定されたピアへのホップ カウントを決定します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 5	**neighbor** *ip-address* **ttl-security hops** *hop-count* 例： `Device(config-router)# neighbor 10.1.1.1 ttl-security hops 2`	2 つのピアを区切るホップの最大数を設定します。 • *hop-count* 引数は、ローカル ピアとリモート ピアを区切るホップ カウントに設定されます。IP パケット ヘッダーの予想される TTL 値が 254 の場合、数値 1 を *hop-count* 引数に設定する必要があります。値の範囲は、1 ～ 254 の数番です。 • TTL セキュリティ チェックに対する BGP サポート機能が有効な場合、BGP は、予想値以上の TTL 値を持つ着信 IP パケットを受け入れます。受け入れられないパケットは廃棄されます。 • この設定例では、予想される着信 TTL 値が 253（255 引く TTL 値の 2）以上に設定されます。これは、BGP ピアから予想される最小 TTL 値です。ローカル ルータは、10.1.1.1 ネイバーが 1 または 2 ホップ離れている場合だけ、このネイバーからのピアリング セッションを受け入れます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-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。
ステップ 7	**show running-config** 例： `Device# show running-config | begin bgp`	（任意）現在実行中のコンフィギュレーション ファイルの内容を表示します。 • このコマンドの出力は、各ピアの **neighbor ttl-security** コマンドの設定を出力の BGP コンフィギュレーション セクションの下に表示します。そのセクションには、ネイバー アドレスおよび構成されたホップ カウントが含まれます。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**show ip bgp neighbors** [*ip-address*] 例： `Device# show ip bgp neighbors 10.4.9.5`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このコマンドは、TTL セキュリティ チェックに対する BGP サポート機能が有効になっている場合、「External BGP neighbor may be up to *number* hops away」と表示します。この *number* 値は、ホップ カウントを表します。これは、1 ～ 254 の数値です。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

TTL セキュリティ チェックに対する BGP サポート機能の設定は、**show running-config** コマンドおよび **show ip bgp neighbors** コマンドを使用して確認できます。この機能は、各ピアでローカルに設定されるため、確認するリモート設定はありません。

次に、**show running-config** コマンドの出力例を示します。この出力は、着信 IP パケットの予想される TTL カウントが 253 または 254 の場合だけ、ネイバー 10.1.1.1 がネイバー セッションを確立または維持するように設定されていることを示します。

```
Router# show running-config
| begin bgp

router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 55000
 neighbor 10.1.1.1 ttl-security hops 2
 no auto-summary
.
.
.
```

次に、**show ip bgp neighbors** コマンドの出力例を示します。この出力は、10.1.1.1 ネイバーが 2 ホップ以下離れている場合だけ、ローカル ルータがパケットをこのネイバーから受け入れることを示します。この機能の設定は、出力のアドレス ファミリ セクションに表示されます。関連行は、出力に太字で表示されます。

```
Router# show ip bgp neighbors 10.1.1.1
BGP neighbor is 10.1.1.1,  remote AS 55000, external link
  BGP version 4, remote router ID 10.2.2.22
  BGP state = Established, up for 00:59:21
  Last read 00:00:21, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  2          2
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           226        227
    Route Refresh:          0          0
    Total:                228        229
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue sizes : 0 self, 0 replicated
  Index 1, Offset 0, Mask 0x2
  Member of update-group 1
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 2; dropped 1
  Last reset 00:59:50, due to User reset
  External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.2.2.22, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 11001
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
```

```
Event Timers (current time is 0xCC28EC):
Timer          Starts    Wakeups            Next
Retrans            63          0             0x0
TimeWait            0          0             0x0
AckHold            62         50             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss:  712702676  snduna:  712703881  sndnxt:  712703881     sndwnd:  15180
irs: 2255946817  rcvnxt: 2255948041  rcvwnd:      15161  delrcvwnd:   1223
SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 76 (out of order: 0), with data: 63, total data bytes: 1223
Sent: 113 (retransmit: 0, fastretransmit: 0), with data: 62, total data bytes: 4
```

セッションごとの TCP の PMTUD に対する BGP サポートの設定

ここでは、次のタスクについて説明します。

すべての BGP セッションに対する TCP の PMTUD のグローバルな無効化

すべての BGP セッションに対して TCP の PMTUD を無効にするには、次の作業を実行します。BGP セッションを設定するときに TCP の PMTUD は、デフォルトで有効になりますが、**show ip bgp neighbors** コマンドを入力して、TCP の PMTUD が有効になっていることを確認することを推奨します。

始める前に

この作業は、アクティブな TCP 接続を持つ BGP ネイバーを事前に設定済みであることを前提としています。

手順の概要

1. **enable**
2. **show ip bgp neighbors** [*ip-address*]
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **no bgp transport path-mtu-discovery**
6. **end**
7. **show ip bgp neighbors** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• 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 bgp neighbors** [*ip-address*] 例： `Device# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このコマンドを使用して、BGP ネイバーで TCP の PMTUD が無効かどうかを判断します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 50000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 5	**no bgp transport path-mtu-discovery** 例： `Device(config-router)# no bgp transport path-mtu-discovery`	すべての BGP セッションに対して TCP の PMTUD を無効にします。
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。
ステップ 7	**show ip bgp neighbors** [*ip-address*] 例： `Device# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、任意のネイバーで TCP の PMTUD が有効であることは、このコマンドの出力によっては表示されません。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対して有効になっていることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD が有効であることを示します。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

次に、**no bgp transport path-mtu-discovery** コマンドを入力した後の **show ip bgp neighbors** コマンドの出力例を示します。path mtu エントリが欠落していることに注意してください。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle
```

単一の BGP ネイバーに対する TCP の PMTUD の無効化

内部 BGP（iBGP）ネイバーを持つピアリング セッションを確立してから BGP ネイバー セッションに対して TCP の PMTUD を無効にするには、次の作業を実行します。**neighbor transport** コマンドは、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで使用できます。

始める前に

この作業では、TCP の PMTUD がすべての BGP ネイバーに対してデフォルトで有効になっていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address*| *peer-group-name*} **activate**
7. **no neighbor** {*ip-address*| *peer-group-name*} **transport**{**connection-mode** | **path-mtu-discovery**}
8. **end**
9. **show ip bgp neighbors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**ipv4** [**mdt**	**multicast**	**unicast** [**vrf** *vrf-name*]	**vrf** *vrf-name*]	**vpnv4** [**unicast**]} 例：	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、アドレスファミリ固有の設定を受け入れるよう BGP ピアを設定します。

	コマンドまたはアクション	目的
	`Device(config-router)# address-family ipv4 unicast`	• この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 172.16.1.1 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。
ステップ 7	**no neighbor** {*ip-address*| *peer-group-name*} **transport**{**connection-mode** | **path-mtu-discovery**} 例： `Device(config-router-af)# no neighbor 172.16.1.1 transport path-mtu-discovery`	単一の BGP ネイバーに対して TCP の PMTUD を無効にします。 • この例では、TCP の PMTUD がネイバー 172.16.1.1 に対して無効になります。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、このネイバーが TCP の PMTUD を有効にしたことを表示しません。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力例は、TCP の PMTUD が BGP ネイバー 172.16.1.1 に対して無効にされたが、BGP ネイバー 192.168.2.2 に対しては引き続き有効であることを示します。この出力の

2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD が有効であることを示します。

```
Router# show ip bgp neighbors
BGP neighbor is 172.16.1.1,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.17.1.99
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.1
  Address tracking requires at least a /24 route to the peer
  Connections established 1; dropped 0
  Last reset never
.
.
.
SRTT: 165 ms, RTTO: 1172 ms, RTV: 1007 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle
.
.
.
BGP neighbor is 192.168.2.2,  remote AS 50000, external link
  BGP version 4, remote router ID 10.2.2.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 192.168.2.2
  Address tracking requires at least a /24 route to the peer
  Connections established 2; dropped 1
  Last reset 00:05:11, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 210 ms, RTTO: 904 ms, RTV: 694 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

すべての BGP セッションに対する TCP の PMTUD のグローバルな有効化

すべての BGP セッションに対して TCP の PMTUD を有効にするには、次の作業を実行します。BGP セッションを設定するときに TCP の PMTUD はデフォルトで有効になりますが、セッションごとの TCP の PMTUD に対する BGP サポート機能が無効になっている場合、この作業によってこの機能を再度有効にできます。TCP の PMTUD が有効であることを確認するには、**show ip bgp neighbors** コマンドを使用します。

始める前に

この作業は、アクティブな TCP 接続を持つ BGP ネイバーを事前に設定済みであることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp transport path-mtu-discovery**
5. **end**
6. **show ip bgp neighbors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**bgp transport path-mtu-discovery** 例： `Device(config-router)# bgp transport path-mtu-discovery`	すべての BGP セッションに対して TCP の PMTUD を有効にします。
ステップ 5	**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 6	**show ip bgp neighbors** 例： `Device# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、すべてのネイバーが TCP の PMTUD を有効にしたことを表示します。

	コマンドまたはアクション	目的
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対して有効になっていることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD が有効であることを示します。

```
Router# show ip bgp neighbors
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

単一の BGP ネイバーに対する TCP の PMTUD の有効化

eBGP ネイバーを持つピアリング セッションを確立してから BGP ネイバー セッションに対して TCP の PMTUD を有効にするには、次の作業を実行します。**neighbor transport** コマンドは、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで使用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*

6. **neighbor** {*ip-address*| *peer-group-name*} **activate**
7. **neighbor** {*ip-address*| *peer-group-name*} **transport**{**connection-mode** | **path-mtu-discovery**}
8. **end**
9. **show ip bgp neighbors** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**ipv4** [**mdt**	**multicast**	**unicast** [**vrf** *vrf-name*]	**vrf** *vrf-name*]	**vpnv4** [**unicast**]} 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.2.2 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.2 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。
ステップ 7	**neighbor** {*ip-address*	*peer-group-name*} **transport**{**connection-mode**	**path-mtu-discovery**} 例：	単一の BGP ネイバーに対して TCP の PMTUD を有効にします。

	コマンドまたはアクション	目的
	`Device(config-router-af)# neighbor 192.168.2.2 transport path-mtu-discovery`	
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp neighbors** [*ip-address*] 例： `Device# show ip bgp neighbors 192.168.2.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバー 192.168.2.2 に対して有効になっていることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD が有効であることを示します。

```
Router# show ip bgp neighbors 192.168.2.2
BGP neighbor is 192.168.2.2,  remote AS 50000, external link
  BGP version 4, remote router ID 10.2.2.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 192.168.2.2
  Address tracking requires at least a /24 route to the peer
  Connections established 2; dropped 1
  Last reset 00:05:11, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 210 ms, RTTO: 904 ms, RTV: 694 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

BGP ネイバー セッション オプションの設定例

例：BGP ネイバーの高速セッションの非アクティブ化の設定

次の例では、BGP ルーティング プロセスがデバイス A およびデバイス B で設定され、この 2 つのデバイス間でネイバー セッションの高速ピアリング セッションの非アクティブ化をモニタし、使用します。高速ピアリング セッションの非アクティブ化は、このネイバー セッションの両方のデバイスで必要ではありませんが、このネイバーセッションが非アクティブ化されている場合、両方の自律システムの BGP ネットワークのより高速なコンバージェンスに役立ちます。

デバイス A

```
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 fall-over
 end
```

デバイス B

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

例：高速セッションの非アクティブ化の選択的アドレストラッキングの設定

次に、/28 のプレフィックスを持つルートまたはピアの宛先へのさらに特定されたルートを使用できなくなった場合に、BGP ピアリング セッションをリセットするようにこのセッションを設定する方法の例を示します。

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 end
```

例：BGP IPv6 ネイバーの BFD の設定

次に、IPv6 アドレス 2001:DB8:4:1::1 の FastEthernet インターフェイス 0/1 を設定する例を示します。双方向フォワーディング検出（BFD）は BGP ネイバー 2001:DB8:5:1::2 に対して設定さ

れます。BFD は、BGP ネイバーの転送パスの障害を追跡し、転送パス障害後の BGP 再コンバージェンス時間を短縮します。

```
ipv6 unicast-routing
ipv6 cef
interface fastethernet 0/1
 ipv6 address 2001:DB8:4:1::1/64
 bfd interval 500 min_rx 500 multiplier 3
 no shutdown
 exit
router bgp 65000
 no bgp default ipv4-unicast
 address-family ipv6 unicast
 neighbor 2001:DB8:5:1::2 remote-as 65001
 neighbor 2001:DB8:5:1::2 fall-over bfd
 end
```

例：TTL セキュリティ チェックの設定

このセクションの設定例は、TTL セキュリティ チェックに対する BGP サポート機能を設定する方法を示します。

次の例では、**trace** コマンドを使用して、eBGP ピアへのホップ カウントを決定します。このホップ カウント数は、指定されたネイバーに到着するために IP パケットが通過する各ネットワーキング デバイスの出力に表示されます。次の例では、10.1.1.1 ネイバーのホップ カウントは 1 です。

```
Router# trace ip 10.1.1.1
Type escape sequence to abort.
Tracing the route to 10.1.1.1
  1 10.1.1.1 0 msec *  0 msec
```

次の例では、10.1.1.1 ネイバーのホップ カウントを 2 に設定します。hop-count 引数が 2 に設定されるため、BGP は、ヘッダーの TTL カウントが 253 以上の IP パケットだけを受け入れます。

```
Router(config-router)# neighbor 10.1.1.1 ttl-security hops 2
```

例：セッションごとの TCP の PMTUD に対する BGP サポートの設定

ここでは、次の設定例を示します。

例：すべての BGP セッションに対する TCP の PMTUD のグローバルな無効化

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD を無効にする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD が無効になっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  no bgp transport path-mtu-discovery
```

```
  end
show ip bgp neighbors
```

例：単一の BGP ネイバーに対する TCP の PMTUD の無効化

次に、eBGP ネイバー 192.168.2.2 に対して TCP の PMTUD を無効にする方法の例を示します。

```
enable
configure terminal
 router bgp 45000
  neighbor 192.168.2.2 remote-as 50000
  neighbor 192.168.2.2 activate
  no neighbor 192.168.2.2 transport path-mtu-discovery
  end
show ip bgp neighbors 192.168.2.2
```

例：すべての BGP セッションに対する TCP の PMTUD のグローバルな有効化

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD を有効にする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD が有効になっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  bgp transport path-mtu-discovery
  end
show ip bgp neighbors
```

例：単一の BGP ネイバーに対する TCP の PMTUD の有効化

次に、eBGP ネイバー 192.168.2.2 に対して TCP の PMTUD を有効にする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD が有効になっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  neighbor 192.168.2.2 remote-as 50000
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 transport path-mtu-discovery
  end
show ip bgp neighbors 192.168.2.2
```

次の作業

拡張コミュニティとして自律システム出口リンクの帯域幅をアドバタイズする方法については、「BGP リンク帯域幅」モジュールを参照してください。

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』
BGP 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、コマンド履歴、使用上の注意事項、および例	『Cisco IOS IP Routing: BGP Command Reference』
Cisco BGP のコンセプト情報の概要と各 BGP モジュールへのリンク	「Cisco BGP 概要」モジュール
BGP の基本作業の概念および設定の詳細	「基本 BGP ネットワークの設定」モジュール
BGP の高度な作業の概念および設定の詳細	「BGP の拡張機能の設定」モジュール
双方向フォワーディング検出の設定作業	『*IP Routing: BFD Configuration Guide*』

標準

標準	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB のリンク
CISCO-BGP4-MIB	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	タイトル
RFC 1191	『*Path MTU Discovery*』

RFC	タイトル
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

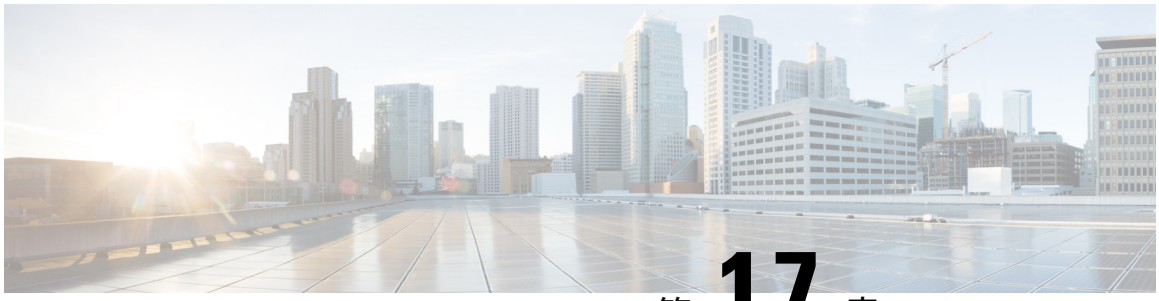
BGP ネイバー セッションのオプション設定の機能情報

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

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *32 : BGP* ネイバー セッションのオプション機能設定の機能情報

機能名	リリース	機能情報
セッションごとの TCP の PMTUD に対する BGP サポート	12.2(33)SRA 12.2(31)SB 12.2(33)SXH 12.4(20)T 15.0(1)S	TCP の Path MTU Discovery（PMTUD）に対する BGP サポートにより、各 BGP セッションに対する最良 TCP の Path MTU を BGP が自動的に検出する機能が導入されました。この TCP の Path MTU はすべての BGP ネイバー セッションに対してデフォルトでイネーブルになりますが、すべての BGP セッションに対してグローバルにまたは個別の BGP ネイバーセッションに対してディセーブルにでき、その後イネーブルにできます。 この機能により、次のコマンドが導入または変更されました。**bgp transport**、**neighbor transport**、**show ip bgp neighbors**
TTL セキュリティ チェックに対する BGP サポート	12.0(27)S 12.3(7)T 12.2(25)S 12.2(18)SXE 15.0(1)S	TTL セキュリティ チェックに対する BGP サポート機能により、簡単なセキュリティメカニズムが導入され、外部ボーダーゲートウェイ プロトコル（eBGP）ピアリング セッションを偽造 IP パケットを使用する CPU 利用率に基づく攻撃から防御します。この機能をイネーブルにすると、どちらの BGP ネットワークの一部でもないネットワーク セグメント上のホストまたは eBGP ピア間にないネットワーク セグメント上のホストによる eBGP ピアリング セッションを乗っ取ろうとする試みを防ぐことができます。 この機能により、次のコマンドが導入または変更されました。**neighbor ttl-security**、 **show ip bgp neighbors**
シングルホップ BFD に対する BGP IPv6 クライアント	15.1(2)S 15.2(3)T 15.2(4)S	IPv6 アドレスを使用する BGP ネイバーの高速転送パス障害を追跡するために、双方向フォワーディング検出（BFD）を使用できます。 この機能により、**neighbor fall-over** コマンドが変更されました。 Cisco IOS Release 15.2(4)S では、Cisco 7200 シリーズ ルータのサポートが追加されました。



第 17 章

BGP ネイバー ポリシー

BGP ネイバー ポリシー機能により、ローカル ポリシー、および継承されたポリシーに関する情報を表示するための既存の 2 つのコマンドに新しいキーワードが導入されます。BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。

- 機能情報の確認 （457 ページ）
- BGP ネイバー ポリシーに関する情報 （458 ページ）
- BGP ネイバー ポリシー情報の表示方法 （458 ページ）
- その他の参考資料 （459 ページ）
- BGP ネイバー ポリシーの機能情報 （459 ページ）

機能情報の確認

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

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

BGP ネイバー ポリシーに関する情報

BGP ネイバー ポリシー機能の利点

BGP ネイバー ポリシー機能により、ローカル ポリシー、および継承されたポリシーに関する情報を表示するための **show ip bgp neighbors policy** コマンドと **show ip bgp template peer-policy** コマンドに新しいキーワードが導入されます。BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。

BGP ネイバー ポリシー情報の表示方法

BGP ネイバー ポリシー情報の表示

手順の概要

1. **enable**
2. **show ip bgp neighbors** { *ip-address* | *ipv6-address* } **policy** [**detail**]
3. **show ip bgp template peer-policy** [*policy-template-name* [**detail**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp neighbors** { *ip-address* | *ipv6-address* } **policy** [**detail**] 例： `Device# show ip bgp neighbors 192.168.2.3 policy detail`	指定したネイバーに適用されるポリシーを表示します。
ステップ 3	**show ip bgp template peer-policy** [*policy-template-name* [**detail**]] 例： `Device# show ip bgp template peer-policy`	ローカルに設定されたピア ポリシー テンプレートを表示します。

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

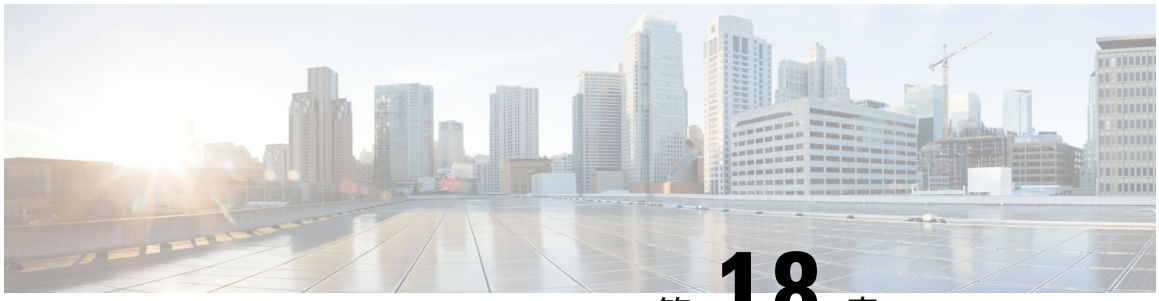
BGP ネイバー ポリシーの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *33 : BGP* ネイバー ポリシーの機能情報

機能名	リリース	機能情報
BGP ネイバー ポリシー		BGP ネイバー ポリシー機能により、ローカル ポリシー、および継承されたポリシーに関する情報を表示するための既存の 2 つのコマンドに新しいキーワードが導入されます。BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。継承されたポリシーは、ピア グループ、またはピア ポリシー テンプレートからネイバーが継承したポリシーです。 次のコマンドが変更されました。**show ip bgp neighbors**、**show ip bgp template peer-policy**



第 18 章

BGP ダイナミック ネイバー

BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。各範囲は、サブネット IP アドレスとして設定できます。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。

- 機能情報の確認 （461 ページ）
- BGP ダイナミック ネイバーに関する情報 （462 ページ）
- BGP ダイナミック ネイバーの設定方法 （462 ページ）
- BGP ダイナミック ネイバーの設定例 （472 ページ）
- その他の参考資料 （475 ページ）
- BGP ダイナミック ネイバーの機能情報 （476 ページ）

機能情報の確認

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

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

BGP ダイナミック ネイバーに関する情報

BGP ダイナミック ネイバー

BGP ダイナミック ネイバーに対するサポート機能が Cisco Catalyst 6500 シリーズ スイッチの Cisco IOS Release 12.2(33)SXH に導入されました。BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。各範囲は、サブネット IP アドレスとして設定できます。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。

Cisco IOS XE Denali 16.3 リリースでは、BGP ダイナミック ネイバーのサポートが、VRF のサポートを含む IPv6 BGP ピアリングに拡張されました。

サブネットの範囲が BGP ピア グループに対して設定され、TCP セッションがそのサブネットの範囲の IP アドレスに対して別のルータによって開始された後、新しい BGP ネイバーがそのグループのメンバとしてダイナミックに作成されます。サブネットの範囲の初期設定および（受信範囲グループと呼ばれる）ピア グループのアクティベーションの後、ダイナミック BGP ネイバーの作成には、初期ルータへのさらなる CLI 設定は必要ありません。その他のルータは、初期ルータを使用する BGP セッションを確立できますが、BGP セッションに使用されるリモート ピアの IP アドレスが設定された範囲内にない場合、この初期ルータは、この BGP セッションを設定する必要はありません。

BGP ダイナミック ネイバー機能をサポートするために、**show ip bgp neighbors**、**show ip bgp peer-group**、および **show ip bgp summary** コマンドの出力がダイナミック ネイバーに関する情報を表示するように更新されました。

ダイナミック BGP ネイバーは、ピア グループのすべての設定を継承します。大きい BGP ネットワークで BGP ダイナミック ネイバーを実装すると CLI 設定の量と複雑さが軽減され、CPU とメモリの使用量が節約されます。IPv4 ピアリングだけがサポートされます。

BGP ダイナミック ネイバーの設定方法

サブネット範囲を使用する BGP ダイナミック ネイバーの実装

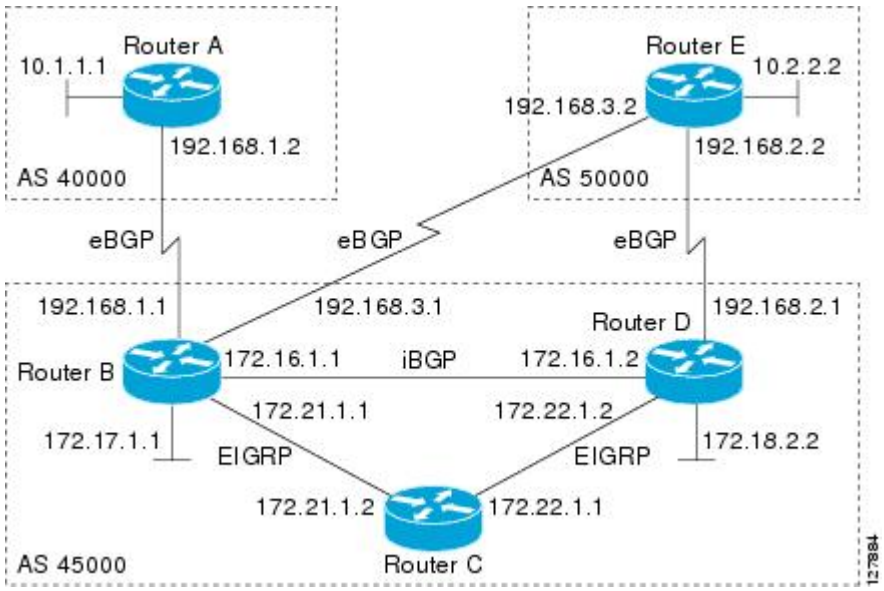
Cisco IOS Release 12.2(33)SXH では、BGP ダイナミック ネイバーに対するサポートが導入されました。サブネット範囲を使用する BGP ネイバーのダイナミックな作成を実装するには、次の作業を実行します。

この作業では、BGP ピア グループが下の図のルータ B に作成され、ダイナミック BGP ネイバー数に関してグローバル制限が設定されて、サブネット範囲がピア グループに関連付けられます。サブネット範囲を設定すると、ダイナミック BGP ネイバー プロセスがイネーブルになります。ピア グループがローカル ルータの BGP ネイバー テーブルに追加され、代替自律シス

テム番号も設定されます。ピア グループは、IPv4 アドレス ファミリの下でアクティブ化されます。

次の手順では、別のルータ（下の図のルータ E）に移動します。ここで、BGP セッションが開始され、ネイバー ルータであるルータ B がリモート BGP ピアとして設定されます。このピアリング設定は、TCP セッション（192.168.3.2）を開始する IP アドレスがダイナミック BGP ピアに対して設定されたサブネット範囲内にあるため、TCP セッションを開き、ルータ B にダイナミック BGP ネイバーを作成させます。この作業では、最初のルータであるルータ B に戻り、ダイナミック BGP ピア情報を表示するように変更された 3 つの **show** コマンドが実行されます。

図 *36 : BGP* ダイナミック ネイバー トポロジ



始める前に

この作業では、Cisco IOS Release 12.2(33)SXH、またはこれ以降のリリースが実行中である必要があります。

（注） この作業は、IPv4 BGP ピアリングだけをサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **neighbor** *peer-group-name* **peer-group**
6. **bgp listen** [**limit** *max-number*]

7. **bgp listen** [**limit** *max-number* | **range** *network* / *length* **peer-group** *peer-group-name*]
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
9. **neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
10. **address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]]
11. **neighbor** {*ip-address* | *peer-group-name*} **activate**
12. **end**
13. この作業で設定された BGP ピア グループのサブネット範囲内にインターフェイスを持つ別のルータに移動します。
14. **enable**
15. **configure terminal**
16. **router bgp** *autonomous-system-number*
17. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
18. 最初のルータに戻ります。
19. **show ip bgp summary**
20. **show ip bgp peer-group** [*peer-group-name*] [**summary**]
21. **show ip bgp neighbors** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `DeviceB> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 • この設定はルータ B に入力されます。
ステップ 2	**configure terminal** 例： `DeviceB# 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： `DeviceB(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp log-neighbor-changes** 例： `DeviceB(config-router)# bgp log-neighbor-changes`	（任意）BGP ネイバー ステータスの変更（アップまたはダウン）およびネイバーのリセットのロギングをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高い

	コマンドまたはアクション	目的
		ことやパケット損失の多いことが考えられるので、調査するようにしてください。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `DeviceB(config-router)# neighbor group192 peer-group`	BGP ピア グループを作成します。 • この例では、グループ 192 という名前のピア グループが作成されます。このグループは、受信範囲グループとして使用されます。
ステップ 6	**bgp listen** [**limit** *max-number*] 例： `DeviceB(config-router)# bgp listen limit 200`	BGP ダイナミック サブネット範囲ネイバーのグローバル制限を設定します。 • オプションの **limit** キーワードおよび *max-number* 引数を使用して、作成可能な BGP ダイナミック サブネット範囲ネイバーの最大数を定義します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細な構文については、手順 7 を参照してください。
ステップ 7	**bgp listen** [**limit** *max-number* | **range** *network* / *length* **peer-group** *peer-group-name*] 例： `DeviceB(config-router)# bgp listen range 192.168.0.0/16 peer-group group192`	サブネット範囲を BGP ピア グループと関連付け、BGP ダイナミック ネイバー機能をアクティブにします。 • オプションの **limit** キーワードおよび *max-number* 引数を使用して、作成可能な BGP ダイナミック ネイバーの最大数を定義します。 • オプションの **range** キーワードおよび *network* / *length* 引数を使用して、指定したピア グループに関連付けられるプレフィックス範囲を定義します。 • この例では、プレフィックス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲グループに関連付けられます。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `DeviceB(config-router)# neighbor group192 ebgp-multihop 255`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

	コマンドまたはアクション	目的
ステップ 9	**neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] 例： `DeviceB(config-router)# neighbor group192 remote-as 40000 alternate-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • オプションの **alternate-as** キーワードおよび *autonomous-system-number* 引数を使用して、受信範囲ネイバーに対して最大 5 つの代替自律システム番号を特定します。 • この例では、グループ 192 という名前のピア グループが 2 つの可能な自律システム番号とともに設定されます。 （注） **alternate-as** キーワードは、受信範囲ピア グループとともにだけ使用され、個別の BGP ネイバーとは使用されません。
ステップ 10	**address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]] 例： `DeviceB(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `DeviceB(config-router-af)# neighbor group192 activate`	設定されたアドレス ファミリに対してネイバーまたは受信範囲ピア グループをアクティブにします。 • この例では、ネイバー 172.16.1.1 が IPv4 アドレス ファミリに対してアクティブにされます。 （注） 通常、BGP ピア グループは、このコマンドを使用してアクティブにできませんが、受信範囲ピア グループは特別です。
ステップ 12	**end** 例： `DeviceB(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 13	この作業で設定された BGP ピア グループのサブネット範囲内にインターフェイスを持つ別のルータに移動します。	-
ステップ 14	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`DeviceE> enable`	• この設定はルータ E に入力されます。
ステップ 15	**configure terminal** 例： `DeviceE# 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 16	**router bgp** *autonomous-system-number* 例： `DeviceE(config)# router bgp 50000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 17	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] 例： `DeviceE(config-router)# neighbor 192.168.3.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ルータ E のインターフェイス（上の図の 192.168.3.2）が BGP 受信範囲グループであるグループ 192 用に設定されたサブネット範囲とともにあります。TCP がルータ B のピアに対してセッションを開くと、ルータ B はこのピアをダイナミックに作成します。
ステップ 18	最初のルータに戻ります。	-
ステップ 19	**show ip bgp summary** 例： `DeviceB# show ip bgp summary`	（任意）BGP ネイバーへのすべての接続の BGP パス、プレフィックス、および属性情報を表示します。 • この手順では、この設定はルータ B に戻っています。
ステップ 20	**show ip bgp peer-group** [*peer-group-name*] [**summary**] 例： `DeviceB# show ip bgp peer-group group192`	（任意）BGP ピア グループの情報を表示します。
ステップ 21	**show ip bgp neighbors** [*ip-address*] 例： `DeviceB# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの BGP および TCP 接続についての情報を表示します。 • この例では、ダイナミックに作成されたネイバー 192.168.3.2 の情報が表示されます。この BGP ネイバーの IP アドレスは、**show ip bgp summary** コマンドまたは **show ip bgp peer-group** コマンドの出力にあります。

	コマンドまたはアクション	目的
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に示す出力例は、この作業の適切な設定手順が上の図のルータ B とルータ E の両方で完了した後に、ルータ B から取得されました。

show ip bgp summary コマンドの次の出力は、BGP ネイバー 192.168.3.2 がダイナミックに作成され、この受信範囲グループであるグループ 192 のメンバーであることを示します。この出力は、IP プレフィックス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲に定義されることも示します。

```
Router# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

show ip bgp peer-group コマンドの次の出力は、この作業で設定された受信範囲グループであるグループ 192 の情報を示します。

```
Router# show ip bgp peer-group group192
BGP peer-group is group192,  remote AS 40000
  BGP peergroup group192 listen range group members:
  192.168.0.0/16
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP neighbor is group192, peer-group external, members:
  *192.168.3.2
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
```

show ip bgp neighbors コマンドの次の出力例は、ネイバー 192.168.3.2 がこのピア グループであるグループ 192 のメンバーで、このピアがダイナミックに作成されたことを示すサブセット範囲グループ 192.168.0.0/16 に属していることを示します。

```
Router# show ip bgp neighbors 192.168.3.2
BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
```

```
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

VRF のサポートを含む BGP IPv6 ダイナミック ネイバー サポートの設定

Cisco IOS XE Denali 16.3 リリースでは、BGP ダイナミック ネイバーのサポートが IPv6 BGP ピアリングに拡張されました。

（注） VRF のサポートなしで BGP IPv6 ダイナミック ネイバーを設定することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp listen** [**limit** *max-number* | **range** *network / length* **peer-group** *peer-group-name*]
5. **address-family** [**ipv4** | **ipv6**] [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]]
6. **bgp listen** [**limit** *max-number*]
7. **neighbor** *peer-group-name* **peer-group**
8. **neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
9. **address-family** [**ipv4** | **ipv6**] [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]]
10. **neighbor** {*ip-address* | *peer-group-name*} **activate**
11. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 • この設定はルータ B に入力されます。
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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp listen** [**limit** *max-number* | **range** *network* / *length* **peer-group** *peer-group-name*] 例： `Device(config-router)# bgp listen range 2001::0/64 peer-group group192`	サブネット範囲を BGP ピア グループと関連付け、BGP ダイナミック ネイバー機能をアクティブにします。 • オプションの **limit** キーワードおよび *max-number* 引数を使用して、作成可能な BGP ダイナミック ネイバーの最大数を定義します。 • オプションの **range** キーワードおよび *network* / *length* 引数を使用して、指定したピア グループに関連付けられるプレフィックス範囲を定義します。 • この例では、プレフィックス範囲 2001::0/64 が group192 という名前の受信範囲グループに関連付けられます。
ステップ 5	**address-family** [**ipv4** | **ipv6**] [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]] 例： `Device(config-router-af)# address-family ipv6 unicast vrf vrf1`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 6	**bgp listen** [**limit** *max-number*] 例： `Device(config-router)# bgp listen limit 500`	VRF アドレス ファミリでのプレフィックスの最大数を指定します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router)# neighbor group192 peer-group`	BGP ピア グループを作成します。 • この例では、グループ 192 という名前のピア グループが作成されます。このグループは、受信範囲グループとして使用されます。
ステップ 8	**neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] 例： `Device(config-router)# neighbor group192 remote-as 101 alternate-as 102`	指定した自律システム内のネイバーの IP アドレスまたはピア グループ名を IPv6 BGP ネイバー テーブルに追加します。 • オプションの **alternate-as** キーワードおよび *autonomous-system-number* 引数を使用して、受信範囲ネイバーに対して最大 5 つの代替自律システム番号を特定します。 • この例では、グループ 192 という名前のピア グループが 2 つの可能な自律システム番号とともに設定されます。 （注） **alternate-as** キーワードは、受信範囲ピア グループとともにだけ使用され、個別の BGP ネイバーとは使用されません。
ステップ 9	**address-family** [**ipv4** | **ipv6**] [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]] 例： `Device(config-router-af)# address-family ipv4 unicast vrf vrf1`	このピアグループに対して IPv4 アドレス ファミリを有効にします。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor group192 activate`	設定されたアドレス ファミリに対してネイバーまたは受信範囲ピア グループをアクティブにします。
ステップ 11	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP IPv6 ダイナミック ネイバー設定の確認

グローバル ルーティング テーブルの BGP IPv6 ユニキャスト アドレス ファミリ設定を確認するには、**show bgp ipv6 unicast summary** コマンドを使用します。

```
Device# show bgp ipv6 unicast summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*2001::1 4 50000 2 2 0 0 0 00:00:37 0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
2001::0/64
```

グローバル ルーティング テーブルの IPv6 ダイナミック ネイバー設定を確認するには、**show bgp { ipv4 | ipv6 } unicast peer-group< name>** コマンドを使用します。

```
Device# show bgp ipv6 unicast peer-group group192
BGP peer-group is group192, remote AS 40000
BGP peergroup group192 listen range group members:
2001::0/64
BGP version 4
Default minimum time between advertisement runs is 30 seconds
For address family: IPv6 Unicast
BGP neighbor is group192, peer-group external, members:
*2001::1
Index 0, Offset 0, Mask 0x0
Update messages formatted 0, replicated 0
Number of NLRIs in the update sent: max 0, min 0
```

次のコマンドを使用して、VRF ルーティング テーブルの BGP IPv6 ダイナミック ネイバー設定を確認できます。

- **show bgp vpnv6 unicast vrf <name> neighbors**
- **show bgp vpnv6 unicast vrf <name> summary**
- **show bgp vpnv6 unicast vrf <name> peer-group <name>**
- **debug bgp [ipv6 | vpnv6] unicast range**

BGP ダイナミック ネイバーの設定例

例：サブネット範囲を使用する BGP ダイナミック ネイバーの実装

次の例では、2 つの BGP ピア グループが下の図のルータ B に作成され、ダイナミック BGP ネイバー数に関してグローバル制限が設定され、サブネット範囲がピア グループに関連付けられます。サブネット範囲を設定すると、ダイナミック BGP ネイバー プロセスがイネーブルになります。このピア グループは、ローカル ルータの BGP ネイバー テーブルに追加され、代替自律システム番号もこのピア グループの 1 つであるグループ 192 に設定されます。このサブネット範囲ピア グループおよび標準 BGP ピアは、その後 IPv4 アドレス ファミリの下でアクティブ化されます。

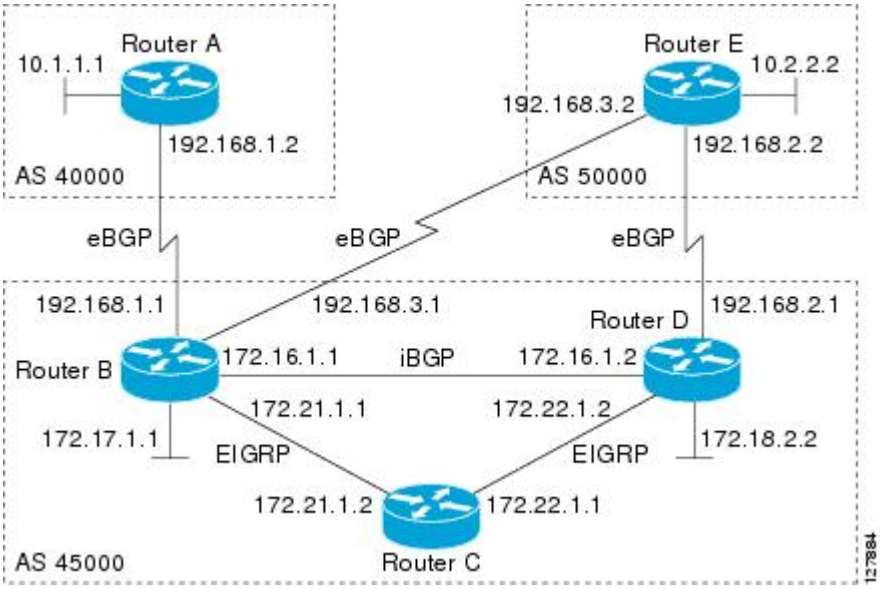
この設定は、別のルータ（下の図のルータ A）に移動します。ここで、BGP セッションが開始され、ネイバー ルータであるルータ B がリモート BGP ピアとして設定されます。このピアリング設定は、TCP セッション（192.168.1.2）を開始する IP アドレスがダイナミック BGP ピア

に対して設定されたサブネット範囲内にあるため、TCP セッションを開き、ルータ B にダイナミック BGP ネイバーを作成させます。

3 番目のルータ（下の図のルータ E）もルータ B を持つ BGP ピアリング セッションを開始します。ルータ E は、代替自律システムに設定されている自律システム 50000 にあります。ルータ B は、別のダイナミック BGP ピアを作成することにより、結果として得られた TCP セッションに応答します。

この例は、ルータ B で入力される **show ip bgp summary** コマンドの出力で終了します。

図 *37 : BGP* ダイナミック ネイバー トポロジ



ルータ B

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 bgp listen limit 200
 bgp listen range 172.21.0.0/16 peer-group group172
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group172 peer-group
 neighbor group172 remote-as 45000
 neighbor group192 peer-group
 neighbor group192 remote-as 40000 alternate-as 50000
 neighbor 172.16.1.2 remote-as 45000
 address-family ipv4 unicast
 neighbor group172 activate
 neighbor group192 activate
 neighbor 172.16.1.2 activate
 end
```

ルータ A

```
enable
```

```
configure terminal
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 exit
```

ルータ E

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

ルータ A とルータ E の両方が設定された後、**show ip bgp summary** コマンドがルータ B で実行されます。この出力は、正規 BGP ネイバー 172.16.1.2 およびルータ A とルータ E がルータ B に対する BGP ピアリングの TCP セッションを開始したときにダイナミックに作成された 2 つの BGP ネイバーを表示します。この出力は、設定された受信範囲サブネット グループに関する情報も表示します。

```
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.2      4 45000      15      15        1    0    0 00:12:20        0
*192.168.1.2    4 40000       3       3        1    0    0 00:00:37        0
*192.168.3.2    4 50000       6       6        1    0    0 00:04:36        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 2/(200 max), Subnet ranges: 2
BGP peergroup group172 listen range group members:
  172.21.0.0/16
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

例：VRF のサポートを含む BGP IPv6 ダイナミック ネイバー サポートの設定

VRF のサポートを含む BGP IPv6 ダイナミック ネイバー サポートの設定

```
enable
configure terminal
router bgp 55000
 bgp listen range 2001::0/64 peer-group group182
  address-family ipv6 unicast vrf vrf2
  bgp listen limit 600
  neighbor group182 peer-group
  neighbor group182 remote-as 103 alternate-as 104
  address-family ipv4 unicast vrf vrf2
  neighbor group182 activate
 end
```

VRF のサポートなしでの BGP IPv6 ダイナミック ネイバー サポートの設定

```
enable
configure terminal
router bgp 100
```

```
bgp listen range 2001::0/64 peer-group group192
bgp listen limit 500
neighbor group192 peer-group
neighbor group192 remote-as 101 alternate-as 102
address family ipv6 unicast
 neighbor group192 activate
 address family ipv4 unicast
 neighbor group192 activate
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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 ダイナミック ネイバーの機能情報

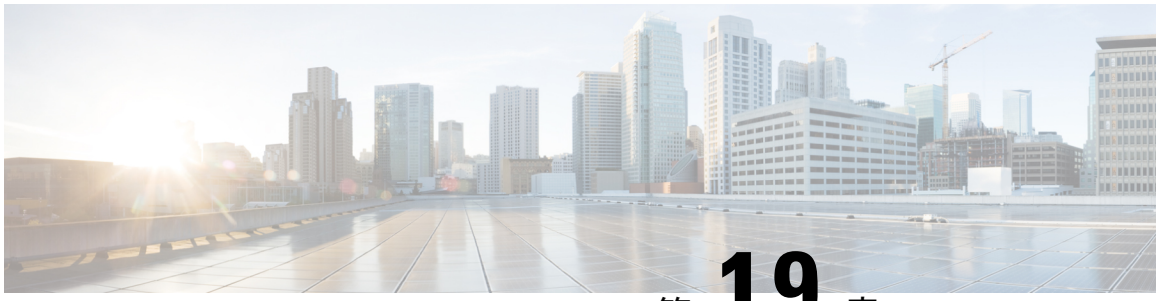
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *34 : BGP* ダイナミック ネイバーの機能情報

機能名	リリース	機能情報
BGP ダイナミック ネイバー		BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。各範囲は、サブネット IP アドレスとして設定できます。BGP ダイナミック ネイバーは、IP アドレスおよびBGP ピア グループの範囲を使用して設定されます。サブネットの範囲が BGP ピア グループに対して設定され、TCP セッションがそのサブネットの範囲の IP アドレスに対して開始された後、新しい BGP ネイバーがそのグループのメンバとしてダイナミックに作成されます。この新しい BGP ネイバーは、ピア グループのすべての設定を継承します。 この機能により、次のコマンドが導入または変更されました。**bgp listen**、**debug ip bgp range**、**neighbor remote-as**、**show ip bgp neighbors**、**show ip bgp peer-group**、**show ip bgp summary**

機能名	リリース	機能情報
BGP IPv6 ダイナミック ネイバー サポートと VRF サポート	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3 リリースでは、BGP ダイナミック ネイバーのサポートが、VRF のサポートを含む IPv6 BGP ピアリングに拡張されました。 この機能により、次のコマンドが導入または変更されました。**bgp listen**、**debug ip bgp range**、**neighbor remote-as**、**show bgp neighbors**、**show bgp summary**、 **show bgp vpnv6 unicast vrf neighbors**、 **show bgp vpnv6 unicast vrf peer-group** 、 **show bgp vpnv6 unicast vrf summary**



第 19 章

ネクストホップ アドレス トラッキングに対する BGP サポート

ネクストホップ アドレス トラッキングに対する BGP サポート機能は、サポート シスコ ソフトウェア イメージがインストールされている場合はデフォルトで有効になっています。BGP ネクストホップ アドレス トラッキングはイベント ドリブンです。BGP プレフィックスは、ピアリング セッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、RIB での更新時に BGP ルーティング プロセスに迅速に報告されます。この最適化によって、RIBにインストールされているルートのネクストホップの変更に対する応答時間が短縮されることで、全体的な BGP コンバージェンスが改善されます。BGP スキャナ サイクル間でのベスト パスの計算の実行時に、ネクストホップの変更だけがトラッキングおよび処理されます。

- 機能情報の確認 （479 ページ）
- ネクストホップアドレストラッキングに対するBGPサポートに関する情報 （480ページ）
- ネクストホップ アドレス トラッキングに対する BGP サポートの設定方法 （482 ページ）
- ネクストホップ アドレス トラッキングに対する BGP サポートの設定例 （493 ページ）
- その他の参考資料 （495 ページ）
- ネクストホップ アドレス トラッキングに対する BGP サポートの機能情報 （497 ページ）

機能情報の確認

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

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

ネクストホップ アドレス トラッキングに対する BGP サポートに関する情報

BGP ネクストホップ アドレス トラッキング

BGP ネクストホップ アドレス トラッキング機能は、サポート Cisco ソフトウェア イメージがインストールされている場合はデフォルトでイネーブルになっています。BGP ネクストホップ アドレス トラッキングはイベント ドリブンです。BGP プレフィックスは、ピアリング セッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、RIB での更新時に BGP ルーティング プロセスに迅速に報告されます。この最適化によって、RIB にインストールされているルートのネクストホップの変更に対する応答時間が短縮されることで、全体的な BGP コンバージェンスが改善されます。BGP スキャナ サイクル間でのベストパスの計算の実行時に、ネクストホップの変更だけがトラッキングおよび処理されます。

BGP ネクストホップ ダンプニングのペナルティ

ペナルティ値が 950 よりも高い場合は、ダンプニング計算を使用して、遅延が再利用時間として計算されます。ダンプニング計算では、次のパラメータが使用されます。

- ペナルティ
- ハーフライフ時間
- 再利用時間
- max-suppress-time

使用されるダンプニング パラメータの値は、max-suppress-time が 60 秒、half-life が 8 秒、reuse-limit が 100 です。

たとえば、最初にペナルティとして 1600 が追加された場合、ペナルティは、16 秒後に 800 になり、40 秒後に 100 になります。したがって、ルート更新のペナルティが 1600 の場合、BGP スキャナのスケジュールには 40 秒の遅延が使用されます。

これらのパラメータ（ペナルティしきい値およびすべてのダンプニング パラメータ）は変更できません。

BGP スキャナのデフォルトの動作

BGP は、インストールされているルートのネクスト ホップを監視して、ネクスト ホップの到達可能性を確認し、BGP ベスト パスを選択、インストール、および検証します。デフォルトでは、BGP スキャナを使用して、60 秒ごとにこの情報について RIB をポーリングします。スキャン サイクル間の 60 秒の期間中に、内部ゲートウェイ プロトコル（IGP）の不安定さ、ま

たはその他のネットワーク障害によってブラック ホールが生じ、一時的にルーティング ループが発生することがあります。

BGP Next_Hop 属性

Next_Hop 属性は、宛先への BGP ネクスト ホップとして使用されるネクスト ホップ IP アドレスを示します。デバイスは、再帰的ルックアップによってルーティング テーブルで BGP ネクスト ホップを検索します。外部 BGP（eBGP）では、ネクスト ホップはアップデートを送信したピアの IP アドレスです。内部 BGP（iBGP）は、内部で生成されたルートのプレフィックスをアドバタイズしたピアの IP アドレスを、ネクストホップのアドレスとして設定します。eBGP から学習した iBGP へのルートのいずれかがアドバタイズされた場合、Next_Hop 属性は変更されません。

デバイスが BGP ルートを使用するためには、BGP ネクストホップの IP アドレスが到達可能でなければなりません。到着可能性情報は通常 IGP によって提供され、IGP での変更はネットワーク バックボーンを介したネクストホップ アドレスの転送に影響を与える可能性があります。

選択的 BGP ネクストホップ ルート フィルタリング

BGP ネクストホップ アドレス トラッキングをサポートするために、選択的 BGP ネクストホップ ルート フィルタリングが、BGP の選択的アドレス トラッキング機能の一部として実装されていました。選択的ネクスト ホップ ルーティング フィルタリングは、BGP ネクスト ホップを解決するために、ルート マップを使用してルートを選択的に定義します。

bgp nexthop コマンドでルート マップを使用できることで、BGP Next_Hop 属性に適用されるプレフィックスの長さを設定できます。ルート マップは BGP ベスト パスの計算中に使用され、BGP プレフィックスのネクストホップ属性が記載されたルーティング テーブル内のルートに適用されます。ネクストホップ ルートがルート マップの評価に失敗した場合は、ネクストホップ ルートは到達不能とマークされます。このコマンドはアドレス ファミリ単位で実行されるため、異なるアドレス ファミリ内のネクストホップ ルートでは別のルート マップを適用できます。

（注） ASR シリーズ デバイスでルート マップを使用して、ネクスト ホップをルートの BGP ピアとして設定し、ピアに向かってアウトバウンド方向にそのルート マップを適用します。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

高速ピアリング セッションの非アクティブ化に対する BGP サポート

BGP ホールド タイマー

デフォルトでは、BGP ホールド タイマーは、シスコ ソフトウェアで 180 秒ごとに実行するように設定されます。このタイマー値は、デフォルトとして設定され、BGP ルーティング プロセスを別のルーティング プロトコルを持つピアリング セッションが原因になっている可能性がある不安定な状態から保護します。BGP デバイスは、通常、大きなルーティング テーブルを持っているため、頻繁にセッションをリセットすることは好ましくありません。

BGP の高速ピアリング セッションの非アクティブ化

BGP の高速ピアリング セッションを無効にすると、BGP コンバージェンスおよび BGP ネイバーの隣接変更に対する応答時間が向上します。この機能は、イベントによって引き起こされ、ネイバーごとに設定されます。この機能をイネーブルにすると、BGP は指定したネイバーでピアリングセッションをモニタします。隣接変更が検出され、終了したピアリングセッションがデフォルトのまたは設定した BGP スキャン間隔中に無効にされます。

BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング

Cisco IOS XE Release 2.1 以降のリリースでは、BGP の選択的アドレス トラッキング機能により、BGP の高速セッションの非アクティブ化とともにルートマップの使用が導入されました。**route-map** キーワードおよび *map-name* 引数は、**neighbor fall-over** BGP ネイバー セッション コマンドとともに使用され、BGP ピアへのルートが変更されたときに、この BGP ネイバーのあるピアリング セッションをリセットする必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、 deny 文が返された場合、ピア セッションがリセットされます。このルート マップはセッションの確立には使用されません。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

ネクストホップ アドレス トラッキングに対する BGP サポートの設定方法

BGP ネクストホップ アドレス トラッキングの設定

このセクションの作業は、BGP ネクストホップ アドレス トラッキングの設定方法を示しています。BGP ネクストホップ アドレス トラッキングによって、RIB でのネクストホップの変更に対する BGP の応答時間が大幅に改善されます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP ネイバーセッションが不安定になることがあります。BGP への

影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。ルート ダンプニングの設定の詳細については、「BGP ルート ダンプニングの設定」を参照してください。

BGP 選択的ネクストホップ ルート フィルタリングの設定

この作業は、潜在的なネクストホップ ルートをフィルタリングするためにルート マップを使用して選択的ネクストホップ ルート フィルタリングを設定する場合に実行します。この作業では、プレフィックス リストとルート マップを使用して、IP アドレスまたは送信元プロトコルのマッチングを行います。また、この作業を使用して、集約アドレスと BGP プレフィックスがネクストホップ ルートであると見なされないようにすることができます。**match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

bgp nexthop コマンドの使用方法のその他の例については、このモジュールの「例：BGP 選択的ネクストホップ ルート フィルタリングの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
5. **bgp nexthop route-map** *map-name*
6. **exit**
7. **exit**
8. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
9. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
10. **match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*]
11. **exit**
12. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
13. **end**
14. **show ip bgp** [*network*] [*network-mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**bgp nexthop route-map** *map-name* 例： `Device(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP`	BGP ネクスト ホップを解決するために、ルート マップがルートを選択的に定義できるようにします。 • この例では、CHECK-NEXTHOP という名前のルート マップが作成されます。
ステップ 6	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 7	**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 8	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]	BGP ネクストホップ ルート フィルタリングのプレフィックス リストを作成します。

	コマンドまたはアクション	目的
	例： `Device(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25`	• 選択的ネクストホップ ルート フィルタリングでは、アドレス ファミリ単位でのプレフィックス長のマッチングまたは送信元プロトコルのマッチングがサポートされます。 • この例では、マスク長が 25 を超える場合だけルートを許可する、FILTER25 という名前のプレフィックスリストを作成します。これによって、集約ルートがネクストホップ ルートであると見なされないようにします。
ステップ 9	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map CHECK-NEXTHOP deny 10`	ルート マップを設定し、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。 • この例では、CHECK-NEXTHOP という名前のルート マップが作成されます。次の **match** コマンドに IP アドレスの一致がある場合は、その IP アドレスは拒否されます。
ステップ 10	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] 例： `Device(config-route-map)# match ip address prefix-list FILTER25`	指定されたプレフィックス リスト内の IP アドレスのマッチングを行います。 • プレフィックスリストの名前を指定するには、*prefix-list-name* 引数を使用します。省略記号は、複数のプレフィックス リストを指定できることを意味します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 11	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了して、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 12	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map CHECK-NEXTHOP permit 20`	ルート マップを設定し、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。 • この例では、その他すべての IP アドレスがルート マップ CHECK-NEXTHOP によって許可されます。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show ip bgp** [*network*] [*network-mask*] 例： `Device# show ip bgp`	BGP ルーティング テーブル内のエントリを表示します。 • ルートごとのネクストホップ アドレスを表示するには、このコマンドを入力します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

show ip bgp コマンドの次の例は、ルートごとのネクストホップ アドレスを示しています。

```
BGP table version is 7, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.1.0/24      192.168.1.2              0             0 40000 i
*  10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
*> 172.17.1.0/24    0.0.0.0                  0         32768
```

BGP ネクストホップ アドレス トラッキングの遅延間隔の調整

この作業は、BGP ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を調整する場合に実行します。

すべてのルーティング テーブル ウォーク間の遅延間隔を調整して、内部ゲートウェイ プロトコル（IGP）の調整パラメータと一致させることで、この機能のパフォーマンスを向上させることができます。デフォルトの遅延間隔は 5 秒です。この値は、高速調整された IGP に最適です。よりゆっくり収束する IGP の場合は、IGP コンバージェンス時間に応じて遅延間隔を 20 秒以上に変更できます。

BGP ネクストホップ アドレス トラッキングによって、RIB でのネクストホップの変更に対する BGP の応答時間が大幅に改善されます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP ネイバー セッションが不安定になることがあります。BGP への影響

の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [[**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]]
5. **bgp nexthop trigger delay** *delay-timer*
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 64512`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4** [[**mdt**	**multicast**	**tunnel**	**unicast** [**vrf** *vrf-name*]	**vrf** *vrf-name*]	**vpnv4** [**unicast**]] 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**bgp nexthop trigger delay** *delay-timer* 例： `Device(config-router-af)# bgp nexthop trigger delay 20`	ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を設定します。 • この期間によって、通知の受信後に完全なルーティング テーブル ウォークを開始するまで BGP が待機する時間の長さが決まります。 • *delay-timer* 引数の値は、1 ～ 100 秒までの数値です。デフォルト値は 5 秒です。

	コマンドまたはアクション	目的
		• この例では、20 秒の遅延間隔を設定します。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP ネクストホップ アドレス トラッキングの無効化

この作業は、BGP ネクストホップアドレス トラッキングを無効にする場合に実行します。BGP ネクストホップ アドレス トラッキングは、IPv4 アドレス ファミリと VPNv4 アドレス ファミリではデフォルトで有効になっています。Cisco IOS Release 12.2(33)SB6 以降では、BGP ネクストホップ アドレス トラッキングは、VPNv6 アドレス ファミリでネクスト ホップが IPv6 ネクストホップ アドレスにマッピングされる IPv4 アドレスである場合は、デフォルトで有効になっています。

ネットワークに不安定な IGP ピアがあり、ルート ダンプニングを行っても安定性の問題が解決しない場合は、ネクスト ホップ アドレス トラッキングを無効にすると役立つことがあります。BGP ネクストホップ アドレス トラッキングを再度有効にするには、**trigger** キーワードと **enable** キーワードを指定して **bgp nexthop** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [[**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**] | **vpnv6** [**unicast**]]
5. **no bgp nexthop trigger enable**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 64512`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4** [[**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**] | **vpnv6** [**unicast**]] 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**no bgp nexthop trigger enable** 例： `Device(config-router-af)# no bgp nexthop trigger enable`	BGP ネクストホップ アドレス トラッキングを無効にします。 • ネクストホップアドレストラッキングは、IPv4 アドレス ファミリ セッションと VPNv4 アドレス ファミリ セッションではデフォルトで有効になっています。 • この例では、ネクストホップ アドレス トラッキングを無効にします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

高速セッションの非アクティブ化の設定

この項の作業は、BGP ネクストホップアドレストラッキングの設定方法を示しています。BGP ネクストホップアドレストラッキングによって、RIB でのネクストホップの変更に対する BGP の応答時間が大幅に改善されます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP ネイバー セッションが不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。ルートのダンプニングの詳細については、「内部 BGP 機能の設定」モジュールを参照してください。

BGP ネイバー の高速セッションの非アクティブ化の設定

BGP ネイバーを持つピアリング セッションを確立し、このピアリング セッションを高速セッションの非アクティブ化に設定して、このピアリングセッションが無効にされた場合のネットワーク コンバージェンス時間を向上するには、次の作業を実行します。

BGP ネイバーの高速セッションの非アクティブ化を有効にすると、BGP コンバージェンス時間が大幅に向上します。ただし、不安定な IGP ピアにより、引き続き BGP ネイバー セッションが不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **fall-over**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 10.0.0.1 remote-as 50000`	BGP ネイバーを持つピアリング セッションを確立します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **fall-over** 例： `Device(config-router-af)# neighbor 10.0.0.1 fall-over`	高速セッションを無効にするようにBGP ピアリングを設定します。 • BGP は、セッションが無効になると、このピアで学習したすべてのルートを削除します。
ステップ 7	**end** 例： `Device(config-router-af)# end`	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。

高速セッションの非アクティブ化の選択的アドレス トラッキングの設定

高速セッションの非アクティブ化の選択的アドレス トラッキングを設定するには、次の作業を実行します。**neighbor fall-over** コマンドのオプションの **route-map** キーワードおよび *map-name* 引数を使用して、BGP ピアへのルートが変更されたときに BGP ネイバーを持つピアリング セッションを非アクティブ化（リセット）する必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、deny 文が返された場合、ピア セッションがリセットされます。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **fall-over** [**route-map** *map-name*]
6. **exit**
7. **ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network / length* | **permit** *network / length*}[**ge** *ge-value*] [**le** *le-value*]
8. **route-map** *map-name* [**permit** | **deny**][*sequence-number*]
9. **match ip address prefix-list** *prefix-list-name* [*prefix-list-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	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **fall-over** [**route-map** *map-name*] 例： `Device(config-router)# neighbor 192.168.1.2 fall-over route-map CHECK-NBR`	BGP へのルートが変更されるときにルート マップを適用します。 • この例では、ネイバー 192.168.1.2 へのルートが変更されるときに、CHECK-NBR という名前のルート マップが適用されます。
ステップ 6	**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 7	**ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network / length* | **permit** *network / length*}[**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28`	BGP ネクストホップ ルート フィルタリングのプレフィックス リストを作成します。 • 選択的ネクストホップ ルート フィルタリングでは、アドレス ファミリ単位でのプレフィックス長のマッチングまたは送信元プロトコルのマッチングがサポートされます。 • この例では、マスク長が28以上の場合だけルートを許可する FILTER28 という名前のプレフィックス リストが作成されます。
ステップ 8	**route-map** *map-name* [**permit** | **deny**][*sequence-number*] 例：	ルート マップを設定し、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
	`Device(config)# route-map CHECK-NBR permit 10`	• この例では、CHECK-NBR という名前のルート マップが作成されます。次の **match** コマンドで IP アドレスの一致がある場合、その IP アドレスは許可されます。
ステップ 9	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] 例： `Device(config-route-map)# match ip address prefix-list FILTER28`	指定されたプレフィックス リスト内の IP アドレスのマッチングを行います。 • プレフィックスリストの名前を指定するには、*prefix-list-name* 引数を使用します。省略記号は、複数のプレフィックス リストを指定できることを意味します。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 10	**end** 例： `Device(config-route-map)# end`	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。

ネクストホップ アドレス トラッキングに対する BGP サポートの設定例

例：BGP ネクストホップ アドレス トラッキングの有効化と無効化

次の例では、ネクストホップ アドレス トラッキングは、IPv4 アドレス ファミリ セッションではディセーブルになっています。

```
router bgp 50000
 address-family ipv4 unicast
 no bgp nexthop trigger enable
```

例：BGP ネクストホップ アドレス トラッキングの遅延間隔の調整

次の例では、ネクストホップ トラッキングの遅延期間は、IPv4 アドレス ファミリ セッションでは 20 秒ごとに発生するよう設定されています。

```
router bgp 50000
 address-family ipv4 unicast
 bgp nexthop trigger delay 20
```

例：BGP 選択的ネクストホップ ルート フィルタリングの設定

次に、BGP プレフィックスがネクストホップ ルートとして使用されるのを回避するために、BGP 選択的ネクストホップ ルート フィルタリングを設定する例を示します。ネクスト ホップを対象とする最も固有性の高いルートが BGP ルートである場合は、BGP ルートは到達不能とマーキングされます。ネクスト ホップは IGP またはスタティック ルートでなければなりません。

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP
 exit
 exit
route-map CHECK-BGP deny 10
 match source-protocol bgp 1
 exit
route-map CHECK-BGP permit 20
 end
```

次に、BGP プレフィックスがネクストホップ ルートとして使用されるのを回避して、プレフィックスの固有性が /25 よりも高くなるようにするために、BGP 選択的ネクストホップ ルート フィルタリングを設定する例を示します。

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP25
 exit
 exit
ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25
route-map CHECK-BGP25 deny 10
 match ip address prefix-list FILTER25
 exit
route-map CHECK-BGP25 deny 20
 match source-protocol bgp 1
 exit
route-map CHECK-BGP25 permit 30
 end
```

例：BGP ネイバーの高速セッションの非アクティブ化の設定

次の例では、BGP ルーティング プロセスがデバイス A およびデバイス B で設定され、この 2 つのデバイス間でネイバー セッションの高速ピアリング セッションの非アクティブ化をモニタし、使用します。高速ピアリング セッションの非アクティブ化は、このネイバー セッションの両方のデバイスで必要ではありませんが、このネイバーセッションが非アクティブ化されている場合、両方の自律システムの BGP ネットワークのより高速なコンバージェンスに役立ちます。

デバイス A

```
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 fall-over
 end
```

デバイス B

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

例：高速セッションの非アクティブ化の選択的アドレストラッキングの設定

次に、/28 のプレフィックスを持つルートまたはピアの宛先へのさらに特定されたルートを使用できなくなった場合に、BGP ピアリング セッションをリセットするようにこのセッションを設定する方法の例を示します。

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

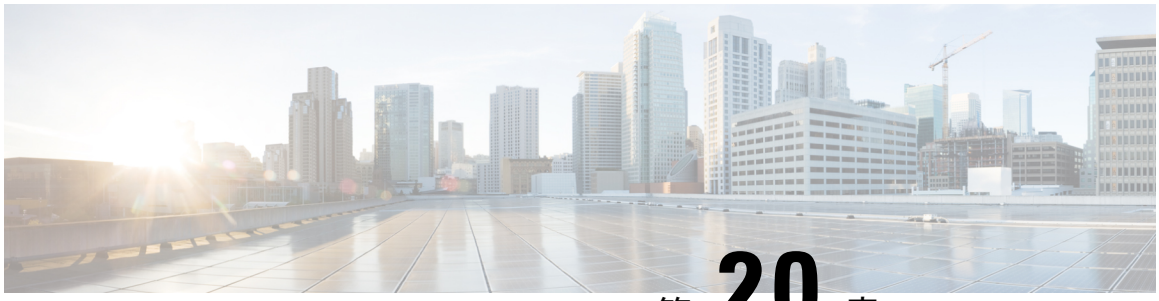
ネクストホップ アドレス トラッキングに対する BGP サポートの機能情報

表 *35 :* ネクストホップ アドレス トラッキングに対する *BGP* サポートの機能情報

機能名	リリース	機能情報
ネクストホップ アドレス トラッキングに対する BGP サポート		ネクストホップ アドレス トラッキングに対する BGP サポート機能は、サポート Cisco IOS ソフトウェア イメージがインストールされている場合はデフォルトでイネーブルになっています。BGP ネクストホップ アドレス トラッキングはイベント ドリブンです。BGP プレフィックスは、ピアリング セッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、RIB での更新時に BGP ルーティング プロセスに迅速に報告されます。この最適化によって、RIB にインストールされているルートのネクストホップの変更に対する応答時間が短縮されることで、全体的な BGP コンバージェンスが改善されます。BGP スキャナ サイクル間でのベスト パスの計算の実行時に、ネクストホップの変更だけがトラッキングおよび処理されます。 この機能により、**bgp nexthop** コマンドが導入されました。

機能名	リリース	機能情報
BGP の選択的アドレス トラッキング		BGP の選択的アドレス トラッキング機能によって、ネクストホップ ルート フィルタリングと高速なセッション非アクティブ化にルート マップが使用されるようになりました。選択的ネクスト ホップ フィルタリングは、ルート マップを使用して、BGP ネクスト ホップの解決に役立つルートを選択的に定義します。または、ルート マップを使用して、BGP ピアへのルートの変更時に BGP ネイバーとのピアリング セッションをリセットする必要があるかどうかを判別できます。 この機能により、次のコマンドが変更されました。**bgp nexthop**、**neighbor fall-over**

機能名	リリース	機能情報
高速ピアリング セッションの非アクティブ化に対する BGP サポート		高速ピアリング セッションの非アクティブ化に対する BGP サポート機能により、イベントによって起動される通知システムが導入され、ボーダーゲートウェイ プロトコル（BGP）プロセスでネイバーごとに BGP ピアリング セッションをモニタできるようになりました。この機能により、BGP が隣接変更を検出し、標準の BGP スキャン間隔中に終了したセッションを無効にできるようになり、BGP の隣接変更に対する応答時間が向上します。この機能をイネーブルにすると、BGP コンバージェンス全体が向上します。 この機能により、**neighbor fall-over** コマンドが変更されました。



第 20 章

最大プレフィックス制限到達後の BGP ネイバー セッション再起動

最大プレフィックス制限到達後の BGP セッション再起動機能により、**restart** キーワードが **neighbor maximum-prefix** コマンドに追加されます。これにより、ネットワーク オペレータは、ピアから受信したプレフィックス数が最大プレフィックス制限を超えたときに、ピアリング セッションをデバイスで再確立するまでの時間を設定できます。

- 機能情報の確認 （501 ページ）
- 最大プレフィックス制限到達後の BGP ネイバーセッション再起動に関する情報 （502 ページ）
- 最大プレフィックス制限を超えた後にネイバーセッションを再確立するためのデバイスの設定方法 （503 ページ）
- 最大プレフィックス制限到達後の BGP ネイバーセッション再起動の設定例 （507 ページ）
- 最大プレフィックス制限到達後の BGP ネイバーセッション再起動に関する追加情報 （508 ページ）
- 最大プレフィックス制限後の BGP ネイバー セッション再起動の機能情報 （509 ページ）

機能情報の確認

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

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

最大プレフィックス制限到達後のBGPネイバーセッション再起動に関する情報

プレフィックス制限および BGP ピアリング セッション

BGPを実行しているデバイスがピアから受信できるプレフィックスの最大数を制限するには、**neighbor maximum-prefix** コマンドを使用します。デバイスがピア デバイスから過剰のプレフィックスを受信し、最大プレフィックス制限を超えると、このピアリングセッションは無効になるか、ダウン状態になります。このセッションは、格納されているプレフィックスをクリアする **clear ip bgp** コマンドを入力することによってネットワーク オペレータが手動でアップ状態に戻すまで、ダウン状態のままです。

最大プレフィックス制限による BGP ネイバー セッションの再起動

restart キーワードが **neighbor maximum-prefix** コマンドに追加されたため、ネットワーク オペレータは、BGP ネイバー ピアリング セッションが無効またはダウン状態のときにこのピアリングセッションを自動的に再確立するようにデバイスを設定できます。ピアリングを自動的に再確立できるようになるまでの時間が設定可能です。**restart** キーワードの *restart-interval* を分単位で指定します。値の範囲は 1 ～ 65,535 分です。

BGP 中止通知のサブコード

ボーダー ゲートウェイ プロトコル（BGP）では、特定のアドレス ファミリのピアから受け取るプレフィックスの最大数に制限を設けています。この制限は、デバイスにとって、ローカルまたはリモート ネイバーのいずれかの設定ミスに起因する、リソースの枯渇に対する予防措置となります。アドバタイズメントによりピアが BGP をフラッディングしないようにするために、サポートされているアドレス ファミリごとに、1つのピアから受け入れるプレフィックスの数に対する制限が課されます。デフォルトの制限値は、該当するアドレス ファミリのピアに対して maximum-prefix limit コマンドを設定することにより、上書きできます。

BGP 中止通知メッセージでは、次のサブコードがサポートされています。

- 最大プレフィックス数到達
- 管理シャットダウン
- ピア設定解除
- 管理リセット

特定のアドレス ファミリのピアから受信したプレフィックスの数が、このアドレス ファミリに対する最大制限値（デフォルト設定またはユーザ設定のいずれかによる）を超えると、停止通知メッセージがそのネイバーに送信され、このネイバーとのピアリングが終了されます。特定のアドレス ファミリのネイバーとのピアリングが確立され、そのネイバーから一定数のプレ

フィックスをすでに受信した後で、そのネイバーのプレフィックスの最大数が設定されていることがあります。設定されたプレフィックスの最大数が、アドレスファミリのネイバーからすでに受信したプレフィックスの数よりも小さい場合は、設定直後に停止通知メッセージがそのネイバーに送信され、そのネイバーとのピアリングが終了されます。

最大プレフィックス制限を超えた後にネイバーセッションを再確立するためのデバイスの設定方法

最大プレフィックス制限到達後にネイバーセッションを再確立するためのルータの設定

BGP ピアから受信されたプレフィックス数が最大プレフィックス制限を超えたときに、デバイスによって BGP ネイバー セッションが再確立される時間間隔を設定するには、次の作業を実行します。

ネットワーク オペレータは、設定された最大プレフィックス制限を超えたためにダウン状態になったネイバー セッションを自動的に再確立するように、BGP を実行しているデバイスを設定できます。この機能がイネーブルのときには、ネットワーク オペレータの介入は必要ありません。

（注） この作業は、ディセーブルになった BGP ネイバー セッションをネットワーク オペレータが指定した時間間隔で再確立しようとします。ただし、再起動タイマーの設定だけでは、送信しているプレフィックス数が超過しているピアを変更または修正できません。ネットワーク オペレータは、最大プレフィックス制限を再設定するか、そのピアから送信されるプレフィックス数を減らす必要があります。プレフィックスを過剰に送信するように設定されたピアは、ネットワークに不安定な状態をもたらす可能性があり、過剰な数のプレフィックスが急速にアドバタイズおよび除去されます。この場合、ネットワーク オペレータは、原因となっている問題を修正する際に、**neighbor maximum-prefix** コマンドの **warning-only** キーワードを設定して再起動機能を無効にすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **peer-group** *peer-group-name*
6. **neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
7. **neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]

8. **neighbor** {*ip-address* | *ipv6-address***%** | } **maximum-prefix** *maximum* [*threshold*] [**restart** *minutes*] [**warning-only**]
9. **end**
10. **show ip bgp neighbors** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 101`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **peer-group** 例： `Device(config-router)# neighbor internal peer-group`	BGP ピア グループまたはマルチプロトコル BGP ピア グループを作成します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **peer-group** *peer-group-name* 例： `Device(config-router)# neighbor 10.4.9.5 peer-group internal`	ピア グループのメンバになるように BGP ネイバーを設定します。 • **%** キーワードは、IPv6 リンクローカル アドレス識別子です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] 例： `Device(config-router)# neighbor internal remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにピア グループを追加します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *ipv6-address***%** | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] 例： `Device(config-router)# neighbor 10.4.9.5 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address***%** | } **maximum-prefix** *maximum* [*threshold*] [**restart** *minutes*] [**warning-only**] 例： `Device(config-router)# neighbor 10.4.9.5 maximum-prefix 1000 90 restart 60`	BGP を実行しているルータの最大プレフィックス制限を設定します。 • **restart** キーワードおよび *minutes* 引数を使用して、最大プレフィックス制限を超えたために無効になったネイバー セッションを自動的に再確立するようにルータを設定します。*minutes* の設定可能範囲は 1 ～ 65535 分です。 • 過剰なプレフィックスを送信しているピアを調整できるように、**warning-only** キーワードを使用して、再起動機能が無効になるようデバイスを設定します。 （注） *minutes* 引数が設定されていないと、最大プレフィックス制限を超えた後も無効になったセッションはダウン状態のままになります。これはデフォルトの動作です。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp neighbors** *ip-address* 例： `Device# show ip bgp neighbors 10.4.9.5`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、指定したネイバーの最大プレフィックス制限および設定された再起動タイマー値を表示します。

例

show ip bgp neighbors コマンドの次の出力例により、無効になったネイバー セッションを自動的に再確立するようにデバイスが設定されたことを確認できます。この出力は、ネイバー 10.4.9.5 の最大プレフィックス制限が 1000 プレフィックス、再起動しきい値が 90%、再起動間隔が 60 分に設定されていることを示します。

```
Device# show ip bgp neighbors 10.4.9.5

BGP neighbor is 10.4.9.5,  remote AS 101, internal link
  BGP version 4, remote router ID 10.4.9.5
  BGP state = Established, up for 2w2d
  Last read 00:00:14, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:         23095      23095
    Route Refresh:          0          0
    Total:              23096      23096
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor versions 1/0 1/0
  Output queue sizes : 0 self, 0 replicated
  Index 2, Offset 0, Mask 0x4
  Member of update-group 2
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
!Configured maximum number of prefixes and restart interval information!
  Maximum prefixes allowed 1000
  Threshold for warning message 90%, restart interval 60 min
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.4.9.21, Local port: 179
Foreign host: 10.4.9.5, Foreign port: 11871
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x5296BD2C):
Timer          Starts    Wakeups            Next
Retrans         23098          0             0x0
TimeWait            0          0             0x0
AckHold         23096      22692             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1900546793  snduna: 1900985663  sndnxt: 1900985663     sndwnd:  14959
irs: 2894590641  rcvnxt: 2895029492  rcvwnd:      14978  delrcvwnd:   1406
SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 316 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
Datagrams (max data segment is 1460 bytes):
Rcvd: 46021 (out of order: 0), with data: 23096, total data bytes: 438850
```

```
Sent: 46095 (retransmit: 0, fastretransmit: 0), with data: 23097, total data by9
```

トラブルシューティングのヒント

BGP ソフト再構成を使用して BGP 接続をリセットするには、**clear ip bgp** コマンドを使用します。このコマンドは、格納されたプレフィックスをクリアして、BGP を実行しているデバイスが最大プレフィックス制限を超えないようにするために使用できます。

次のエラー メッセージの表示は、ネイバー セッションがディセーブルになる根本的な問題を示す可能性があります。**neighbor maximum-prefix** コマンドに対して設定された値および過剰な数のプレフィックスを送信しているすべてのピアの設定を確認する必要があります。次のエラー メッセージ例は、表示される可能性のあるエラー メッセージと類似しています。

```
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Up
00:01:14:%BGP-4-MAXPFX:No. of unicast prefix received from 10.10.10.2 reaches 5, max 6
00:01:14:%BGP-3-MAXPFXEXCEED:No.of unicast prefix received from 10.10.10.2:7 exceed
limit6
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Down - BGP Notification sent
00:01:14:%BGP-3-NOTIFICATION:sent to neighbor 10.10.10.2 3/1 (update malformed) 0 byte
```

bgp dampening コマンドを使用して、ピアが過剰な数のプレフィックスを送信し、ネットワークに不安定な状態をもたらすときにフラッピング ルートまたはインターフェイスのダンプニングを設定できます。過剰な数のプレフィックスを送信しているデバイスをトラブルシューティングまたは調整する場合にだけこのコマンドを使用します。BGP ルート ダンプニングの詳細については、「BGP の拡張機能の設定」モジュールを参照してください。

最大プレフィックス制限到達後のBGPネイバーセッション再起動の設定例

例：最大プレフィックス制限到達後にネイバーセッションを再確立するためのルータの設定

次の例では、ネイバー 192.168.6.6 で許可されるプレフィックスの最大数が 2000 に設定され、ピアリング セッションが無効になった場合に、30 分後にそのピアリング セッションを再確立するようにデバイスが設定されます。

```
Device(config)# router bgp 101
Device(config-router)# neighbor internal peer-group
Device(config-router)# neighbor 10.4.9.5 peer-group internal
Device(config-router)# neighbor internal remote-as 100
Device(config-router)# neighbor 10.4.9.5 remote-as 100
Device(config-router)# neighbor 10.4.9.5 maximum-prefix 2000 90 restart 30
Device(config-router)# end
```

最大プレフィックス制限到達後のBGPネイバーセッション再起動に関する追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 4486	『*Subcodes for BGP Cease Notification Message*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

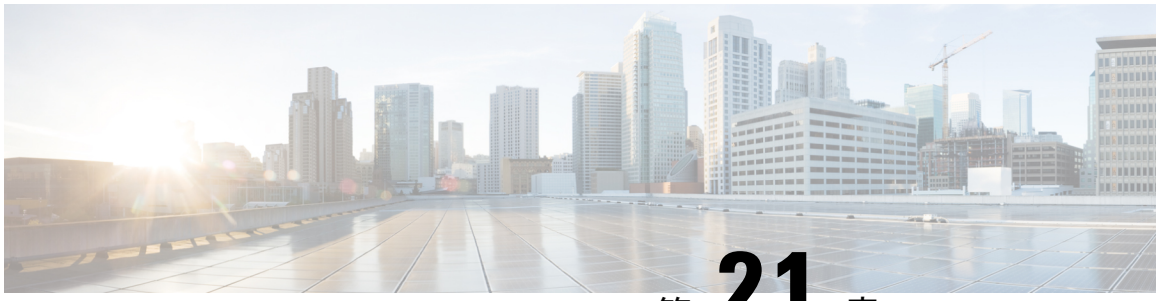
最大プレフィックス制限後のBGPネイバーセッション再起動の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *36* : 最大プレフィックス制限後の *BGP* セッション再起動の機能情報

機能名	リリース	機能情報
最大プレフィックス制限後の BGP 再起動セッション		最大プレフィックス制限到達後の BGP セッション再起動機能により、**restart** キーワードが **neighbor maximum-prefix** コマンドに追加されます。これにより、ネットワーク オペレータは、ピアから受信したプレフィックス数が最大プレフィックス制限を超えたときに、ピアリング セッションをデバイスで再確立するまでの時間を設定できます。 次のコマンドが変更されました。**neighbor maximum-prefix**、**show ip bgp neighbors**
BGP - BGP 中止通知のサブコード		BGP 中止通知のサブコードに対するサポートが追加されました。



第 21 章

ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポート

ネットワーク AS 移行のためのデュアル AS 設定に対する BGP サポート機能により、自律システム パスのカスタマイズ設定オプションが追加され、BGP Local-AS 機能が拡張されました。この機能の設定は、お客様のピアリングセッションに対して透過的で、お客様のピアリング環境を中断せずにプロバイダーが 2 つの自律システムを結合することを可能にします。お客様のピアリングセッションは、その後メンテナンス時間中またはその他のスケジュール済みのダウンタイム中に更新できます。

- 機能情報の確認 （511 ページ）
- ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートに関する情報 （512 ページ）
- ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの設定方法 （514 ページ）
- ネットワーク移行のためのデュアル AS ピアリングの設定例 （516 ページ）
- その他の参考資料 （518 ページ）
- ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの機能情報 （518 ページ）

機能情報の確認

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

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

ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートに関する情報

BGP ネットワークの自律システムの移行

自律システムの移行は、テレコミュニケーションまたはインターネットサービスプロバイダーが別のネットワークを購入したときに必要になる場合があります。お客様の既存のピアリング環境を中断せずにプロバイダーが2番目の自律システムを統合できることが望ましいです。お客様のネットワークで必要な設定の量によっては、サービスを中断せずに完了するのが困難な、煩雑な作業となります。

BGP ネットワーク自律システムの移行に対するデュアル自律システムのサポート

Cisco IOS Release 12.0(29)S、12.3(14)T、12.2(33)SXH、およびこれら以降のリリースでは、デュアル BGP 自律システム設定のサポートが追加され、お客様のピアリング セッションを中断せずにセカンダリ自律システムをプライマリ自律システムの下に結合できます。この機能の設定は、お客様のネットワークに対して透過的です。デュアル BGP 自律システム設定により、自律システムの移行中にルータをセカンダリ自律システムのメンバとして外部ピアに対して表示できます。この機能により、ネットワーク オペレータは、複数の自律システムを結合でき、その後、通常のサービス時間に既存のピアリング環境を中断せずにお客様を新しい設定に移行できます。

neighbor local-as コマンドを使用して、eBGP ネイバーから受信するルートの自律システム番号を追加および削除して、AS_PATH 属性がカスタマイズされます。この機能により、自律システム番号を移行するために、外部ピアに対して別の自律システムのメンバとしてルータを表示できます。この機能は、ネットワーク オペレータがセカンダリ自律システムをプライマリ自律システムに結合し、その後、通常のサービス時間中に既存のピアリング環境を中断せずにお客様の設定をアップデートすることにより、BGP ネットワークでの自律システム番号の変更プロセスを簡略化します。

コンフェデレーション、個別のピアリング セッション、およびピア グループに対する BGP 自律システムの移行サポート

この機能は、コンフェデレーション、個別のピアリング セッション、およびピア グループとピア テンプレートによって適用される設定をサポートします。この機能がグループ ピアに適用されると、個別ピアはカスタマイズできません。

BGP 自律システムの移行中のフィルタリングの入力

自律システム パスのカスタマイズにより、このようなカスタマイズが誤って設定されている場合に、ルーティング ループが作成される可能性が高くなります。お客様のピアリング数が増加

するにつれ危険が高まります。入力インターフェイスに関するポリシーを適用して、遷移中または **local-as** 設定のないルートの自律システム番号をブロックすることにより、この可能性を低減できます。

注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。この機能は、自律システムの移行のためだけに設定する必要があり、遷移が完了した後設定解除する必要があります。不適切に設定するとルーティング ループが作成される可能性があるため、この手順は、経験を積んだネットワーク オペレータだけが行ってください。

BGP ネットワークの 4 バイト自律システム番号への移行

4 バイト ASN に対する BGP サポート機能により、4 バイト自律システム番号がサポートされるようになりました。自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 バイト自律システム番号の割り当てを開始しました。

Cisco の 4 バイト自律システム番号の実装は、RFC 4893 をサポートします。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。新しい予約済み（プライベート）自律システム番号（23456）はRFC 4893 により作成された番号で、Cisco IOS CLI ではこの番号を自律システム番号として設定できません。

ご使用の BGP ネットワークを 4 バイト自律システム番号に移行するには計画が必要です。4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

スムーズな移行を確実に行うには、4 バイト自律システム番号を使用して識別される自律システム内の BGP スピーカーをすべて、4 バイト自律システム番号をサポートするようにアップグレードすることを推奨します。

BGP ネットワークを 4 バイトの自律システムのフル サポートにアップグレードする手順の詳細については、『Migration Guide for Explaining 4-Byte Autonomous System』ホワイト ペーパーを参照してください。

ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの設定方法

ネットワーク移行のためのデュアル AS ピアリングの設定

自律システム番号を移行するために、別の自律システムのメンバとして外部ピアに対してBGP ピア ルータを表示するように設定するには、次の作業を実行します。BGP ピアにデュアル自律システム番号が設定されると、ネットワーク オペレータは、セカンダリ自律システムをプライマリ自律システムに結合し、今後のサービス時間中に既存のピアリング環境を中断せずにお客様の設定をアップデートできます。

show ip bgp コマンドおよび **show ip bgp neighbors** コマンドを使用して、ルーティング テーブルのエントリ用の自律システム番号およびこの機能の状況を確認できます。

（注）

- ネットワーク AS 移行のためのデュアル AS 設定に対する BGP サポートは、正しい eBGP ピアリング セッションだけに設定できます。この機能は、コンフェデレーションの異なるサブ自律システム内の 2 つのピアには設定できません。
- ネットワーク AS 移行のためのデュアル AS 設定に対する BGP サポートは、ピア グループとピア テンプレートによって適用される個別のピアリング セッションおよび設定に設定できます。このコマンドがピア グループに適用されると、ピアは個別にカスタマイズできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]
6. **neighbor** *ip-address* **remove-private-as**
7. **end**
8. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter-prefixes** *mask-length*]
9. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 40000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.0.0.1 remote-as 45000`	BGP ネイバーを持つピアリング セッションを確立します。
ステップ 5	**neighbor** *ip-address* **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]] 例： `Router(config-router)# neighbor 10.0.0.1 local-as 50000 no-prepend replace-as dual-as`	eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズします。 • **replace-as** キーワードを使用して、（*ip-address* 引数で設定される）ローカル自律システム番号だけを AS_PATH 属性の前に付加します。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。 • **dual-as** キーワードを使用し、（ローカル BGP ルーティング プロセスからの）実際の自律システム番号を使用するか、*ip-address* 引数（local-as）で設定された自律システム番号を使用して、ピアリング セッションを確立するように eBGP ネイバーを設定します。 • この例では、実際の自律システム番号および local-as 番号を受け入れるように 10.0.0.1 ネイバーを持つピアリング セッションが設定されます。
ステップ 6	**neighbor** *ip-address* **remove-private-as** 例：	（任意）プライベート自律システム番号をアウトバウンド ルーティング アップデートから削除します。

	コマンドまたはアクション	目的
	`Router(config-router)# neighbor 10.0.0.1 remove-private-as`	• このコマンドを **replace-as** 機能とともに使用して、プライベート自律システム番号を削除し、この番号を外部自律システム番号に置き換えることができます。 • このコマンドが設定されると、プライベート自律システム番号（64512～65535）は、AS_PATH 属性から自動的に削除されます。
ステップ 7	**end** 例： `Router(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。
ステップ 8	**show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter-prefixes** *mask-length*] 例： `Router# show ip bgp`	BGP ルーティング テーブル内のエントリを表示します。 • この出力を使用して、実際の自律システム番号または local-as 番号が設定されているかどうかを確認できます。
ステップ 9	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*] 例： `Router# show ip bgp neighbors`	ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この出力は、**local AS**、**no-prepend**、**replace-as**、および **dual-as** を対応する自律システム番号とともに表示します（これらのオプションが設定されている場合）。

ネットワーク移行のためのデュアル AS ピアリングの設定例

例：デュアル AS の設定

次に、この機能を使用して、お客様のネットワークのピアリング環境を中断せずに2つの自律システムを結合する方法の例を示します。**neighbor local-as** コマンドを設定して、ルータ 1 で自律システム 40000 と自律システム 45000 を使用してピアリング セッションを維持できるようにします。ルータ 2 は、BGP ルーティング プロセスを自律システム 50000 で実行するお客様のルータで、自律システム 45000 を持つピアに対して設定されます。

自律システム 40000（プロバイダーのネットワーク）のルータ 1

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 40000
 no synchronization
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
 neighbor 10.3.3.33 local-as 45000 no-prepend replace-as dual-as
```

自律システム 45000（プロバイダーのネットワーク）のルータ 1

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 45000
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
```

自律システム 50000（お客様のネットワーク）のルータ 2

```
interface Serial3/0
 ip address 10.3.3.33 255.255.255.0
!
router bgp 50000
 bgp router-id 10.0.0.3
 neighbor 10.3.3.11 remote-as 45000
```

遷移完了後、通常のメンテナンス時間中またはその他のスケジュール済みのダウンタイム中にルータ 50000 の設定を自律システム 40000 を持つピアに対してアップデートできます。

```
 neighbor 10.3.3.11 remote-as 100
```

例：デュアル AS コンフェデレーションの設定

次の例は、「例：デュアル AS の設定」の例にあるルータ 1 の設定の代わりに使用できます。これらの設定の唯一の相違は、ルータ 1 がコンフェデレーションの一部になるように設定されていることです。

```
interface Serial3/0/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 65534
 no synchronization
 bgp confederation identifier 100
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
 neighbor 10.3.3.33 local-as 45000 no-prepend replace-as dual-as
```

例：ルーティング アップデートでの AS の置換

次の例では、プライベート自律システム 64512 を 10.3.3.33 ネイバーに対するアウトバウンド ルーティング アップデートから取り除き、これを自律システム 50000 に置き換えます。

```
router bgp 64512
 neighbor 10.3.3.33 local-as 50000 no-prepend replace-as
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

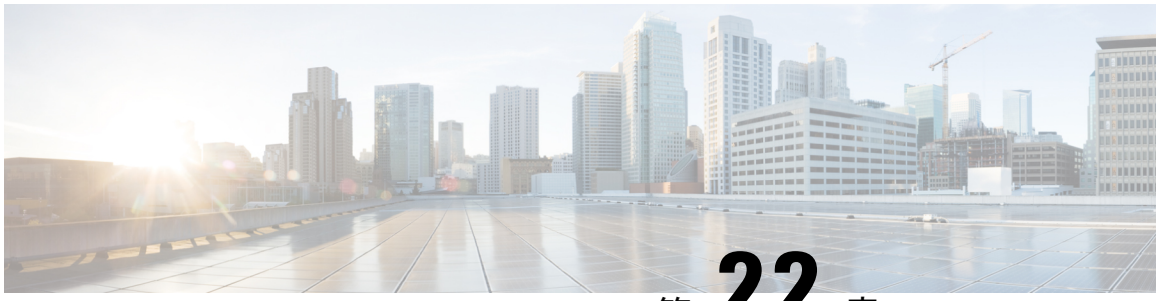
ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *37*：ネットワーク *AS* 移行のためのデュアル *AS* 構成に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポート		ネットワーク AS 移行のためのデュアル AS 設定に対する BGP サポート機能により、自律システム パスのカスタマイズ設定オプションが追加され、BGP Local-AS 機能が拡張されました。この機能の設定は、お客様のピアリング セッションに対して透過的で、お客様のピアリング環境を中断せずにプロバイダーが 2 つの自律システムを結合することを可能にします。お客様のピアリング セッションは、その後メンテナンス時間中またはその他のスケジュール済みのダウンタイム中に更新できます。 この機能により、**neighbor local-as** コマンドが変更されました。



第 22 章

内部 BGP 機能の設定

このモジュールでは、内部ボーダー ゲートウェイ プロトコル（BGP）機能を設定する手順について説明します。内部 BGP（iBGP）とは、単一の自律システム内部にあるネットワーキング デバイスで実行中の BGP のことです。BGP は、独自のルーティング ポリシーを持つ異なるルーティング ドメイン（自律システム）間に、ループのないルーティングを行うように設計されたドメイン間ルーティング プロトコルです。現在は大規模な内部ネットワークを持つ会社が多く、ネットワークの効率を維持したまま、トラフィック需要の増加に合わせて既存の内部ルーティング プロトコルをスケーリングするには課題が山積しています。

- 機能情報の確認 （521 ページ）
- 内部 BGP 機能に関する情報 （522 ページ）
- 内部 BGP 機能の設定法 （528 ページ）
- 内部 BGP 機能の設定例 （542 ページ）
- 内部 BGP 機能に関する追加情報 （545 ページ）
- 内部 BGP 機能設定用の機能情報 （547 ページ）

機能情報の確認

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

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

内部 BGP 機能に関する情報

BGP ルーティング ドメイン コンフェデレーション

内部 BGP（iBGP）メッシュを削減する方法の 1 つとして、ある自律システムを複数の副自律システムに分割し、単一のコンフェデレーションにグループ化することがあげられます。外部からは、このコンフェデレーションは単一の自律システムであるかのように見えます。各自律システムは内部で完全にメッシュ化されていて、同じコンフェデレーション内の他の自律システムとの間には数本の接続があります。他の自律システムのピアに外部BGP（eBGP）セッションがある場合でも、iBGP ピアであるかのようにルーティング情報を交換します。特に、ネクスト ホップ、Multi Exit Discriminator（MED）属性、およびローカル プリファレンス情報は保持されます。この機能により、自律システムすべてに対して単一の内部ゲートウェイ プロトコル（IGP）を保持することができます。

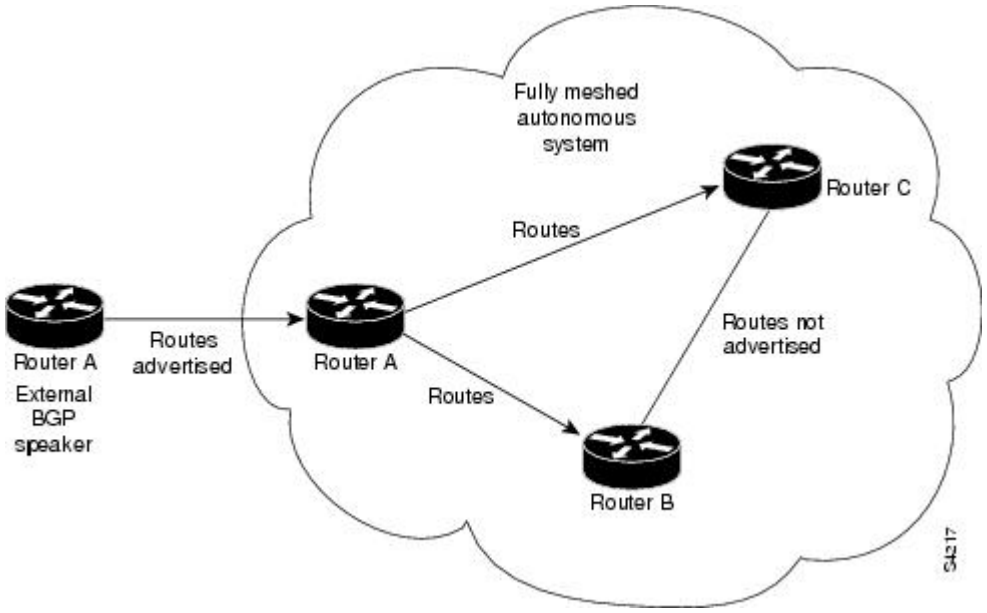
BGP コンフェデレーションを設定するには、コンフェデレーション ID を指定する必要があります。自律システムのグループは、外部からはコンフェデレーション ID を自律システム番号として持つ単一の自律システムのように見えます。

BGP ルート リフレクタ

BGP を使用するには、すべての iBGP スピーカーが完全メッシュ化されている必要があります。ただし、iBGP スピーカーの数が多い場合、この要件には適切な拡張性がありません。コンフェデレーションを設定せずに iBGP メッシュを減らす別の方法として、ルート リフレクタの設定があります。

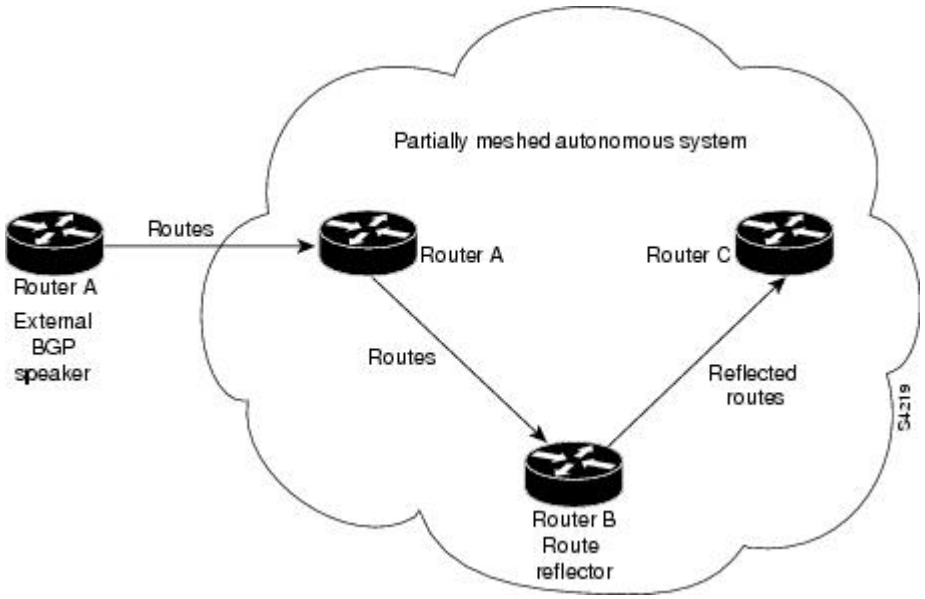
下の図に、3 つの iBGP スピーカー（ルータ A、B、C）で構成された単純な iBGP 設定を示します。ルート リフレクタがない場合、ルータ A は外部ネイバーからルートを受け取ると、そのルートをルータ B と C の両方にアドバタイズする必要があります。ルータ B と C は iBGP が学習したルートを他の iBGP スピーカーに再アドバタイズしません。これは、これらのルータが内部ネイバーから他の内部ネイバーに学習したルートを渡さないことで、ルーティング情報のループを防ぐためです。

図 *38* : 完全メッシュ化された *3* つの *iBGP* スピーカー



ルート リフレクタがある場合は、学習したルートをネイバーに渡す方法があるため、すべての iBGP スピーカーを完全にメッシュ化する必要はありません。このモデルでは、iBGP が学習したルートを一連の iBGP ネイバーに渡す役割を持つルート リフレクタとして、1 つの iBGP ピアを設定しています。下の図では、ルータ B がルート リフレクタとして設定されています。ルータ A からアドバタイズされたルートをルート リフレクタが受信すると、ルータ C にアドバタイズします。逆の場合も同じです。このスキームにより、ルータ A とルータ C 間の iBGP セッションは不要になります。

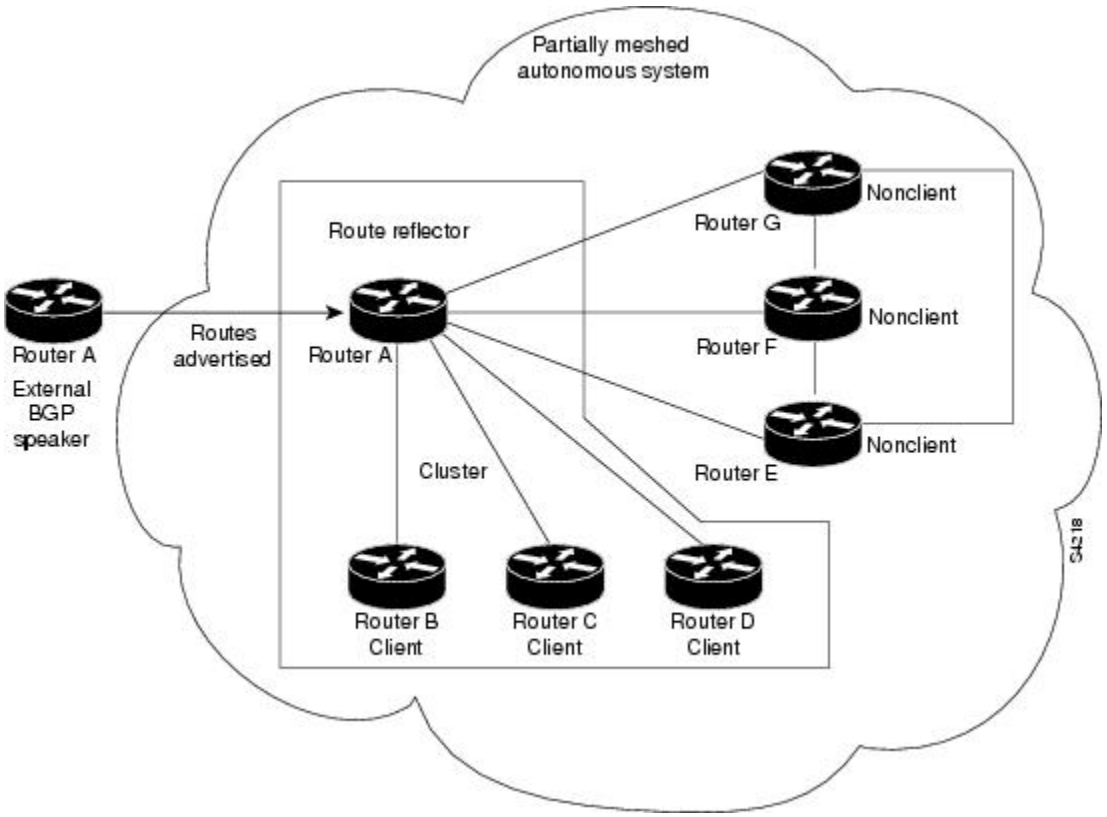
図 *39* : ルート リフレクタのある単純な *BGP* モデル



ルート リフレクタの内部ピアは、次の 2 種類のグループに分けられます。クライアントのピア、および自律システム（非クライアント ピア）の他のルータすべてです。ルート リフレクタは、これらの2つのグループ間でルートを反映させます。ルートリフレクタおよびそのクライアント ピアは、クラスタを形成します。非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、クラスタ外の iBGP スピーカーとは通信しません。

下の図に、より複雑なルート リフレクタのスキームを示します。ルータ A は、ルータ B、C、および D があるクラスタ内のルート リフレクタです。ルータ E、F、および G は完全にメッシュ化された非クライアント ルータです。

図 *40 :* より複雑な *BGP* ルート リフレクタのモデル



ルートリフレクタがアドバタイズされたルートを受信すると、ネイバーに応じて、次のようなアクションを取ります。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

ルート リフレクタ対応の BGP スピーカーとともに、ルート リフレクタの概念に対応していない BGP スピーカーを併用することもできます。これらは、クライアントまたは非クライアント グループのメンバとなることが可能で、旧 BGP モデルからルート リフレクタ モデルへ、簡単に順次移行することができます。たとえば、最初に、ルートリフレクタおよびいくつかのクライアントを持つ単一のクラスタを作成します。他のすべての iBGP スピーカーはルート リフレクタに対して非クライアント ピアとすることができ、クラスタを作成して徐々に追加していくことができます。

自律システムは複数のルート リフレクタを持つことができます。ルート リフレクタは、他のルートリフレクタを他の iBGP スピーカーと同様に扱います。ルートリフレクタは、他のルート リフレクタをクライアント グループまたは非クライアント グループに含むように設定できます。単純な設定では、バックボーンを多数のクラスタに分割してもかまいません。各ルートリフレクタは、非クライアント ピアとして他のルート リフレクタとともに設定されます（このため、すべてのルートリフレクタは完全メッシュ化されます）。クライアントは、所属するクラスタのルート リフレクタとだけ、iBGP セッションを維持するように設定されます。

通常、クライアントのクラスタには、1 つのルート リフレクタがあります。その場合、クラスタはルート リフレクタのルータ ID で識別されます。冗長性を向上させ、シングル ポイント障害を避けるために、クラスタは複数のルートリフレクタを含むことがあります。この場合、クラスタ内のすべてのルート リフレクタに 4 バイトのクラスタ ID を設定し、ルート リフレクタが同一クラスタ内のルートリフレクタからのアップデートを識別できるようにする必要があります。クラスタの役割を果たすルートリフレクタはすべて完全メッシュ化され、同一のクライアントおよび非クライアント ピアのセットを持っている必要があります。

ルーティング ループを回避するルート リフレクタのメカニズム

iBGP が学習したルートが反映されるため、ルーティング情報がループする場合があります。ルート リフレクタ モデルには、ルーティングのループを防ぐ、次のようなメカニズムがあります。

- 送信元 ID は、任意で非推移的な BGP 属性です。これは 4 バイトの属性で、ルート リフレクタにより作成されます。この属性は、ローカル自律システムのルートの送信元のルータ ID を保持します。したがって、設定ミスによりルーティング情報が送信元に戻ってくる場合、その情報は無視されます。
- クラスタ リストは任意で非推移的な BGP 属性です。これは、ルートが渡したクラスタ ID のシーケンスです。ルート リフレクタがクライアントから非クライアント ピアへのルート、およびその逆を反映するとき、ローカル クラスタ ID をクラスタ リストにアペンドします。クラスタ リストが空の場合は、新規のクラスタ リストが作成されます。ルート リフレクタでは、この属性を使用して、設定ミスによりルーティング情報が同じクラスタにループ バックしているかどうかを識別できます。クラスタ リストにローカル クラスタ ID が見つかった場合、そのアドバタイズメントは無視されます。
- アウトバウンド ルート マップで **set** 句を使用すると、属性を変更できるだけでなく、場合によってはルーティング ループが発生することもあります。この動作を回避する目的で、アウトバウンド ルート マップのほとんどの **set** 句は、iBGP ピアに反映されるルートとしては無視されます。処理されたアウトバウンド ルート マップの唯一の **set** 句が **set ip next-hop** 句です。

iBGP ピアに対する IP ネクスト ホップを設定するルート リフレクタの BGP アウトバウンド ルート マップ

IP ネクストホップを設定するルートリフレクタの BGP アウトバウンドルートマップ機能は、反映されたルートのネクスト ホップ属性をルート リフレクタが変更できるようにします。

アウトバウンド ルート マップで **set** 句を使用すると、属性を変更できるだけでなく、場合によってはルーティングループが発生することもあります。この動作を回避する目的で、アウトバウンド ルート マップのほとんどの **set** 句は、iBGP ピアに反映されるルートとしては無視されます。ルート リフレクタ（RR）の処理されるアウトバウンド ルート マップの唯一の **set** 句が **set ip next-hop** 句です。**set ip next-hop** 句は反映されるルートに適用されます。

アウトバウンドルートマップを持つRRを設定すると、ネットワーク管理者が反映されたルートのネクスト ホップ属性を変更できます。**set ip next-hop** 句でルート マップを設定すると、管理者は転送パスに RR を配置し、ロード バランシングを実行するために iBGP マルチパス ロード シェアリングを設定できます。つまり、RR は複数の出力ポイント間の発信パケットを配信できます。「iBGP マルチパス ロード シェアリングの設定」モジュールを参照してください。

⚠

注意 反映されたルートの BGP 属性を誤って設定すると、不整合ルーティング、ルーティング ループ、または接続の切断が発生することがあります。反映されるルートの BGP 属性の設定は、設計上の問題を十分理解しているユーザだけが行うようにする必要があります。

BGP ルート ダンプニング

ルート ダンプニングは、インターネットワーク間でフラッピング ルートの伝搬を最小限に抑えるように設計された BGP 機能です。ルートは、その可用性が繰り返し切り替わる場合にフラッピングすると見なされます。

たとえば、自律システム 1、自律システム 2、および自律システム 3 の 3 つの BGP 自律システムがあるネットワークについて考えます。自律システム 1 のネットワーク A へのルートがフラッピングする（利用できなくなる）と仮定します。ルート ダンプニングがない状況では、自律システム 1 から自律システム 2 への eBGP ネイバーは、取り消しメッセージを自律システム 2 に送信します。次に自律システム 2 内の境界ルータは、取り消しメッセージを自律システム 3 に伝播します。ネットワーク A へのルートが再出現したとき、自律システム 1 は自律システム 2 に、自律システム 2 は自律システム 3 にアドバタイズメント メッセージを送信します。ネットワーク A へのルートが利用可能になったり不可になったりを繰り返す場合、取り消しメッセージおよびアドバタイズメント メッセージが多数送信されます。これは、インターネットに接続されたインターネットワークで問題となります。インターネットのバックボーンでルートのフラッピングが生じると、通常、多くのルートに影響を与えるからです。

（注） ルート ダンプニングがイネーブルになっている場合、BGP ピア リセットにペナルティは適用されません。リセットするとそのルートは取り消されますが、ルート フラップ ダンプニングがイネーブルの場合でも、このインスタンスにペナルティは課されません。

ルート ダンプニングによるルート フラッピングの最小化

ルートダンプニング機能は、次のようにしてフラッピングの問題を最小限に抑えます。ここでも、ネットワーク A へのルートがフラッピングしたと仮定します。（ルート ダンプニングがイネーブルになっている）自律システム 2 内のルータは、ネットワーク A にペナルティ 1000 を割り当てて、履歴状態に移行させます。自律システム2内のルータは、引き続きネイバーにルートのステータスをアドバタイズします。ペナルティは累積されます。ルートフラップが非常に頻繁に発生し、ペナルティが設定可能な抑制制限を超える場合は、フラップの発生回数に関係なく、ルータはネットワーク A へのルートのアドバタイズを停止します。このようにして、ルート ダンプニングが発生します。

ネットワークAに課されたペナルティは再使用制限に達するまで減衰し、達すると同時にそのルートは再びアドバタイズされます。再使用制限の半分の時点で、ネットワークAへのルートのダンプニング情報が削除されます。

BGP ルート ダンプニングの用語

ルート ダンプニングについて説明する際には、次の用語が使用されます。

- フラップ：可用性が繰り返し切り替わるルート。
- 履歴状態：一度ルートフラップが発生した後で、そのルートにはペナルティが割り当てられ、履歴状態になります。これは、ルータに履歴情報に基づいたベストパスがないことを意味します。
- ペナルティ：ルート フラップが発生するたびに、別の自律システム内でルート ダンプニングについて設定されているルータは、ルートにペナルティ 1000 を割り当てます。ペナルティは累積します。そのルートのペナルティは、抑制限度を超えるまで BGP ルーティング テーブルに保存されます。抑制限度を超えると、ルート ステートは履歴からダンプに変更されます。
- ダンプ ステート：この状態では、ルート フラップが非常に頻繁に発生したため、ルータはこのルートを BGP ネイバーにアドバタイズしなくなります。
- 抑制限度：ペナルティがこの制限を超えるとルートは抑制されます。デフォルト値は2000です。
- 半減期：ルートにペナルティが割り当てられると、半減期期間（デフォルトでは 15 分）後にペナルティは半減されます。ペナルティを小さくするプロセスは5秒ごとに発生します。
- 再使用制限：フラッピング ルートのペナルティが減少し、この再使用制限を下回ると、ルートの抑制は解除されます。つまり、ルートは再びBGPテーブルに追加され、フォワー

ディングに再び使用されます。デフォルトの再使用制限は 750 です。ルートの抑制中止プロセスは、10 秒経過ごとに発生します。10 秒ごとに、ルータは、現在抑制が解除されているルートを検索して、アドバタイズします。

- 最大抑制制限：この値は、ルートを抑制できる最大時間です。デフォルト値は半減期の 4 倍です。

iBGP から取得した、自律システムの外部にあるルートはダンプニングされません。このポリシーによって、iBGP ピアが自律システムの外部にあるルートに高いペナルティを設定できなくなります。

BGP ルート マップ ネクスト ホップ セルフ

BGP ルート マップ ネクスト ホップ セルフ機能は、bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定を選択的にオーバーライドする方法を提供します。これらの設定はアドレス ファミリに対してグローバルに適用されます。ルートによっては、これは適切でない場合があります。たとえば、スタティック ルートは、自身をネクスト ホップとして再配布する必要がある一方で、接続されたルート、および内部ボーダーゲートウェイ プロトコル（IBGP）または外部ボーダーゲートウェイ プロトコル（EBGP）を介して学習されたルートは、引き続きネクスト ホップを変更せずに再配布する場合があります。

BGP ルート マップ ネクスト ホップ セルフ機能は、bgp next-hop unchanged 設定と bgp next-hop unchanged allpaths 設定をオーバーライドする新しい ip next-hop self 設定を構成できるように、既存のルート マップ インフラストラクチャを変更します。

ip next-hop self 設定は、VPNv4 および VPNv6 アドレス ファミリにのみ適用されます。BGP 以外のプロトコルによって配布されるルートは影響を受けません。

新しい bgp route-map priority 設定を使用すると、bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定よりもルート マップが優先されることを BGP に通知できます。bgp route-map priority 設定は、BGP にのみ影響します。bgp next-hop unchanged または bgp next-hop unchanged allpaths 設定を構成していない場合、bgp route-map priority 設定は効果がありません。

内部 BGP 機能の設定法

ルーティング ドメイン コンフェデレーションの設定

BGP コンフェデレーションを設定するには、コンフェデレーション ID を指定する必要があります。自律システムのグループは、外部からはコンフェデレーション ID を自律システム番号として持つ単一の自律システムのように見えます。BGP 連合 ID を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-router)# bgp confederation identifier as-number`	BGP コンフェデレーションを設定します。

コンフェデレーション内の他の自律システムから特別な eBGP としてネイバーを処理するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-router)# bgp confederation peers as-number [as-number]`	コンフェデレーションに属する自律システムを指定します。

iBGP メッシュを削減する他の方法については、「ルート リフレクタの設定 （529 ページ）」を参照してください。

ルート リフレクタの設定

ルート リフレクタおよびそのクライアントを設定するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-router)# neighbor {ip-address | peer-group-name} route-reflector-client`	ローカル ルータを BGP ルート リフレクタとして、指定されたネイバーをクライアントとして、それぞれ設定します。

クラスタが複数のルート リフレクタを持つ場合は、次のコマンドをルータ コンフィギュレーション モードで使用して、クラスタ ID を設定します。

コマンド	目的
`Router(config-router)# bgp cluster-id cluster-id`	クラスタ ID の設定

show ip bgp コマンドを使用して、送信元 ID およびクラスタリスト属性を表示します。

デフォルトでは、ルート リフレクタのクライアントは完全メッシュ化されている必要はなく、クライアントからのルートは他のクライアントに反映されます。ただし、クライアントが完全メッシュ化されている場合は、ルート リフレクタはルートをクライアントに反映する必要はありません。

クライアントからクライアントへのルートの反映を無効にするには、**no bgp client-to-client reflection** 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。

コマンド	目的
`Router(config-router)# no bgp client-to-client reflection`	クライアントからクライアントへのルート リフレクションをディセーブルにします。

iBGP ピアのネクスト ホップを設定するルート マップを使用するルート リフレクタの設定

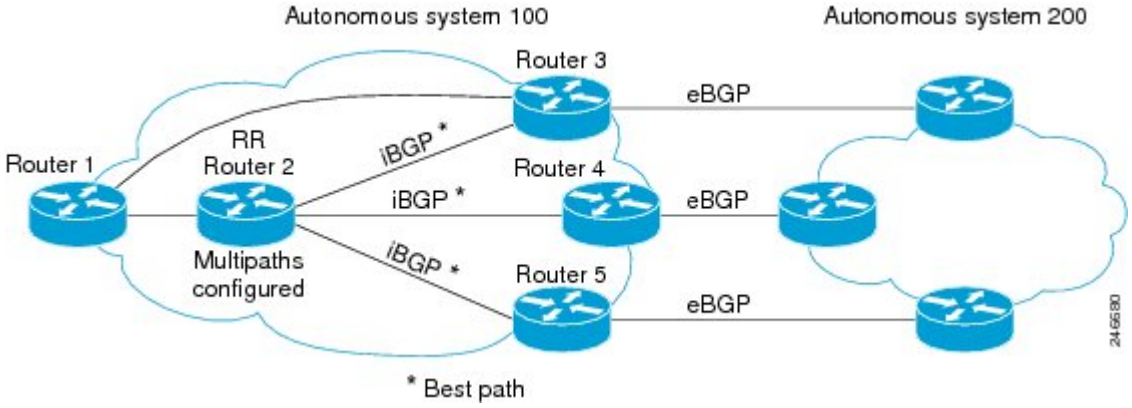
iBGP ピアのネクスト ホップを設定する RR で次の手順を実行します。次の手順を実行する理由の 1 つに挙げられるのが、iBGP のロード シェアリングを設定できるように RR をルートのネクスト ホップにする場合です。RR クライアントにアドバタイズされる、RR のアドレスになるネクスト ホップを設定するルート マップを作成します。ルート マップは、ルート マップが適用されるルータからのアウトバウンド ルートだけに適用されます。

注意 反映されたルートの BGP 属性を誤って設定すると、不整合ルーティング、ルーティング ループ、または接続の切断が発生することがあります。反映されるルートの BGP 属性の設定は、設計上の問題を十分理解しているユーザだけが行うようにする必要があります。

（注） **neighbor next-hop-self** コマンドを使用して RR のネクスト ホップ属性を変更しないでください。RR で **neighbor next-hop-self** コマンドを使用すると、RR クライアントから反映されている意図したルートではなく、非反映ルートについてだけネクスト ホップ属性が変更されます。ルートを反映するときにネクスト ホップ属性を変更するには、アウトバウンド ルート マップを使用します。

ここでは、下の図に示すシナリオのRR（ルータ 2）を設定します。この場合、ルータ 1 はルートのネクスト ホップが設定された iBGP ピアです。ルート マップが存在しない場合、ルータ 1 からのアウトバウンド ルートは、ネクスト ホップ ルータ 3 に進みます。代わりに、RR のアドレスにネクスト ホップを設定すると、ルータ 1 からのルートが RR に送られ、RR は、ルータ 3、4、および 5 間のロード バランシングを実行できます。

図 *41 : iBGP* ピアのネクスト ホップを設定するルート マップを使用するルート リフレクタ



手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag*
4. **set ip next-hop** *ip-address*
5. **exit**
6. **router bgp** *as-number*
7. **address-family ipv4**
8. **maximum-paths ibgp** *number*
9. **neighbor** *ip-address* **remote-as** *as-number*
10. **neighbor** *ip-address* **activate**
11. **neighbor** *ip-address* **route-reflector-client**
12. **neighbor** *ip-address* **route-map** *map-name* **out**
13. その他の RR クライアントごとにステップ 12 ～ 14 を繰り返します。
14. **end**
15. **show ip bgp neighbors**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**route-map** *map-tag* 例： `Router(config)# route-map rr-out`	ルート マップ コンフィギュレーション モードを開始して、ルート マップを設定します。 • ルート マップはルート リフレクタ クライアントのネクストホップを設定するために作成されます。
ステップ 4	**set ip next-hop** *ip-address* 例： `Router(config-route-map)# set ip next-hop 10.2.0.1`	このルート マップが適用される、アドバタイズされるルートに対して、ネクスト ホップ属性をこの IPv4 アドレスに設定することを指定します。 • この作業では、RR のアドレスになるようにネクスト ホップを設定します。
ステップ 5	**exit** 例： `Router(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、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**router bgp** *as-number* 例： `Router(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 7	**address-family ipv4** 例： `Router(config-router-af)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 8	**maximum-paths ibgp** *number* 例： `Router(config-router)# maximum-paths ibgp 5`	ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。
ステップ 9	**neighbor** *ip-address* **remote-as** *as-number* 例： `Router(config-router-af)# neighbor 10.1.0.1 remote-as 100`	エントリを BGP ネイバー テーブルに追加します。
ステップ 10	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 10.1.0.1 activate`	ピアとの情報交換をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**neighbor** *ip-address* **route-reflector-client** 例： `Router(config-router-af)# neighbor 10.1.0.1 route-reflector-client`	ローカル ルータを BGP ルート リフレクタに設定し、指定されたネイバーをルート リフレクタ クライアントに設定します。
ステップ 12	**neighbor** *ip-address* **route-map** *map-name* **out** 例： `Router(config-router-af)# neighbor 10.1.0.1 route-map rr-out out`	このネイバーから発信ルートにルート マップを適用します。 • ステップ 3 で作成したルート マップを参照してください。
ステップ 13	その他の RR クライアントごとにステップ 12 ～ 14 を繰り返します。	その他の RR クライアントにはルート マップを適用しません。
ステップ 14	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show ip bgp neighbors** 例： `Router# show ip bgp neighbors`	（任意）RR クライアントとしてのステータスを含む BGP ネイバーに関する情報、および設定されたルート マップに関する情報を表示します。

BGP タイマーの調整

BGP は、ある種のタイマーを使用して、キープアライブ メッセージの送信や、キープアライブ メッセージを受信しなくなってからの間隔（この期間を経過すると、シスコ ソフトウェアがピアのデッドを宣言する）などの周期的なアクティビティを制御しています。デフォルトでは、キープアライブ タイマーは 60 秒で、ホールドタイム タイマーは 180 秒です。これらのタイマーは調整できます。接続が開始されたとき、BGP はホールドタイムをネイバーとネゴシエーションします。2 つのホールドタイムのうちの小さい方が選択されます。次に、ネゴシエーションされたホールドタイムおよび設定されたキープアライブ時間をもとにキープアライブ タイマーが設定されます。

すべてのネイバーに対して BGP タイマーを調整するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Device(config-router)# timers bgp keepalive holdtime`	すべてのネイバーに対して BGP タイマーを調整します。

BGP のキープアライブ タイマーおよびホールドタイム タイマーを特定のネイバー用に調整するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Device(config-router)# neighbor [ip-address | peer-group-name] timers keepalive holdtime`	指定されたピアまたはピア グループに対し、キープアライブまたはホールドタイム タイマー（秒単位）を設定します。

（注） 特定のネイバーまたはピア グループに対して設定されたタイマーは、**timers bgp** ルータ コンフィギュレーション コマンドを使用してすべての BGP ネイバーに対して設定されたタイマーをオーバーライドします。

BGP ネイバーまたはピア グループのタイマーをクリアするには、**neighbor timers** コマンドの **no** 形式を使用します。

削除された MED を最も条件の悪いパスと見なすようにルータを設定

削除されたMED属性を持つパスを最も条件の悪いパスと見なすようにルータを設定するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-router)# bgp bestpath med missing-as-worst`	削除された MED は無限大の値を持つと見なし、MED 値を持たないそのパスを最も条件の悪いパスとするようにルータを設定します。

MEDが副自律システムパスからパスを選択すると見なすようにルータを設定

パスを選択する際に MED 値を考慮するようにルータを設定するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-router)# bgp bestpath med confed`	コンフェデレーション内の複数の副自律システムによりアドバタイズされた中からパスを選択する際に MED を考慮するようにルータを設定します。

MED 間での比較が行われるのは、パスに外部自律システムがない場合に限ります（外部自律システムとは、コンフェデレーションの内部にない自律システムのことです）。パスに外部自律システムがある場合、外部 MED は透過的にコンフェデレーションを通過し、比較は行われません。

次の例では、ルート A をこれらのパスと比較します。

```
path= 65000 65004, med=2
path= 65001 65004, med=3
path= 65002 65004, med=4
path= 65003 1, med=1
```

このケースでは、**bgp bestpath med confed router configuration** コマンドが有効の場合、パス 1 が選択されます。4 番目のパスの方が MED の値が低いですが、このパスには外部自律システムがあるため、MED を比較する対象にはなりません。

コンフェデレーションのパスの選択にMEDを使用するようにルータを設定

コンフェデレーション内の単一の副自律システムによりアドバタイズされたパスの中から最良のパスを選択するために MED を使用するようルータを設定するには、次のコマンドをルータ コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-router)# bgp deterministic med`	同一自律システムの異なるピアによりアドバタイズされたルートから選択する際、MED 変数を比較するようにルータを設定します。

（注） **bgp always-compare-med** ルータ コンフィギュレーション コマンドが有効な場合は、すべてのパスは完全に比較可能で、**bgp deterministic med** コマンドが有効になっている場合でも、コンフェデレーションの他の自律システムからのパスも比較対象です。

BGP ルート ダンプニングのイネーブル化と設定

この作業は、BGP ルート ダンプニングをイネーブルにして設定する場合に実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** as-*number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **bgp dampening** [*half-life reuse suppress max-suppress-time*] [**route-map** *map-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** as-*number* 例： `Router(config)# router bgp 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーションモードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**bgp dampening** [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*] 例： `Router(config-router-af)# bgp dampening 30 1500 10000 120`	BGP ルート ダンプニングをイネーブルにして、ルート ダンプニング係数のデフォルト値を変更します。 • *half-life*、*reuse*、*suppress*、および *max-suppress-time* 引数は、すべて位置に依存します。引数を 1 つ入力する場合は、すべての引数を入力する必要があります。 • BGP ルート ダンプニングを有効にする場所を制御するには、**route-map** キーワードと *map-name* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP ルート ダンプニングのモニタリングおよびメンテナンス

フラッピングしているすべてのパスのフラップをモニタできます。ルートの抑制が解除され、少なくとも 1 半減期の間安定すれば、統計情報は削除されます。フラップの統計情報を表示するには、次のコマンドを必要に応じて使用します。

コマンド	目的
`Router# show ip bgp dampening flap-statistics`	すべてのパスの BGP フラップ統計情報を表示します。
`Router# show ip bgp dampening flap-statistics regexp` *regexp*	正規表現に一致するすべてのパスの BGP フラップ統計情報を表示します。
`Router# show ip bgp dampening flap-statistics filter-list access-` *list*	フィルタを通過したすべてのパスの BGP フラップ統計情報を表示します。
`Router# show ip bgp dampening flap-statistics` *ip-address mask*	単一エントリの BGP フラップ統計情報を表示します。
`Router# show ip bgp dampening flap-statistics` *ip-address mask* **longer-prefix**	さらに限定したエントリの BGP フラップ統計情報を表示します。

BGP フラップ統計情報をクリアする（したがってルートがダンプニングされる可能性を減少させる）には、次のコマンドを必要に応じて使用します。

コマンド	目的
`Router# clear ip bgp flap-statistics`	すべてのルートの BGP フラップ統計情報をクリアします。
`Router# clear ip bgp flap-statistics regexp` *regexp*	正規表現に一致するすべてのパスの BGP フラップ統計情報をクリアします。

コマンド	目的
`Router# clear ip bgp flap-statistics filter-list list`	フィルタを通過したすべてのパスのBGPフラップ統計情報をクリアします。
`Router# clear ip bgp flap-statistics ip-address mask`	単一エントリのBGPフラップ統計情報をクリアします。
`Router# clear ip bgp ip-address flap-statistics`	ネイバーからのすべてのパスのBGPフラップ統計情報をクリアします。

（注） BGPピアがリセットされたときも、ルートのフラップ統計情報はクリアされます。リセットするとそのルートは取り消されますが、ルートフラップダンプニングがイネーブルの場合でも、このインスタンスにペナルティは課されません。

ルートがダンプニングされると、ダンプニングされたルートが抑制解除されるまでの時間を含むBGPルートダンプニング情報が表示されます。情報を表示するには、次のコマンドを使用します。

コマンド	目的
`Router# show ip bgp dampening dampened-paths`	抑制が解除されるまでの時間を含む、ダンプニングされたルートを表示します。

次のコマンドを使用して、BGPダンプニング情報をクリアし、抑制されたルートを抑制解除することができます。

コマンド	目的
`Router# clear ip bgp dampened-paths [ip-address network-mask]`	ルートダンプニング情報をクリアし、抑制されたルートを抑制解除します。

BGP ルート マップの next-hop self の設定

ip next-hop self 設定を追加し、bgp next-hop unchanged 設定と bgp next-hop unchanged allpaths 設定をオーバーライドして、既存のルートマップを変更するには、この作業を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **route-map** *map-tag* **permit** *sequence-number*
4. **match source-protocol** *source-protocol*
5. **set ip next-hop self**
6. **exit**
7. **route-map** *map-tag* **permit** *sequence-number*
8. **match route-type internal**
9. **match route-type external**
10. **match source-protocol** *source-protocol*
11. **exit**
12. **router bgp** *autonomous-system-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **address-family vpnv4**
15. **neighbor** *ip-address* **activate**
16. **neighbor** *ip-address* **next-hop unchanged allpaths**
17. **neighbor** *ip-address* **route-map** *map-name* **out**
18. **exit**
19. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
20. **bgp route-map priority**
21. **redistribute** *protocol*
22. **redistribute** *protocol*
23. **exit-address-family**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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** *sequence-number* 例： `Device(config)# route-map static-nexthop-rewrite 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 4	**match source-protocol** *source-protocol* 例： `Device(config-route-map)# match source-protocol static`	送信元プロトコルに基づいて、Enhanced Interior Gateway Routing Protocol（EIGRP）の外部ルートを照合します。
ステップ 5	**set ip next-hop self** 例： `Device(config-route-map)# set ip next-hop self`	自身をネクスト ホップとするようにローカル ルート（BGP の場合のみ）を設定します。
ステップ 6	**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、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 7	**route-map** *map-tag* **permit** *sequence-number* 例： `Device(config)# route-map static-nexthop-rewrite permit 20`	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 8	**match route-type internal** 例： `Device(config-route-map)# match route-type internal`	指定されたタイプのルートを再配布します。
ステップ 9	**match route-type external** 例： `Device(config-route-map)# match route-type external`	指定されたタイプのルートを再配布します。
ステップ 10	**match source-protocol** *source-protocol* 例： `Device(config-route-map)# match source-protocol connected`	送信元プロトコルに基づいて、Enhanced Interior Gateway Routing Protocol（EIGRP）の外部ルートを照合します。
ステップ 11	**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、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 12	**router bgp** *autonomous-system-number* 例：	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 45000`	
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 172.16.232.50 remote-as 65001`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 14	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	VPNv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 172.16.232.50 activate`	ボーダーゲートウェイプロトコル（BGP）ネイバーとの情報交換を有効にします。
ステップ 16	**neighbor** *ip-address* **next-hop unchanged allpaths** 例： `Device(config-router-af)# neighbor 172.16.232.50 next-hop unchanged allpaths`	マルチホップとして設定されている外部 EBGP ピアで、ネクスト ホップを変更せずに伝播できるようにします。
ステップ 17	**neighbor** *ip-address* **route-map** *map-name* **out** 例： `Device(config-router-af)# neighbor 172.16.232.50 route-map static-nexthop-rewrite out`	発信ルートにルート マップを適用します。
ステップ 18	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 19	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast vrf inside`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 20	**bgp route-map priority** 例： `Device(config-router-af)# bgp route-map priority`	ローカル BGP ルーティング プロセスについてルート マップを優先することを設定します。

	コマンドまたはアクション	目的
ステップ 21	**redistribute** *protocol* 例： `Device(config-router-af)# redistribute static`	ルートを1つのルーティング ドメインから他のルーティング ドメインに再配布します。
ステップ 22	**redistribute** *protocol* 例： `Device(config-router-af)# redistribute connected`	ルートを1つのルーティング ドメインから他のルーティング ドメインに再配布します。
ステップ 23	**exit-address-family** 例： `Device(config-router-af)# exit address-family`	アドレス ファミリ コンフィギュレーション モードを終了し、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 24	**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。

内部 BGP 機能の設定例

例：ルート マップのある BGP コンフェデレーション設定

ここでは、BGP コミュニティおよびルート マップを含む BGP コンフェデレーション設定の使用例を説明します。BGP コンフェデレーションを設定する方法のその他の例については、この章の「例：BGP コンフェデレーション」の項を参照してください。

この例では、BGP コンフェデレーション設定でルートをフィルタするために BGP コミュニティ属性がどのように使用されるかを説明します。

この例では、*set-community* という名前のルート マップがネイバー 172.16.232.50 へのアウトバウンドのアップデートに適用され、local-as コミュニティ属性がそのルートをフィルタ処理するために使用されます。アクセス リスト 1 を渡すルートは、local-as という特別なコミュニティ属性値を持っています。残りのルートは通常どおりアドバタイズされます。この特別なコミュニティ値は、自律システム 200 内の BGP スピーカーがそれらのルートのアドバタイズメントを行うのを自動的に防止します。

```
router bgp 65000
 network 10.0.1.0 route-map set-community
 bgp confederation identifier 200
 bgp confederation peers 65001
 neighbor 172.16.232.50 remote-as 100
 neighbor 172.16.233.2 remote-as 65001
!
```

```
route-map set-community permit 10
 match ip address 1
 set community local-as
!
```

例：BGP コンフェデレーション

次に、コンフェデレーションのいくつかのピアを表示する設定の例を示します。このコンフェデレーションは、自律システム番号 6001、6002、および 6003 の 3 つの内部自律システムから構成されています。コンフェデレーション外の BGP スピーカーには、このコンフェデレーションは（**bgp confederation identifier** ルータ コンフィギュレーション コマンドを通じて指定される）自律システム番号 500 を持つ通常の自律システムのように見えます。

自律システム 6001 の BGP スピーカーで、**bgp confederation peers** ルータ コンフィギュレーション コマンドは、自律システム 6002 および 6003 からのピアを特別な eBGP ピアとしてマークします。したがって、ピア 172.16.232.55 および 172.16.232.56 は、ローカル プリファレンス、ネクスト ホップ、および未変更の MED をこのアップデートで取得します。10.16.69.1 のルータは通常の eBGP スピーカーで、このピアから受け取る更新は、自律システム 6001 のピアからの通常の eBGP 更新とまったく同じです。

```
router bgp 6001
 bgp confederation identifier 500
 bgp confederation peers 6002 6003
 neighbor 172.16.232.55 remote-as 6002
 neighbor 172.16.232.56 remote-as 6003
 neighbor 10.16.69.1 remote-as 777
```

自律システム 6002 の BGP スピーカーでは、自律システム 6001 および 6003 からのピアは特別な eBGP ピアとして設定されます。10.70.70.1 は通常の iBGP ピアであり、10.99.99.2 は自律システム 700 からの通常の eBGP ピアです。

```
router bgp 6002
 bgp confederation identifier 500
 bgp confederation peers 6001 6003
 neighbor 10.70.70.1 remote-as 6002
 neighbor 172.16.232.57 remote-as 6001
 neighbor 172.16.232.56 remote-as 6003
 neighbor 10.99.99.2 remote-as 700
```

自律システム 6003 の BGP スピーカーでは、自律システム 6001 および 6002 からのピアは特別な eBGP ピアとして設定されます。10.200.200.200 は、自律システム 701 からの通常の eBGP ピアです。

```
router bgp 6003
 bgp confederation identifier 500
 bgp confederation peers 6001 6002
 neighbor 172.16.232.57 remote-as 6001
 neighbor 172.16.232.55 remote-as 6002
 neighbor 10.200.200.200 remote-as 701
```

次に、同じ例の自律システム 701 からの BGP スピーカー 10.200.200.205 からの設定の一部を示します。ネイバー 172.16.232.56 は、自律システム 500 からの 通常の eBGP スピーカーとして

設定されます。コンフェデレーション外部のピアは、この自律システムが複数の自律システムに内部分割されることを認識しません。

```
router bgp 701
 neighbor 172.16.232.56 remote-as 500
 neighbor 10.200.200.205 remote-as 701
```

例：iBGP ピアのネクスト ホップを設定するルート マップを使用するルート リフレクタ

次の例は、上の図に基づいています。ルータ2は、クライアント（ルータ1、3、4、および5）のルート リフレクタですルータ 1 はルータ 3 に接続されますが、ルータ 3 をネクスト ホップとして使用する（つまり、ルータ 3 との直接リンクを使用する）ためにルータ 1 が AS 200 宛てのトラフィックを転送しないようにします。ルータ 3、4、および 5 の間でロード シェアリングを実行できる RR にトラフィックを送信します。

次に、RR（ルータ 2）を設定する例を示します。rr-out という名前のルート マップが、ルータ 1 に適用されます。ルート マップは、ネクスト ホップが 10.2.0.1 の RR になるように設定します。ネクスト ホップが RR アドレスであることをルータ 1 が確認すると、ルータ 1 は RR にルートを転送します。RR はパケットを受信すると、自動的に iBGP パス間でロード シェアリングを実行します。最大 5 個の iBGP パスが許可されます。

ルータ 2

```
route-map rr-out
 set ip next-hop 10.2.0.1
!
interface gigabitethernet 0/0
 ip address 10.2.0.1 255.255.0.0
router bgp 100
 address-family ipv4 unicast
 maximum-paths ibgp 5
 neighbor 10.1.0.1 remote-as 100
 neighbor 10.1.0.1 activate
 neighbor 10.1.0.1 route-reflector-client
 neighbor 10.1.0.1 route-map rr-out out
!
 neighbor 10.3.0.1 remote-as 100
 neighbor 10.3.0.1 activate
 neighbor 10.3.0.1 route-reflector-client
!
 neighbor 10.4.0.1 remote-as 100
 neighbor 10.4.0.1 activate
 neighbor 10.4.0.1 route-reflector-client
!
 neighbor 10.5.0.1 remote-as 100
 neighbor 10.5.0.1 activate
 neighbor 10.5.0.1 route-reflector-client
end
```

例：BGP ルート マップの next-hop self の設定

この項では、BGP ルート マップの next-hop self を設定する方法の例を示します。

この例では、bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定をオーバーライドするネットワークを照合するルート マップを設定します。次に、next-hop self を設定します。その後、指定したアドレス ファミリに対して bgp route-map priority を設定して、指定済みのルート マップが bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定よりも優先されるようにします。この設定により、スタティック ルートは自身をネクスト ホップとして再配布されますが、接続されたルートおよび IBGP または EBGP を介して学習されたルートは引き続きネクスト ホップを変更せずに再配布されます。

```
route-map static-nexthop-rewrite permit 10
 match source-protocol static
 set ip next-hop self
route-map static-nexthop-rewrite permit 20
 match route-type internal
 match route-type external
 match source-protocol connected
!
router bgp 65000
 neighbor 172.16.232.50 remote-as 65001
 address-family vpnv4
   neighbor 172.16.232.50 activate
   neighbor 172.16.232.50 next-hop unchanged allpaths
   neighbor 172.16.232.50 route-map static-nexthop-rewrite out
 exit-address-family
 address-family ipv4 unicast vrf inside
   bgp route-map priority
   redistribute static
   redistribute connected
 exit-address-family
end
```

内部 BGP 機能に関する追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概要	「Cisco BGP 概要」モジュール
基本的な BGP 設定作業	「基本 BGP ネットワークの設定」モジュール
iBGP のマルチパス ロード シェアリング	「iBGP マルチパス ロード シェアリング」モジュール

関連項目	マニュアル タイトル
サービス プロバイダーへの接続	「外部 BGP を使用したサービス プロバイダーとの接続」モジュール
複数の IP ルーティング プロトコルに適用する機能の設定	『*IP Routing: Protocol-Independent Configuration Guide*』

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4893	『*BGP Support for Four-octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

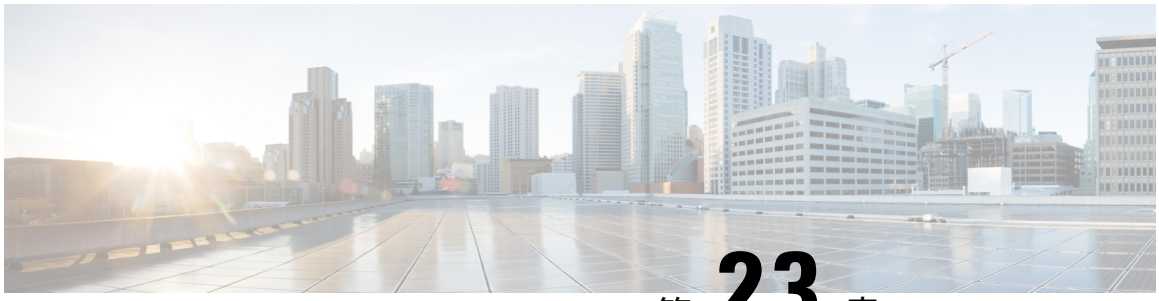
内部 BGP 機能設定用の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *38 :* 内部 *BGP* 機能設定用の機能情報

機能名	リリース	機能の設定情報
内部 BGP 機能の設定	10.3 12.0(7)T 12.0(32)S12 12.2(33)SRA 12.2(33)SXH	このモジュールのすべての機能はレガシー機能と見なされ、すべてのトレインのリリースイメージで動作します。 次のコマンドはこれらの機能により追加または変更されました。 • **bgp always-compare-med** • **bgp bestpath med confed** • **bgp bestpath med missing-as-worst** • **bgp client-to-client reflection** • **bgp cluster-id** • **bgp confederation identifier** • **bgp confederation peers** • **bgp dampening** • **bgp deterministic med** • **clear ip bgp dampening** • **clear ip bgp flap-statistics** • **neighbor route-reflector-client** • **neighbor timers** • **show ip bgp** • **show ip bgp dampening dampened-paths** • **show ip bgp dampening flap-statistics** • **timers bgp**
IP ネクスト ホップを設定するルート リフレクタの BGP アウトバウンド ルート マップ	12.0(16)ST 12.0(22)S 12.2 12.2(14)S 15.0(1)S	IP ネクスト ホップを設定するルート リフレクタの BGP アウトバウンド ルート マップ機能は、反映されたルートのネクスト ホップ属性をルート リフレクタが変更できるようにします。



第 23 章

ルート リフレクタでの BGP VPLS 自動検出のサポート

BGP ルート リフレクタが拡張され、ルート リフレクタで VPLS を明示的に設定しなくても BGP VPLS プレフィックスを反映できるようになりました。

- 機能情報の確認 （549 ページ）
- ルート リフレクタでの BGP VPLS 自動検出のサポートの概要 （550 ページ）
- ルート リフレクタでの BGP VPLS 自動検出のサポートの設定例 （550 ページ）
- その他の参考資料 （551 ページ）
- ルート リフレクタでの BGP VPLS 自動検出のサポートに関する機能情報 （552 ページ）

機能情報の確認

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

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

ルート リフレクタでの BGP VPLS 自動検出のサポートの概要

ルート リフレクタでの BGP VPLS オートディスカバリのサポート

Cisco IOS Release 12.2(33)SRE で、ルート リフレクタでの BGP VPLS オートディスカバリのサポートが導入されました。Cisco 7600 および Cisco 7200 シリーズのルータで、BGP ルート リフレクタが拡張され、ルート リフレクタで VPLS を明示的に設定しなくても BGP VPLS プレフィックスを反映できるようになりました。ルートリフレクタはVPLSプレフィックスを他のプロバイダー エッジ（PE）ルータに反映し、PE が BGP セッションの完全メッシュを持つ必要がないようにします。ネットワーク管理者はルート リフレクタの BGP VPLS アドレス ファミリだけを設定します。

VPLSプレフィックスを反映できるルートリフレクタ設定の例については、「例：ルートリフレクタでの BGP VPLS 自動検出のサポート」の項を参照してください。VPLS 自動検出の詳細については、『*MPLS Layer 2 VPNs Configuration Guide*』の「VPLS Autodiscovery BGP Based」モジュールを参照してください。

ルート リフレクタでの BGP VPLS 自動検出のサポートに関する制約事項

- IOS XE では、ルート リフレクタについて、Inter-AS オプション C の BGP シグナリングを使用した VPLS BGP 自動検出はサポートされていません。

ルート リフレクタでの BGP VPLS 自動検出のサポートの設定例

例：ルート リフレクタでの BGP VPLS 自動検出のサポート

次の例では、PE-RR（プロバイダー エッジ ルート リフレクタであることを示す）という名前のホストが、VPLS プレフィックス可能なルート リフレクタとして設定されます。VPLS アドレス ファミリは **address-family l2vpn vpls** コマンドによって設定されます。

```
hostname PE-RR
!
router bgp 1
 bgp router-id 1.1.1.3
 no bgp default route-target filter
 bgp log-neighbor-changes
neighbor iBGP_PEERS peer-group
```

```
neighbor iBGP_PEERS remote-as 1
neighbor iBGP_PEERS update-source Loopback1
neighbor 1.1.1.1 peer-group iBGP_PEERS
neighbor 1.1.1.2 peer-group iBGP_PEERS
!
address-family l2vpn vpls
  neighbor iBGP_PEERS send-community extended
  neighbor iBGP_PEERS route-reflector-client
  neighbor 1.1.1.1 peer-group iBGP_PEERS
  neighbor 1.1.1.2 peer-group iBGP_PEERS
exit-address-family
!
```

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

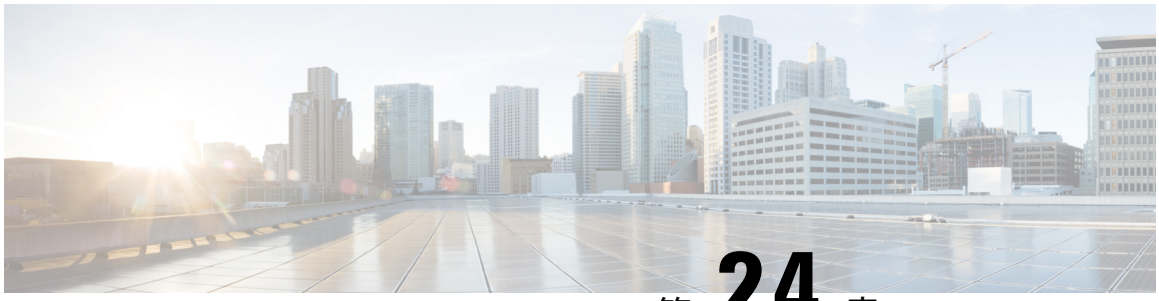
ルート リフレクタでの BGP VPLS 自動検出のサポートに関する機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *39* : ルート リフレクタでの *BGP VPLS* 自動検出のサポートに関する機能情報

機能名	リリース	機能情報
ルート リフレクタでの BGP VPLS 自動検出のサポート		BGP ルート リフレクタが拡張され、ルート リフレクタで VPLS を明示的に設定しなくても BGP VPLS プレフィックスを反映できるようになりました。



第 24 章

BGP FlowSpec ルートリフレクタのサポート

BGP（ボーダー ゲートウェイ プロトコル）FlowSpec (フロー スペック) ルート リフレクタ機能により、サービス プロバイダーはネットワークのトラフィック フローを制御できます。これは、トラフィックのフィルタ処理に有効であり、DDoS トラフィックをドロップするかアナライザに転送することで分散型サービス妨害（DDoS）の軽減を図る際にも役立ちます。

BGP フロー スペックは、BGP のネットワーク層到達可能性情報（NLRI）として配布できるトラフィック フローのフロースペック ルールをエンコードするためのメカニズムを提供します。

- 機能情報の確認 （553 ページ）
- BGP FlowSpec ルートリフレクタのサポートに関する制約事項 （554 ページ）
- BGP FlowSpec ルートリフレクタのサポートに関する情報 （554 ページ）
- BGP FlowSpec ルートリフレクタのサポートの設定方法 （555 ページ）
- BGP FlowSpec ルートリフレクタのサポートの設定例 （562 ページ）
- BGP FlowSpec ルートリフレクタのサポートに関する追加情報 （563 ページ）
- BGP FlowSpec ルートリフレクタのサポートの機能情報 （564 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 FlowSpec ルートリフレクタのサポートに関する制約事項

- Cisco IOS 15.5(S) リリースでは、BGP フロー スペックはルート リフレクタでのみサポートされます。
- アドレスファミリのマッチングとアクションの併用は、フロースペック ルールではサポートされていません。たとえば、IPv4 のマッチングを IPv6 のアクションと組み合わせることはできず、その逆も同様です。

BGP FlowSpec ルートリフレクタのサポートに関する情報

FlowSpec の概要

FlowSpec は、任意のアプリケーションで使用できるボーダー ゲートウェイ プロトコルのネットワーク層到達可能性情報（BGP NLRI）としてフロー スペック ルールを配布する手順を指定します。また、分散型サービス妨害攻撃を軽減するためのパケット フィルタリングを目的とするアプリケーションも定義します。

フロー スペック ルールは、BGP NLRI フィールドでエンコードされたマッチング部分と、RFC 5575 の定義に従って BGP 拡張コミュニティとしてエンコードされたアクション部分で構成されます。フロー スペック ルールは、IP パケット データに適用できる複数のマッチング基準から成るデータのセット（n タプルで表現）です。BGP フロー スペック ルールは、対応するマッチングおよびアクション パラメータを表す同等の Cisco Common Classification Policy Language（C3PL）に内部的に変換されます。

Cisco IOS 15.5(S) リリースでは、FlowSpec は、BGP ルート リフレクタの次の機能をサポートしています。

- RFC 5575 で定義された FlowSpec ルール
- IPv6 拡張
- IP リダイレクト拡張
- BGP FlowSpec 検証

マッチング基準

次の表に、BGP でサポートされるさまざまな FlowSpec のタプルを示します。

BGP FlowSpec NLRI タイプ	QoS マッチング フィールド（IPv6）	QoS マッチング フィールド（IPv4）	入力値
タイプ 1	IPv6 宛先アドレス	IPv4 宛先アドレス	[Prefix length]
タイプ 2	IPv6 送信元アドレス	IPv4 発信元アドレス	[Prefix length]
[Type 3]	IPv6 次ヘッダー	IPv4 プロトコル	複数値の範囲
[Type 4]	IPv6 送信元ポートまたは宛て先ポート	IPv4 送信元ポートまたは宛て先ポート	複数値の範囲
[Type 5]	IPv6 宛て先ポート	IPv4 宛て先ポート	複数値の範囲
タイプ 6	IPv6 送信元ポート	IPv4 送信元ポート	複数値の範囲
[Type 7]	IPv6 ICMP タイプ	IPv4 ICMP タイプ	複数値の範囲
タイプ 8	IPv6 ICMP コード	IPv4 ICMP コード	複数値の範囲
タイプ 9	IPv6 TCP フラグ	IPv4 TCP フラグ（2 バイトに予約ビットを含む）	ビット マスク
タイプ 10	IPv6 パケット長	IPv4 パケット長	複数値の範囲
タイプ 11	IPv6 トラフィック クラス	IPv4 DSCP	複数値の範囲
タイプ 12	予約済み	IPv4 フラグメント ビット	ビット マスク
タイプ 13	IPv6 フロー ラベル	-	複数値の範囲

BGP FlowSpec ルートリフレクタのサポートの設定方法

BGP FlowSpec ルートリフレクタのサポートの設定

ルート リフレクタで BGP FlowSpec を設定するには、次の作業を実行します。この作業では IPv4 アドレス ファミリしか指定しませんが、その他のアドレス ファミリも BGP フロー スペックでサポートされています。

始める前に

BGP ルート リフレクタを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family {ipv4 | ipv6 | vpnv4 | vpnv6} flowspec**
6. **neighbor** *ip-address* **activate**
7. **neighbor** *ip-address* **route-reflector-client**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 1`	BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.1.1.1 remote-as 1`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 5	**address-family {ipv4 | ipv6 | vpnv4 | vpnv6} flowspec** 例： `Device(config-router)# address-family ipv4 flowspec`	アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • FlowSpec は、IPv4、IPv6、VPNv4、VPNv6 アドレス ファミリでサポートされています。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 10.1.1.1 activate`	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** *ip-address* **route-reflector-client** 例： `Device(config-router-af)# neighbor 10.1.1.1 route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	（任意）アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP FlowSpec 検証の無効化

eBGP ピアの BGP フロー スペック検証を無効にする場合は、この作業を実行します。デフォルトでは、検証は有効になっています。

BGP フロー スペック検証の詳細については、RFC 5575（draft-ietf-idr-bgp-flowspec-oid-01-Revised Validation Procedure for BGP Flow Specifications）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family {ipv4 | ipv6 | vpnv4 | vpnv6} flowspec**
5. **neighbor** *ip-address* **validation off**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 1`	BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family {ipv4 | ipv6 | vpnv4 | vpnv6} flowspec** 例：	アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-router)# address-family ipv4 flowspec`	• FlowSpec は、IPv4、IPv6、VPNv4、VPNv6 アドレス ファミリでサポートされています。
ステップ 5	**neighbor** *ip-address* **validation off** 例： `Device(config-router-af)# neighbor 10.1.1.1 validation off`	eBGP ピアのフロースペックの検証を無効にします。

BGP FlowSpec ルートリフレクタのサポートの確認

show コマンドは任意の順序で入力できます。

始める前に

ルート リフレクタで BGP FlowSpec を設定します。

手順の概要

1. **show bgp ipv4 flowspec**
2. **show bgp ipv4 flowspec detail**
3. **show bgp ipv4 flowspec summary**
4. **show bgp ipv6 flowspec**
5. **show bgp ipv6 flowspec detail**
6. **show bgp ipv6 flowspec summary**
7. **show bgp vpnv4 flowspec**
8. **show bgp vpnv4 flowspec all detail**
9. **show bgp vpnv6 flowspec**
10. **show bgp vpnv6 flowspec all detail**

手順の詳細

ステップ 1 **show bgp ipv4 flowspec**

このコマンドは、IPv4 flowspec ルートを表示します。

例：

```
Device# show bgp ipv4 flowspec

BGP table version is 3, local router ID is 10.10.10.2 Status codes: s suppressed, d damped, h
history,
* valid, > best, i - internal, r RIB-failure, S Stale,
m multipath, b backup-path, f RT-Filter, best-external, a additional-path,
c RIB-compressed, Origin codes: i - IGP, e - EGP, ? - incomplete RPKI validation codes: V valid,
I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i Dest:2.2.2.0/24  10.0.101.1                  100      0 i
```

```
 *>i Dest:3.3.3.0/24  10.0.101.1                    100      0 i
```

ステップ 2　show bgp ipv4 flowspec detail

このコマンドは、IPv4 flowspec ルートに関する詳細な情報を表示します。

例：

```
Device# show bgp ipv4 flowspec detail

BGP routing table entry for Dest:2.2.2.0/24, version 2
  Paths: (1 available, best #1, table IPv4-Flowspec-BGP-Table)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local, (Received from a RR-client)
    10.0.101.1 from 10.0.101.1 (10.0.101.1)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: FLOWSPEC Redirect-IP:0x000000000001
      rx pathid: 0, tx pathid: 0x0
BGP routing table entry for Dest:3.3.3.0/24, version 3
  Paths: (1 available, best #1, table IPv4-Flowspec-BGP-Table)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local, (Received from a RR-client)
    10.0.101.1 from 10.0.101.1 (10.0.101.1)
      Origin IGP, localpref 100, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
```

ステップ 3　show bgp ipv4 flowspec summary

このコマンドは、IPv4 flowspec ネイバーを表示します。

例：

```
Device# show bgp ipv4 flowspec summary

BGP router identifier 10.10.10.2, local AS number 239 BGP table version is 3, main routing table
 version 3
2 network entries using 16608 bytes of memory
2 path entries using 152 bytes of memory
2/2 BGP path/bestpath attribute entries using 304 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory BGP using 17136 total bytes of memory BGP
 activity 18/0
prefixes, 18/0 paths, scan interval 15 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.0.101.1      4          239      70      24        3    0    0 00:10:58
       2
10.0.101.2      4          239       0       0        1    0    0 never
Idle
10.0.101.3      4          240       0       0        1    0    0 never
Idle
10.10.10.1      4          239      19      23        3    0    0 00:10:53
```

ステップ 4 show bgp ipv6 flowspec

このコマンドは、IPv6 flowspec ルートを表示します。

例：

```
Device# show bgp ipv6 flowspec

BGP table version is 2, local router ID is 10.10.10.2 Status codes: s suppressed, d damped, h
history,
 * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,

 x best-external, a additional-path, c RIB-compressed, Origin codes: i - IGP, e - EGP,
 ? - incomplete RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i Dest:3::/0-24,Source:4::/0-24
                       FEC0::1001                  100      0 i
```

ステップ 5 show bgp ipv6 flowspec detail

このコマンドは、IPv6 flowspec ルートに関する詳細な情報を表示します。

例：

```
Device# show bgp ipv6 flowspec detail

BGP routing table entry for Dest:3::/0-24,Source:4::/0-24, version 2
  Paths: (1 available, best #1, table Global-Flowspecv6-Table)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  Local
    FEC0::1001 from FEC0::1001 (10.0.101.2)
      Origin IGP, localpref 100, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
```

ステップ 6 show bgp ipv6 flowspec summary

このコマンドは、IPv6 flowspec ネイバーを表示します。

例：

```
Device# show bgp ipv6 flowspec summary

BGP router identifier 10.10.10.2, local AS number 239 BGP table version is 3, main routing table
 version 3
2 network entries using 16608 bytes of memory
2 path entries using 152 bytes of memory
2/2 BGP path/bestpath attribute entries using 304 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory BGP using 17136 total bytes of memory BGP
 activity 18/0
prefixes, 18/0 paths, scan interval 15 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.0.101.1      4          239      70      24        3    0    0 00:10:58
       2
10.0.101.2      4          239       0       0        1    0    0 never
```

```
Idle
10.0.101.3      4          240       0       0        1    0    0 never
Idle
10.10.10.1      4          239      19      23        3    0    0 00:10:53
```

ステップ 7 show bgp vpnv4 flowspec

このコマンドは、VPNv4 flowspec ネイバーを表示します。

例：

```
Device# show bgp vpnv4 flowspec

BGP table version is 2, local router ID is 10.10.10.2 Status codes: s suppressed, d damped, h
history,
* valid, > best, i - internal,r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed, Origin codes: i - IGP, e - EGP,
? - incomplete RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher:  200:200
 *>i Dest:10.0.1.0/24 10.0.101.1                  100      0 i
```

ステップ 8 show bgp vpnv4 flowspec all detail

このコマンドは、VPNv4 flowspec の詳細を表示します。

例：

```
Device# show bgp vpnv4 flowspec all detail

Route Distinguisher: 200:200
BGP routing table entry for 200:200:Dest:10.0.1.0/24, version 2
  Paths: (1 available, best #1, table VPNv4-Flowspec-BGP-Table)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  Local
    10.0.101.1 (via default) from 10.0.101.1 (10.0.101.1)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:100:100
      rx pathid: 0, tx pathid: 0x0
```

ステップ 9 show bgp vpnv6 flowspec

このコマンドは、VPNv6 flowspec ネイバーを表示します。

例：

```
Device# show bgp vpnv6 flowspec

BGP table version is 2, local router ID is 10.10.10.2 Status codes: s suppressed, d damped, h
history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed, Origin codes: i - IGP, e -
EGP, ? - incomplete RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:200
 *>i SPort:=20640     FEC0::1001                  100      0 i
```

ステップ 10 **show bgp vpnv6 flowspec all detail**

このコマンドは、VPNv6 flowspec の詳細を表示します。

例：

```
Device# show bgp vpnv6 flowspec all detail

Route Distinguisher: 200:200
BGP routing table entry for 200:200:SPort:=20640, version 2
  Paths: (1 available, best #1, table VPNv6-Flowspec-BGP-Table)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  Local
    FEC0::1001 (via default) from FEC0::1001 (10.0.101.2)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:100:100
      rx pathid: 0, tx pathid: 0x0
```

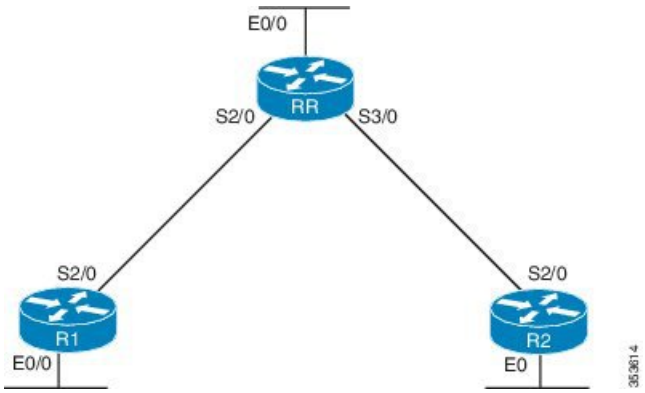
BGP FlowSpec ルートリフレクタのサポートの設定例

例：BGP FlowSpec ルートリフレクタのサポート

例：ルート リフレクタでの BGP FlowSpec の設定

BGP ルート リフレクタを設定し、ルート リフレクタに flowspec を挿入します。

図 *42 : BGP* ルート リフレクタ トポロジ




```
! Configure the topology

!Configure the interfaces on RR

RR> enable
RR# configure terminal
RR(config)# interface E0/0
RR(config-if)# ip address 10.0.0.1 255.224.0.0
```

```
RR(config-if)# no shutdown
RR(config-if)# exit
RR(config)# interface S2/0
RR(config-if)# ip address 10.32.0.1 255.224.0.0
RR(config-if)# no shutdown
RR(config-if)# exit
RR(config)# interface S3/0
RR(config-if)# ip address 10.64.0.1 255.224.0.0
RR(config-if)# no shutdown

!Configure RR as the route reflector with S2/0(R1) and S2/0 (R2) as the neighbors

RR(config)# router bgp 333
RR(config-router)# no synchronization
RR(config-router)# network 10.0.0.0 mask 255.224.0.0
RR(config-router)# network 10.64.0.0 mask 255.224.0.0
RR(config-router)# network 10.32.0.0 mask 255.224.0.0
RR(config-router)# neighbor 10.64.0.2 remote-as 333
RR(config-router)# neighbor 10.32.0.2 remote-as  333


!Configure flowspec on route reflector

RR(config-router)# address-family ipv4 flowspec
RR(configure-router-af)# neighbor 10.64.0.2 activate
RR(config-router)# neighbor 10.64.0.2 route-reflector-client
RR(configure-router-af)# neighbor 10.32.0.2 activate
RR(config-router)# neighbor 10.32.0.2 route-reflector-client

!Verify the configuration

RR> show bgp ipv4 flowspec
```

BGP FlowSpec ルートリフレクタのサポ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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5575	『*Dissemination of Flow Specification Rules*』

シスコのテクニカル サポート

説明	リンク
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

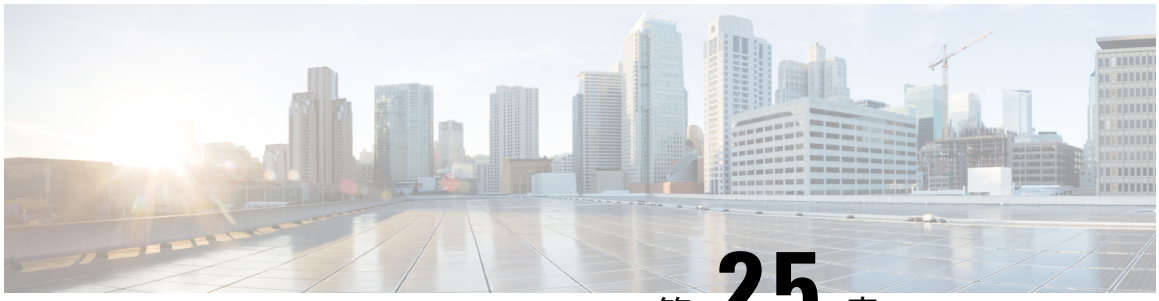
BGP FlowSpec ルートリフレクタのサポートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *40 : BGP FlowSpec* ルートリフレクタのサポートの機能情報

機能名	リリース	機能情報
BGP FlowSpec ルートリフレクタのサポート	15.5(1)S	BGP FlowSpec ルートリフレクタのサポート機能により、サービス プロバイダーはネットワークのトラフィック フローを制御し、DDoS 攻撃を軽減できます。 この機能により、**address-family {ipv4 | ipv6 | vpnv4 | vpnv6} flowspec** コマンドが導入されました。



第 25 章

BGP フロー スペック クライアント

ボーダー ゲートウェイ プロトコル（BGP）のフロー スペック クライアント機能を使用すると、デバイスが BGP フロー スペック クライアントの役割を担い、BGP フロー スペック コントローラからフロー スペック ルールを受信できるようになります。フロー スペック ルールには、マッチング基準とアクション（フローとも呼ばれる）のセットが含まれます。フローは、クライアントデバイスまたはクライアント上の特定のインターフェイスにフローをアドバタイズするコントローラ（デバイス）で設定されます。

注目 IOS XE ソフトウェアでは、BGP フロー スペック クライアント機能がサポートされていますが、BGP フロー スペック コントローラ機能はサポートされていません。

- 機能情報の確認 （565 ページ）
- BGP フロー スペック クライアントの前提条件 （566 ページ）
- BGP フロー スペック クライアントの制約事項 （566 ページ）
- BGP フロー スペック クライアントに関する情報 （566 ページ）
- BGP フロー スペック クライアントの設定方法 （568 ページ）
- BGP フロー スペック クライアントの設定例 （574 ページ）
- BGP フロー スペック クライアントに関する追加情報 （575 ページ）
- BGP フロー スペック クライアントの機能情報 （576 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 フロー スペック クライアントの前提条件

- コントローラでフロー スペック ルールを識別および設定します。

（注） フロー スペック クライアントが有効になっている場合、コントローラのフローのマッチング基準および対応するアクションがクライアント デバイスにリモートで挿入され、クライアント デバイスのプラットフォーム ハードウェアにフローがプログラムされます。

BGP フロー スペック クライアントの制約事項

- Cisco IOS 15.5(S) リリースでは、BGP フロー スペックは BGP フロー スペック クライアントおよびルート リフレクタでのみサポートされます。
- アドレス ファミリのマッチングとアクションの併用は、フロー スペック ルールではサポートされていません。たとえば、IPv4 のマッチングを IPv6 のアクションと組み合わせることはできず、その逆も同様です。

BGP フロー スペック クライアントに関する情報

BGP フロー スペック モデル

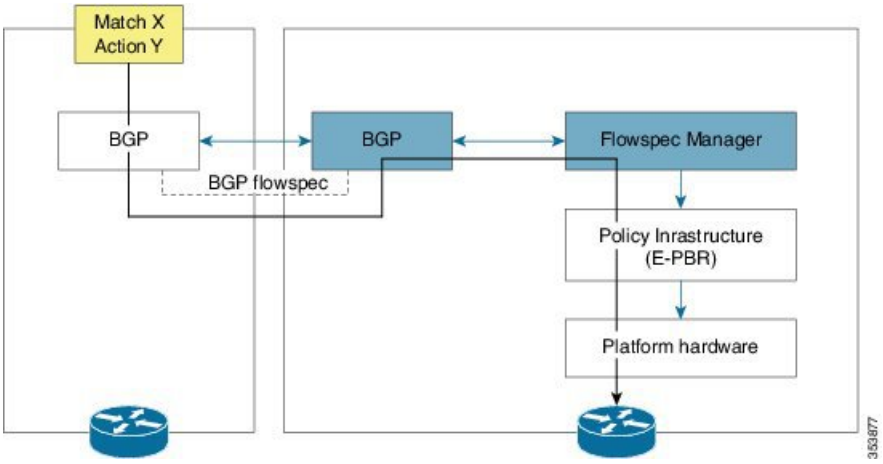
BGP プロトコルは、ほかにはないその利点から、フロー スペックに使用されています。BGP 対応デバイスによるフロー スペックのルーティングには、コントローラ、クライアント、ルート リフレクタ（オプション）という 3 つの要素が使用されます。このドキュメントはクライアント要素機能を対象としています。

IOS XE ソフトウェアを搭載したデバイス（ASR 1000 など）が担うことができる役割は BGP フロー スペックのコントローラではなくクライアントですが、以下では、より深く理解できるように、BGP フロー スペック プロセスの概要を簡単に示します。

BGP フロー スペック機能を使用すると、多数の BGP ピア デバイス間でフィルタリングおよびポリシング機能を迅速に展開および伝播して、ネットワーク上で分散型サービス妨害（DDoS）攻撃の影響を軽減できます。

BGP フロー スペック モデルは、クライアントとコントローラで構成されます（ルート リフレクタの使用はオプションです）。コントローラは、フロー スペックの NRLI エントリの送信または挿入を行います。クライアント（BGP スピーカーとして機能）は、NRLI を受信し、コントローラからの命令に従って動作するようにハードウェア転送をプログラムします。このモデルの図を下に示します。

図 *43 : BGP* フロー スペック モデル



上のトポロジでは、左側にあるコントローラが、フロースペックの NRLI を右側のクライアントに挿入します。クライアントは、この情報を受信してフロー スペック マネージャ コンポーネントに送信し、ePBR（Enhanced Policy Based Routing）インフラストラクチャを設定します。これにより、デバイスのプラットフォームハードウェアがプログラムされます。このようにして、ネットワーク上の DDoS 攻撃に対処するルールを作成できます。

フロー スペック クライアントの設定例

まず、デバイスを BGP 自律システムに関連付け、各種のアドレス ファミリに対してフロー スペック ポリシー マッピング機能を有効にします。次に、IP アドレスを使用してネイバーを BGP ピアとして識別し、**neighbor activate** コマンドによって、デバイス間で情報を交換する機能を有効にします。このようにして、クライアント、コントローラ、およびその他のフロー スペック クライアント デバイスの間でフロー スペック情報を交換できるようにします。

```
!
router bgp 100
 address-family ipv4 flowspec
  neighbor 10.1.1.1 activate
!
```

マッチング基準とアクション

フロー スペック NLRI タイプは、オプションである複数のサブコンポーネントで構成されます。特定のパケットがフロースペックと一致すると見なされるのは、そのスペック内に存在するすべてのコンポーネントの共通点（AND）に合致する場合です。定義できるサポート対象コンポーネントのタイプまたはタプルを次に示します。

BGP FlowSpec NLRI タイプ	**QoS** マッチング フィールド（**IPv6**）	**QoS** マッチング フィールド（**IPv4**）	入力値
タイプ 1	IPv6 宛先アドレス	IPv4 宛先アドレス	[Prefix length]

BGP FlowSpec NLRI タイプ	QoS マッチング フィールド（IPv6）	QoS マッチング フィールド（IPv4）	入力値
タイプ 2	IPv6 送信元アドレス	IPv4 発信元アドレス	[Prefix length]
[Type 3]	IPv6 次ヘッダー	IPv4 プロトコル	複数値の範囲
[Type 4]	IPv6 送信元ポートまたは宛て先ポート	IPv4 送信元ポートまたは宛て先ポート	複数値の範囲
[Type 5]	IPv6 宛て先ポート	IPv4 宛て先ポート	複数値の範囲
タイプ 6	IPv6 送信元ポート	IPv4 送信元ポート	複数値の範囲
[Type 7]	IPv6 ICMP タイプ	IPv4 ICMP タイプ	複数値の範囲
タイプ 8	IPv6 ICMP コード	IPv4 ICMP コード	複数値の範囲
タイプ 9	IPv6 TCP フラグ	IPv4 TCP フラグ（2 バイトに予約ビットを含む）	ビット マスク
タイプ 10	IPv6 パケット長	IPv4 パケット長	複数値の範囲
タイプ 11	IPv6 トラフィック クラス	IPv4 DSCP	複数値の範囲
タイプ 12	予約済み	IPv4 フラグメント ビット	ビット マスク

BGP フロー スペック クライアントの設定方法

フロースペッククライアントとしてのデバイスの設定およびネイバーとの BGP ピア関係の確立

次の作業では、BGP フロー スペック クライアントとしてのデバイスの設定について説明します。VRF インスタンス内のデバイス インターフェイスは、BGP フロー スペック クライアントの役割を担うこともできます。

始める前に

デバイスをフロー スペック クライアントとして設定する前に、フロー スペック コントローラ デバイス（および必要に応じてルートリフレクタ）を識別して設定することをお勧めします。フロースペック ルールがコントローラで設定されている場合、ルールはクライアントにリモー

トで挿入され、マッチング基準および対応するアクションがクライアントのプラットフォーム ハードウェアにプログラムされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**ipv4** | **ipv6**} **flowspec**
5. **neighbor** *ip-address* **activate**
6. **exit**
7. **address-family** {**ipv4** | **ipv6**} **flowspec vrf** *vrf-name*
8. **neighbor** *ip-address* **remote-as** *as-number*
9. **neighbor** *ip-address* **activate**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	自律システム番号を指定し、BGP コンフィギュレーション モードを開始します。このモードでは、BGP ルーティング プロセスを設定できます。
ステップ 4	**address-family** {**ipv4** | **ipv6**} **flowspec** 例： `Device(config-bgp)# address-family ipv4 flowspec`	IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを指定し、BGP 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、フロー スペック ポリシーマッピングのグローバルアドレス ファミリを初期化します。
ステップ 5	**neighbor** *ip-address* **activate** 例： `Device(config-bgp-af)# neighbor 10.1.1.1 activate`	BGP ルーティングのためにデバイスをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。デバイスからその BGP ネイバーに IP アドレスを含む情報をアドバタイズ（および受信）できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-bgp-af)# exit`	BGP 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、BGP コンフィギュレーション モードを開始します。
ステップ 7	**address-family** {**ipv4** | **ipv6**} **flowspec vrf** *vrf-name* 例： `Device(config-bgp)# address-family ipv4 flowspec vrf vrf1`	VRF の IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを指定し、BGP 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、フロー スペック ポリシー マッピングのグローバル アドレス ファミリを初期化します。
ステップ 8	**neighbor** *ip-address* **remote-as** *as-number* 例： `Device(config-bgp-af)# neighbor 2001:DB8:1::1 remote-as 100`	BGP ルーティングのためにデバイスをネイバー コンフィギュレーション モードにして、ネイバー（IP アドレス）を BGP ピアとして設定します。**remote-as** キーワードは、指定されたリモート自律システム番号をネイバーに割り当てます。
ステップ 9	**neighbor** *ip-address* **activate** 例： `Device(config-bgp-af)# neighbor 2001:DB8:1::1 activate`	デバイスからその BGP ネイバーに IP アドレスを含む情報をアドバタイズ（および受信）できるようにします。
ステップ 10	**exit** 例： `Device(config-bgp-af)# exit`	BGP 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、BGP コンフィギュレーション モードを開始します。

デバイスのすべてのインターフェイスでのフロー スペック ポリシーの設定

次の設定作業では、IPv4 アドレス ファミリおよび IPv6 アドレス ファミリのデバイスのすべてのインターフェイスと VRF インスタンス内のインターフェイスでのフロー スペック ポリシーの設定について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flowspec**
4. **address-family ipv4**
5. **local-install interface-all**
6. **exit**
7. **address-family ipv6**
8. **local-install interface-all**
9. **exit**

10. **vrf** *vrf-name*
11. **address-family ipv4**
12. **local-install interface-all**
13. **exit**
14. **address-family ipv6**
15. **local-install interface-all**
16. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**flowspec** 例： `Device(config)# flowspec`	flowspec コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4** 例： `Device(config-flowspec)# address-family ipv4`	IPv4 アドレス ファミリを指定し、フロー スペックのアドレス 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	**local-install interface-all** 例： `Device(config-flowspec-af)# local-install interface-all`	flowspec ポリシーをすべてのインターフェイスにインストールします。
ステップ 6	**exit** 例： `Device(config-flowspec-af)# exit`	フロー スペックのアドレス ファミリ コンフィギュレーション モードを終了し、flowspec コンフィギュレーション モードを開始します。
ステップ 7	**address-family ipv6** 例： `Device(config-flowspec)# address-family ipv6`	IPv6 アドレス ファミリを指定し、フロー スペックのアドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**local-install interface-all** 例： `Device(config-flowspec-af)# local-install interface-all`	flowspec ポリシーをすべてのインターフェイスにインストールします。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-flowspec-af)# exit`	フロー スペックのアドレス ファミリ コンフィギュレーション モードを終了し、flowspec 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-flowspec)# vrf vrf10`	VRF インスタンスを設定し、フロー スペックの 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 11	**address-family ipv4** 例： `Device(config-flowspec-vrf)# address-family ipv4`	IPv4 アドレス ファミリを指定し、フロー スペックの VRF アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 12	**local-install interface-all** 例： `Device(config-flowspec-vrf-af)# local-install interface-all`	flowspec ポリシーをすべてのインターフェイスにインストールします。
ステップ 13	**exit** 例： `Device(config-flowspec-vrf-af)# exit`	フロー スペックの 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、フロー スペックの 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 14	**address-family ipv6** 例： `Device(config-flowspec-vrf)# address-family ipv6`	IPv6 アドレス ファミリを指定し、フロー スペックの VRF アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 15	**local-install interface-all** 例： `Device(config-flowspec-vrf-af)# local-install interface-all`	flowspec ポリシーをすべてのインターフェイスにインストールします。
ステップ 16	**exit** 例： `Device(config-flowspec-vrf-af)# exit`	フロー スペックの 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、フロー スペックの VRF コンフィギュレーション モードを開始します。

BGP フロー スペック クライアントの確認

以下のコマンドは、フロー スペック設定の詳細を表示します。

手順の概要

1. **show flowspec summary**

2. **show bgp ipv4 flowspec**
3. **show flowspec vrf** *vrf-name* **afi-all**

手順の詳細

ステップ 1 show flowspec summary

例：

```
Device # show flowspec summary

FlowSpec Manager Summary:
Tables: 2
Flows: 1
```

ノード上に存在するフロー スペック ルールの概要を示します。

この例では、[**Tables**] フィールドは、フロー スペック ポリシー マッピング機能が IPv4 アドレス ファミリおよび IPv6 アドレス ファミリに対して有効になっていることを示しています。

[**Flows**] フィールドは、テーブル全体で単一のフローが定義されていることを示しています。

ステップ 2 show bgp ipv4 flowspec

例：

```
Device # show bgp ipv4 flowspec

Dest:192.0.2.0/24, Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208
BGP routing table entry for Dest:192.0.2.0/24,
Source:10.1.1.0/24,Proto:=47,DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 <snip>
Paths: (1 available, best #1)
  Advertised to update-groups (with more than one peer):
    0.3
  Path #1: Received by speaker 0
  Advertised to update-groups (with more than one peer):
0.3 Local
0.0.0.0 from 0.0.0.0 (3.3.3.3)
Origin IGP, localpref 100, valid, redistributed, best, group-best
Received Path ID 0, Local Path ID 1, version 42
Extended community: FLOWSPEC Traffic-rate:100,0
```

フロー スペック コントローラ（デバイス）で設定されているフロー スペック ルールが BGP 側で使用可能かどうかを確認するには、このコマンドを使用します。この例では、[*redistributed*] は、フロー スペック ルールが内部では発信されていないが、フロー スペック プロセスから BGP に再配布されていることを示しています。設定されている拡張コミュニティ（マッチング基準およびアクションをピア デバイスに送信するために使用される BGP 属性）も表示されています。

この例では、定義されたアクションはトラフィックのレート制限です。

ステップ 3 show flowspec vrf *vrf-name* afi-all

例：

```
Device # show flowspec vrf vrf100 afi-all

VRF: vrf100     AFI: IPv4
    Flow         :DPort:=101,SPort:=101,TCPFlags:~0xFF,Length:>=100&<=1500,DSCP:=63
    Actions      :Redirect: VRF vrf200 Route-target: ASN2-200:2  (bgp.1)
    Flow         :DPort:=102,SPort:=102,TCPFlags:~0xFF,Length:>=100&<=1500,DSCP:=63
    Actions      :Redirect: VRF vrf200 Route-target: ASN2-200:2  (bgp.1)
```

フロー スペック クライアント（デバイス）に関連付けられた特定の VRF 内にフロー スペック ルールがあるかどうかを確認するには、このコマンドを使用します。

BGP フロー スペック クライアントの設定例

例：フロー スペック クライアントとしてのデバイスの設定およびネイバーとの BGP ピア関係の確立

```
Device> enable
Device# configure terminal
Device (config)# router bgp 100
Device (config-bgp)# address-family ipv4 flowspec
Device (config-bgp-af)# neighbor 10.1.1.1 activate
Device (config-bgp-af)# exit
Device (config-bgp)# address-family ipv4 flowspec vrf vrf1
Device (config-bgp-af)# neighbor 2001:DB8:1::1 remote as 100
Device (config-bgp-af)# neighbor 2001:DB8:1::1 activate
Device (config-bgp-af)# exit
```

例：デバイスのすべてのインターフェイスでのフロー スペック ポリシーの設定

```
Device> enable
Device# configure terminal
Device(config)# flowspec
Device(config-flowspec)# address-family ipv4
Device(config-flowspec-af)# local-install interface-all
Device(config-flowspec-af)# exit
Device(config-flowspec)# address-family ipv6
Device(config-flowspec-af)# local-install interface-all
Device(config-flowspec-af)#  exit
Device(config-flowspec)# vrf vrf10
Device(config-flowspec-vrf)# address-family ipv4
Device(config-flowspec-vrf-af)# local-install interface-all
Device(config-flowspec-vrf-af)# exit
Device(config-flowspec-vrf)# address-family ipv6
```

```
Device(config-flowspec-vrf-af)# local-install interface-all
Device(config-flowspec-vrf-af)# exit
```

BGP フロー スペック クライアン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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP FlowSpec ルートリフレクタのサポート	『*IP Routing: BGP Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 5575	『*Dissemination of Flow Specification Rules*』

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	リンク
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

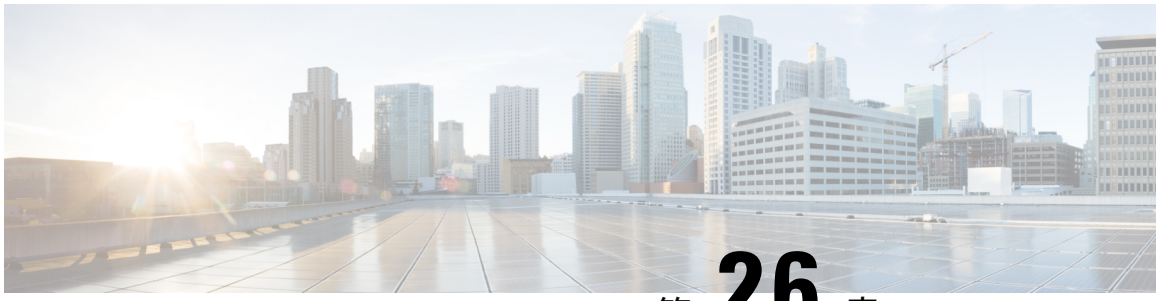
BGP フロー スペック クライアントの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *41 : BGP* フロー スペック クライアントの機能情報

機能名	リリース	機能情報
BGP フロー スペック クライアント	Cisco IOS XE 3.15S	BGP フロースペック クライアント機能を使用すると、デバイスが BGP フロー スペック クライアントの役割を担い、BGP フロースペック コントローラからフロースペック ルールを受信できるようになります。 次のコマンドが導入または変更されました。**flowspec**、**local-install interface-all**



第 26 章

BGP NSF 認識

ノンストップ フォワーディング（NSF）認識を使用すると、ルータは、NSF 対応ネイバーがステートフル スイッチオーバー（SSO）操作中にパケットの転送を続行できるようにします。BGP ノンストップ フォワーディング認識機能では、BGP を実行している NSF 認識ルータが、SSO 操作を実行しているルータのすでに認識されているルートとともにパケットを転送できます。この機能によって、障害が発生したルータの BGP ピアが、そのようなルータによってアドバタイズされたルーティング情報を保持して、障害が発生したルータが通常の動作に戻ってルーティング情報を交換できるようになるまでこの情報を引き続き使用できるようになります。ピアリング セッションは、NSF 操作全体を通じて維持されます。

- 機能情報の確認 （577 ページ）
- BGP NSF 認識に関する情報 （578 ページ）
- BGP NSF 認識の設定方法 （580 ページ）
- BGP NSF 認識の設定例 （586 ページ）
- その他の参考資料 （587 ページ）
- BGP NSF 認識の機能情報 （587 ページ）

機能情報の確認

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

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

BGP NSF 認識に関する情報

Cisco NSF ルーティングと転送操作

Cisco NSF は、ルーティングのために BGP、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、および Intermediate System-to-Intermediate System（IS-IS）プロトコルによってサポートされ、転送のために Cisco Express Forwarding（CEF）によってサポートされています。ルーティング プロトコルの BGP、EIGRP、OSPF、および IS-IS は NSF 機能と NSF 認識によって拡張されています。これは、これらのプロトコルを実行するデバイスがスイッチオーバーを検出して、ネットワーク トラフィックの転送を続行してピア デバイスからルート情報を回復するために必要な処理を行うことができることを意味します。

このモジュールでは、NSF 互換のソフトウェアを実行しているネットワーキング デバイスは NSF 認識であると見なします。NSF をサポートするようにデバイスが設定されている場合にそのデバイスは NSF 対応と見なされます。NSF 認識ネイバーまたは NSF 対応ネイバーからルーティング情報を再構築します。

ルーティング プロトコルがルーティング情報ベース（RIB）テーブルを再作成している間、それぞれのプロトコルは、CEF に依存してスイッチオーバー中にパケットの転送を続行します。ルーティング プロトコルの収束後に、CEF は Forwarding Information Base（FIB; 転送情報ベース）テーブルを更新し、失効したルート エントリを削除します。それから CEF はラインカードに新しい FIB 情報を更新します。

NSF のシスコ エクスプレス フォワーディング

NSF の重要な要素はパケット転送です。シスコのネットワーキング デバイスでは、パケットの転送は CEF によって行われます。CEF は FIB を維持し、スイッチオーバー時に最新だった FIB 情報を使用して、スイッチオーバー中のパケットの転送を続行します。この機能により、スイッチオーバー中のトラフィックの中断を短くします。

通常の NSF 操作中に、アクティブなルート プロセッサ（RP）上の CEF は、現在の FIB と隣接データベースを、スタンバイ RP 上の FIB と隣接データベースと同期させます。アクティブな RP のスイッチオーバー時に、スタンバイ RP には最初、アクティブな RP 上で最新だったもののミラー イメージである FIB と隣接データベースがあります。インテリジェント ラインカードを備えたプラットフォームでは、ラインカードはスイッチオーバーの前後で現行の転送情報を維持します。転送エンジンを備えたプラットフォームでは、CEF は、アクティブな RP の CEF によって送信される変更を使用して、スタンバイ RP の転送エンジンを最新の状態に保ちます。この方法では、転送エンジンのラインカードは、インターフェイスとデータ パスが使用可能になるとすぐに、スイッチオーバー後に転送を続行できます。

ルーティング プロトコルがプレフィックスごとに RIB を再び読み込み始めるため、CEF に対してプレフィックスごとの更新が行われます。CEF はこれを使用して FIB と隣接データベースを更新します。既存エントリと新規エントリには、最新であることを示す新しいバージョン（エポック）番号が付けられます。転送情報はラインカードまたは収束中の転送エンジンで更新されます。RIB が収束すると、RP が信号通知を行います。ソフトウェアは、現在のスイッ

チオーバー エポックよりも前のエポックを持った FIB および隣接エントリをすべて削除します。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

ルーティング プロトコルは、アクティブな RP だけで実行され、ネイバー ルータからルーティングの更新を受信します。ルーティング プロトコルは、スタンバイ RP では実行されません。スイッチオーバーの後、ルーティング プロトコルは、ルーティング テーブルの再構築に役立つステート情報を送信するよう NSF 認識ネイバー デバイスに要求します。

（注） NSF 動作の場合、ルーティング プロトコルは、ルーティング情報を再構築している間にパケットを転送し続ける CEF によって異なります。

NSF のための BGP グレースフル リスタート

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。このメッセージには、NSF 対応ルータまたは NFS 認識ルータにグレースフル リスタート機能があるという宣言が含まれます。グレースフル リスタートは、スイッチオーバーの後に BGP ルーティング ピアでルーティング フラップが発生するのを防ぐメカニズムです。BGP ピアがこの機能を受信した場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応ルータと BGP ピア（NSF 認識ピア）の両方が、セッションの確立時に OPEN メッセージでグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を交換しない場合、セッションはグレースフル リスタート対応になりません。

RP のスイッチオーバー中に BGP セッションが切断された場合、NSF 認識 BGP ピアは、NSF 対応ルータに関連付けられたすべてのルートを失効とマーキングします。ただし、所定の時間内は、引き続きこれらのルートを転送の決定に使用します。この機能により、新しくアクティブになった RP が BGP ピアとのルーティング情報のコンバージェンスを待機している間にパケットが消失することを防ぐことができます。

RP のスイッチオーバーが発生した後、NSF 対応ルータは BGP ピアとのセッションを再確立します。新しいセッションの確立時に、NSF 対応ルータが再起動したことを識別する新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピアの間で交換されます。この交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、RIB と FIB を新しい転送情報で更新します。NSF 認識デバイスは、ネットワーク情報を使用して失効したルートを BGP テーブルから削除します。この後 BGP プロトコルが完全に収束します。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージのグレースフル リスタート機能は無視されますが NSF 対応デバイスを使用して BGP セッションを確立します。この機能により、NSF 非認識（つまり NSF 機能のない）BGP ピアとの相互運用が可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタート機能を使用できません。

BGP NSF 認識

BGP NSF 認識

NSF に対する BGP サポートでは、ネイバー ルータは NSF 認識または NSF 対応でなければなりません。BGP での NSF 認識は、グレースフル リスタート メカニズムによってもイネーブルにされます。NSF 認識ルータは SSO 操作を実行できないという 1 つの例外を除き、NSF 認識ルータは、NSF 対応ルータと同じように機能します。ただし、NSF 認識ルータは、NSF SSO 操作中に NSF 対応ネイバーとのピアリング関係を維持したり、SSO 操作中にこのネイバーのルートを保持したりすることができます。

BGP ノンストップ フォワーディング認識機能は、NSF 認識ルータに、SSO 操作を実行しているネイバーを検出し、このネイバーとのピアリング セッションを維持して、認識されているルートを保持し、これらのルートのパケット転送を続行するための機能を提供します。BGP NSF 認識を配置すると、ルート プロセッサ（RP）の障害状態の影響を最小限に抑え、障害が発生したルータとのピアリングを再確立するために通常必要なリソースの量を減らすことで全体的なネットワークの安定性を向上させることができます。

BGP のための NSF 認識はデフォルトでイネーブルになっていません。BGP を実行しているルータで NSF 認識をグローバルに有効にするには、**bgp graceful-restart** コマンドを使用します。また、NSF 認識操作は、ネットワーク オペレータと、NSF 機能をサポートしていない BGP ピアに対して透過的に行われます。

（注） NSF 認識は、EIGRP、IS-IS、および OSPF などの内部ゲートウェイ プロトコル用のサポートされるソフトウェア イメージでは自動的にイネーブルにされます。BGP では、グローバル NSF 認識は、自動的には有効化されないため、ルータ コンフィギュレーション モードで **bgp graceful-restart** コマンドを発行して開始する必要があります。

BGP NSF 認識の設定方法

BGP グレースフル リスタートを使用した BGP ノンストップ フォワーディング認識の設定

このセクションの作業は、BGP グレースフル リスタート機能を使用して BGP ノンストップ フォワーディング（NSF）認識を設定する方法を示しています。

- 最初の作業では、すべての BGP ネイバーの BGP NSF をグローバルにイネーブルにして、いくつかのトラブルシューティング オプションを提案します。
- 2 番目の作業では、BGP グレースフル リスタート タイマーを調整する方法について説明します。ただし、ほとんどのネットワーク配置では、デフォルト設定が最適です。
- 次の 3 つの作業では、ピア セッション テンプレートとピア グループを含め、個別の BGP ネイバーの BGP グレースフル リスタートを有効または無効にする方法を示します。

• 最後の作業では、BGP NSF のローカルおよびピア ルータ設定を確認します。

BGP グレースフル リスタートを使用した BGP グローバル NSF 認識のイネーブル化

この作業は、すべての BGP ネイバーで BGP NSF 認識をグローバルにイネーブルにする場合に実行します。BGP NSF 認識はグレースフル リスタート メカニズムの一部であり、BGP NSF 認識は、ルータ コンフィギュレーション モードで **bgp graceful-restart** コマンドを実行することで有効にします。BGP NSF 認識を使用すると、NSF 認識ルータが SSO 操作中に NSF 対応ルータをサポートできます。NSF 認識はデフォルトではイネーブルになっておらず、BGP NSF に関与するすべてのネイバーで設定する必要があります。

（注） BGP グレースフル リスタート機能をイネーブルにするには、リスタート タイマーと失効パス タイマーの設定は不要です。デフォルト値はほとんどのネットワーク構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

（注） BGP が実行されているデバイスで NSF 用の Bidirectional Forwarding Detection（BFD）と BGP の両方のグレースフル リスタートを設定すると、最適ではないルーティングが行われる可能性があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds*] [**stalepath-time** *seconds*]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 45000`	
ステップ 4	**bgp graceful-restart** [**restart-time** *seconds*] [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart`	BGP グレースフル リスタート機能と BGP NSF 認識をイネーブルにします。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。 • このコマンドは、再起動ルータとそのすべてのピア（NSF 対応と NSF 認識）で使用してください。
ステップ 5	**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。

トラブルシューティングのヒント

NSF機能をトラブルシューティングするには、必要に応じて特権EXECモードで次のコマンドを使用します。

- **debug ip bgp** ：グレースフル リスタート機能をアドバタイズする OPEN メッセージを表示します。
- **debug ip bgp event** ：リスタート タイマーや失効パス タイマーなどのグレースフル リスタート タイマー イベントを表示します。
- **debug ip bgp updates** ：送受信した EOR メッセージを表示します。EOR メッセージは、失効パス タイマー（設定されている場合）を開始するために NSF 認識ルータによって使用されます。
- **show ip bgp** ：BGP ルーティング テーブル内のエントリを表示します。このコマンドの出力には、それぞれの失効ルートの横に文字「S」を表示することで失効とマーキングされているルートが表示されます。
- **show ip bgp neighbor** ：ネイバー デバイスへの TCP 接続および BGP 接続についての情報を表示します。イネーブルにすると、グレースフル リスタート機能がこのコマンドの出力に表示されます。

次の作業

BGP セッションの確立後に **bgp graceful-restart** コマンドを実行する場合は、グレースフル リスタート機能を交換する前に、**clear ip bgp *** コマンドを実行するかルータをリロードすることによって、セッションをリセットする必要があります。BGP セッションのリセットと **clear ip**

bgp コマンドの使用に関する詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。

BGP NSF 認識タイマーの設定

この作業は、BGP グレースフル リスタート タイマーを調整する場合に実行します。設定できる BGP グレースフル リスタート タイマーは 2 つあります。任意の **restart-time** キーワードと *seconds* 引数は、BGP OPEN メッセージを受信するまでピア ルータが失効したルートを削除するために待機する時間の長さを決定します。デフォルト値は 120 秒です。任意の **stalepath-time** キーワードと *seconds* 引数は、再起動ルータから End Of Record（EOR）メッセージを受信した後で失効したルートを削除するまでルータが待機する時間の長さを決定します。デフォルト値は 360 秒です。

（注） BGP グレースフル リスタート機能をイネーブルにするには、リスタート タイマーと失効パス タイマーの設定は不要です。デフォルト値はほとんどのネットワーク構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds*]
5. **bgp graceful-restart** [**stalepath-time** *seconds*]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
ステップ 4	**bgp graceful-restart** [**restart-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart restart-time 130`	BGP グレースフル リスタート機能と BGP NSF 認識をイネーブルにします。 • **restart-time** 引数は、BGP OPEN メッセージを受信するまでピアルータが失効したルートを削除するために待機する時間の長さを決定します。 • デフォルト値は 120 秒です。指定できる範囲は 1 ～ 3600 秒です。 （注） この例では、この手順に適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 5	**bgp graceful-restart** [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart stalepath-time 350`	BGP グレースフル リスタート機能と BGP NSF 認識をイネーブルにします。 • **stalepath-time** 引数は、再起動ルータから End Of Record（EOR）メッセージを受信した後で失効したルートを削除するまでルータが待機する時間の長さを決定します。 • デフォルト値は 360 秒です。指定できる範囲は 1 ～ 3600 秒です。 （注） この例では、この手順に適用可能な構文だけが使用されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
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 モードを開始します。

次の作業

BGP セッションの確立後に **bgp graceful-restart** コマンドを実行する場合は、グレースフル リスタート機能を交換する前に、**clear ip bgp *** コマンドを実行するかルータをリロードすることによって、ピアセッションをリセットする必要があります。BGP セッションのリセットと **clear ip bgp** コマンドの使用に関する詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。

BGP ノンストップ フォワーディング認識の設定の確認

ルータで BGP NSF 認識のローカル設定を確認して、BGP ネットワーク内にあるピア ルータの NSF 認識の設定を確認するには、次の手順を使用します。

手順の概要

1. **enable**
2. **show running-config** [*options*]
3. **show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]]

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 show running-config [*options*]

ローカル ルータでの実行コンフィギュレーションを表示します。出力には、BGP セクションに **bgp graceful-restart** コマンドの設定が表示されます。すべての BGP ピアが BGP NSF 認識に対して設定されていることを確認するには、すべての BGP ネイバー ルータでこのコマンドを繰り返します。この例では、BGP グレースフル リスタートはグローバルにイネーブルになっており、192.168.1.2 にある外部ネイバーは BGP ピアとして設定されていて、BGP グレースフル リスタート機能がイネーブルになっています。

例：

```
Router# show running-config
.
.
.
router bgp 45000
 bgp router-id 172.17.1.99
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 130
 bgp graceful-restart stalepath-time 350
 bgp graceful-restart
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 activate
.
.
.
```

ステップ 3 show ip bgp neighbors [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]]

ネイバーへの TCP 接続および BGP 接続の情報を表示します。このルータとグレースフル リスタート機能を交換したネイバーごとに「Graceful Restart Capability: advertised」が表示されます。Cisco IOS Release

12.2(33)SRC、12.2(33)SB、またはそれ以降のリリースでは、個別の BGP ネイバー、ピア グループ、またはピア セッション テンプレートの BGP グレースフル リスタート機能をイネーブルまたはディセーブルにする機能が導入され、BGP グレースフル リスタートのステータスを示す出力がこのコマンドに追加されました。

Cisco IOS Release 12.2(33)SRC イメージを使用する次の部分的な出力例には、上の図のルータ C にある内部 BGP ネイバー 172.21.1.2 のグレースフル リスタート情報が表示されます。「Graceful-Restart is enabled」メッセージに注意してください。

例：

```
Router# show ip bgp neighbors 172.21.1.2

BGP neighbor is 172.21.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.22.1.1
  BGP state = Established, up for 00:01:01
  Last read 00:00:02, last write 00:00:07, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    Graceful Restart Capability: advertised
    Multisession Capability: advertised and received
!
  Address tracking is enabled, the RIB does have a route to 172.21.1.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 secs
```

BGP NSF 認識の設定例

例：グレースフル リスタートを使用した BGP グローバル NSF 認識の有効化

次の例では、すべての BGP ネイバーで BGP NSF 認識をグローバルにイネーブルにします。リスタート時間は 130 秒に設定され、失効パス時間は 350 秒に設定されます。これらのタイマーの設定は任意であり、ほとんどのネットワーク配置では設定済みのデフォルト値が最適です。

```
configure terminal
 router bgp 45000
 bgp graceful-restart
 bgp graceful-restart restart-time 130
 bgp graceful-restart stalepath-time 350
 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』
BGP コマンド	『Cisco IOS IP Routing: BGP 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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

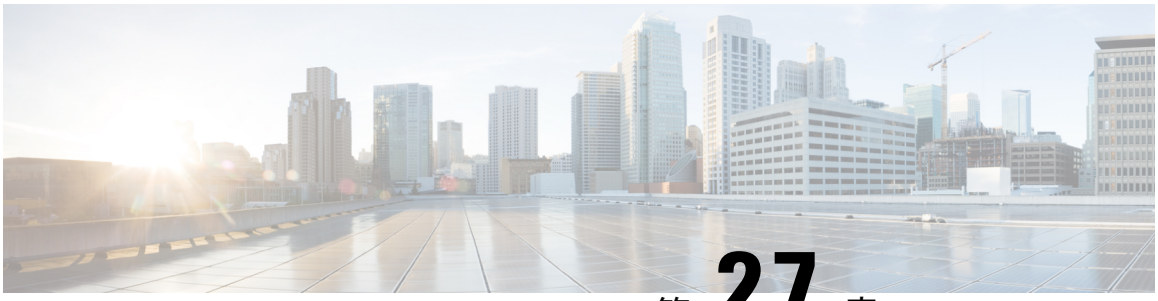
BGP NSF 認識の機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *42 : BGP NSF* 認識の機能情報

機能名	リリース	機能情報
BGP NSF 認識		ノンストップ フォワーディング（NSF）認識を使用すると、デバイスは、NSF 対応ネイバーがステートフル スイッチオーバー（SSO）操作中にパケットの転送を続行できるようにします。BGP ノンストップ フォワーディング認識機能では、BGP を実行している NSF 認識デバイスが、SSO 操作を実行しているデバイスのすでに認識されているルートとともにパケットを転送できます。この機能によって、障害が発生したデバイスの BGP ピアが、そのようなデバイスによってアドバタイズされたルーティング情報を保持して、障害が発生したデバイスが通常の動作に戻ってルーティング情報を交換できるようになるまでこの情報を引き続き使用できるようになります。ピアリング セッションは、NSF 操作全体を通じて維持されます。 次のコマンドが導入または変更されました。**bgp graceful-restart**、**show ip bgp**、**show ip bgp neighbors**



第 27 章

ネイバーごとのBGPグレースフルリスタート

BGPグレースフルリスタート機能は、すでにグローバルに利用可能です。ネイバーごとのBGPグレースフル リスタート機能により、個々のネイバーについてBGPグレースフル リスタートを有効または無効にすることができ、ネットワークの柔軟性やサービスが向上します。

- 機能情報の確認 （589 ページ）
- ネイバーごとの BGP グレースフル リスタートに関する情報 （590 ページ）
- ネイバーごとの BGP グレースフル リスタートの設定方法 （591 ページ）
- ネイバーごとの BGP グレースフル リスタートの設定例 （603 ページ）
- その他の参考資料 （604 ページ）
- ネイバーごとの BGP グレースフル リスタートの機能情報 （605 ページ）

機能情報の確認

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

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

ネイバーごとのBGPグレースフルリスタートに関する情報

ネイバーごとの BGP グレースフル リスタート

BGP ネイバーごとに BGP グレースフル リスタートを有効または無効にする機能が導入されました。既存のグローバル BGP グレースフル リスタート設定に加えて、BGP ピアの BGP グレースフル リスタートを設定するための 3 つの新しい方法が使用可能になりました。BGP ピアまたは BGP ピア グループのグレースフル リスタートは、**neighbor ha-mode graceful-restart** コマンドを使用して有効または無効にできます。または、BGP ピアは、**ha-mode graceful-restart** コマンドを使用して、BGP ピア セッション テンプレートからグレースフル リスタート設定を継承できます。

BGP グレースフル リスタートはデフォルトではディセーブルになっていますが、既存のグローバル コマンドによって、機能に関係なくすべての BGP ネイバーでグレースフル リスタートがイネーブルになります。個別の BGP ネイバーの BGP グレースフル リスタートをイネーブルまたはディセーブルにする機能によって、ネットワーク管理者の制御レベルが上がります。

個別のネイバーで BGP グレースフル リスタート機能が設定されている場合は、グレースフル リスタートを設定するためのそれぞれの方法のプライオリティは同じであり、最後の設定インスタンスがネイバーに適用されます。たとえば、グローバル グレースフル リスタートがすべての BGP ネイバーでイネーブルになっていても、その後個々のネイバーが、グレースフル リスタートがディセーブルになっているピア グループのメンバとして設定されると、そのネイバーのグレースフル リスタートはディセーブルになります。

リスタート タイマーと失効パス タイマーの設定は、グローバル **bgp graceful-restart** コマンドでのみ使用可能ですが、**neighbor ha-mode graceful-restart** コマンドまたは **ha-mode graceful-restart** コマンドが設定されているときはデフォルト値が設定されます。デフォルト値はほとんどのネットワーク構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

BGP ピア セッション テンプレート

ピア セッション テンプレートは、一般的な BGP セッション コマンドの設定をグループ化して、セッションの設定要素を共有するネイバーのグループに適用するために使用されます。異なるアドレス ファミリで設定されているネイバーに共通する一般的なセッション コマンドは、同じピア セッション テンプレートに設定できます。ピア セッション テンプレートの作成と設定は、ピア セッション コンフィギュレーション モードで行います。ピア セッション テンプレートで設定できるのは、一般的なセッション コマンドだけです。

一般的なセッション コマンドをピア セッションで一度設定しておくと、ピア セッション テンプレートの直接適用、またはピア セッション テンプレートの間接継承によって、多数のネイバーに適用できます。ピア セッション テンプレートのコンフィギュレーションにより、自律

システム内のすべてのネイバーに共通に適用される一般的なセッション コマンドのコンフィギュレーションが簡素化されます。

ピア セッション テンプレートは、直接継承と間接継承をサポートします。BGP ネイバーは、一度に 1 つのピア セッション テンプレートだけを使用して設定でき、そのピア セッション テンプレートには、間接的に継承されたピア セッション テンプレートを 1 つだけ含めることができます。BGP ネイバーは、1 つのセッション テンプレートだけを直接継承でき、7 つまでの追加のピア セッション テンプレートを間接的に継承できます。

ピア セッション テンプレートでは継承がサポートされます。直接適用されたピア セッション テンプレートは、7つまでのピアセッションテンプレートから直接または間接的に設定を継承できます。そのため、合計で 8 個のピア セッション テンプレートをネイバーまたはネイバー グループに適用できます。

ピア セッション テンプレートは、一般的なセッション コマンドだけをサポートします。特定のアドレス ファミリ、または NLRI コンフィギュレーション モードだけのために設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

BGP ピア セッション テンプレートを使用して BGP グレースフル リスタートを有効または無効にする場合は、「BGP ピア セッション テンプレートを使用した BGP グレースフル リスタートの有効化と無効化」の項を参照してください。

ネイバーごとの BGP グレースフル リスタートの設定方法

個々の BGP ネイバーの BGP グレースフル リスタートのイネーブル化

上の図のルータ C にある内部 BGP ピアで BGP グレースフル リスタートを有効にするには、上の図のルータ B でこの作業を実行します。IPv4 アドレス ファミリで、ルータ C にあるネイバーが特定され、IP アドレスが 172.21.1.2 のルータ C にあるネイバーの BGP グレースフル リスタートが有効化されます。BGP グレースフル リスタートが有効になっていることを確認するには、オプションの **show ip bgp neighbors** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **activate**
7. **neighbor** *ip-address* **ha-mode graceful-restart** [**disable**]
8. **end**
9. **show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 172.21.1.2 remote-as 45000`	指定された自律システム内の BGP ネイバーとのピアリングを設定します。 • この例では、172.21.1.2 にある BGP ピアは内部 BGP ピアです。これは、BGP コンフィギュレーションが開始されているルータ（手順 3 を参照）と同じ自律システム番号が指定されているためです。
ステップ 6	**neighbor** *ip-address* **activate** 例：	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。

	コマンドまたはアクション	目的
	`Device(config-router-af)# neighbor 172.21.1.2 activate`	• この例では、172.21.1.2 にある内部 BGP ピアがアクティブにされます。
ステップ 7	**neighbor** *ip-address* **ha-mode graceful-restart** [**disable**] 例： `Device(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart`	BGP ネイバーの BGP グレースフル リスタート機能をイネーブルにします。 • BGP グレースフル リスタート機能を無効にするには、**disable** キーワードを使用します。 • BGP セッションの確立後にこのコマンドを入力する場合は、機能を BGP ネイバーと交換するためにセッションを再開する必要があります。 • この例では、172.21.1.2 にあるネイバーの BGP グレースフル リスタート機能はイネーブルになっています。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]] 例： `Device# show ip bgp neighbors 172.21.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このルータとグレースフル リスタート機能を交換したネイバーごとに「Graceful Restart Capability: advertised」が表示されます。 • この例では、172.21.1.2 にある BGP ピアに関する情報を表示するように出力がフィルタリングされます。

例

次に、172.21.1.2 にある BGP ピアに対する **show ip bgp neighbors** コマンドの部分的な出力例を示します。グレースフル リスタートはイネーブルになっていると表示されます。リスタート タイマーと失効パス タイマーのデフォルト値をメモします。これらのタイマーは、グローバル **bgp graceful-restart** コマンドを使用した場合だけ設定できます。

```
Device# show ip bgp neighbors 172.21.1.2

BGP neighbor is 172.21.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.22.1.1
  BGP state = Established, up for 00:01:01
```

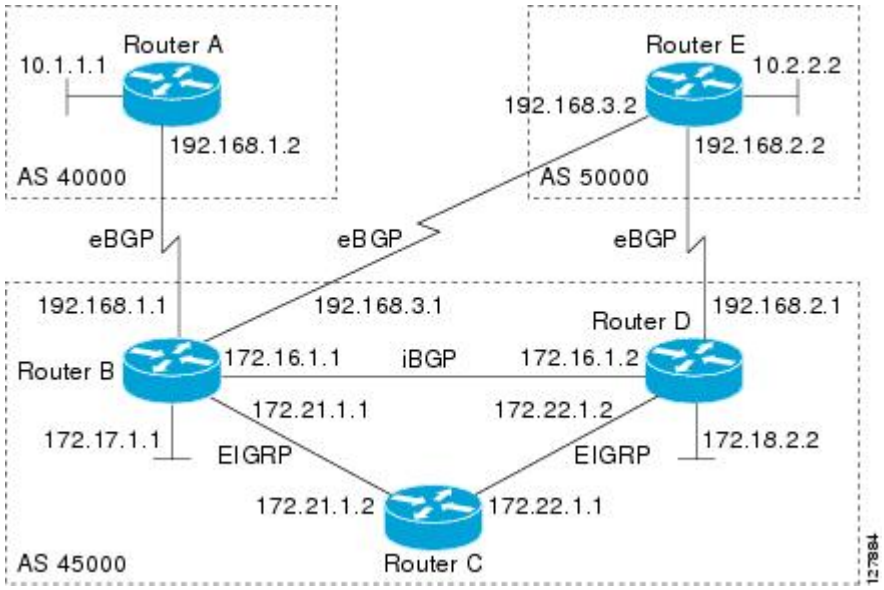
```
  Last read 00:00:02, last write 00:00:07, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    Graceful Restart Capability: advertised
    Multisession Capability: advertised and received
!
  Address tracking is enabled, the RIB does have a route to 172.21.1.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 secs
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

BGP ピア セッション テンプレートを使用した BGP グレースフル リスタートのイネーブル化とディセーブル化

この作業は、ピア セッション テンプレートを使用して BGP ネイバーの BGP グレースフル リスタートをイネーブルおよびディセーブルにする場合に実行します。この作業では、BGP ピア セッションテンプレートが作成され、BGP グレースフル リスタートがイネーブルにされます。別のピア セッション テンプレートが作成され、このテンプレートは BGP グレースフル リスタートをディセーブルにするよう設定されます。

この例では、下の図のルータ B で設定が実行され、2 つの外部 BGP ネイバー（ルータ A とルータ E）が識別されます。ルータ A にある最初の BGP ピアは、BGP グレースフル リスタートを有効にする最初のピア セッション テンプレートを継承するよう設定されます。一方、ルータ E にある 2 番目の BGP ピアは、BGP グレースフル リスタートを無効にする 2 番目のテンプレートを継承します。オプションの **show ip bgp neighbors** コマンドを使用して、この作業で設定される BGP ネイバーごとに BGP グレースフル リスタート機能のステータスを確認します。

図 *44 : BGP* ネイバーを示すネットワーク トポロジ



リスタート タイマーと失効パス タイマーは、グローバル **bgp graceful-restart** コマンドを使用した場合だけ変更できます。リスタート タイマーと失効パス タイマーは、BGP ネイバーの BGP グレースフル リスタートがピア セッション テンプレートを使用してイネーブルになっている場合はデフォルト値に設定されます。

（注） BGP ピアは、ピア ポリシー テンプレートまたはピア セッション テンプレートからの継承と、ピア グループ メンバとしての設定を同時に行うことはできません。BGP テンプレートと BGP ピア グループは同時に使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **ha-mode graceful-restart** [**disable**]
6. **exit-peer-session**
7. **template peer-session** *session-template-name*
8. **ha-mode graceful-restart** [**disable**]
9. **exit-peer-session**
10. **bgp log-neighbor-changes**
11. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
12. **neighbor** *ip-address* **inherit peer-session** *session-template-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **neighbor** *ip-address* **inherit peer-session** *session-template-number*

15. **end**
16. **show ip bgp template peer-session** [*session-template-number*]
17. **show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* 例： `Device(config-router)# template peer-session S1`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。 • この例では、S1 という名前のピア セッション テンプレートが作成されます。
ステップ 5	**ha-mode graceful-restart** [**disable**] 例： `Device(config-router-stmp)# ha-mode graceful-restart`	BGP グレースフル リスタート機能と BGP NSF 認識をイネーブルにします。 • BGP グレースフル リスタート機能を無効にするには、**disable** キーワードを使用します。 • BGP セッションの確立後にこのコマンドを入力する場合は、機能を BGP ネイバーと交換するためにセッションを再開する必要があります。 • この例では、S1 という名前のピア セッション テンプレートの BGP グレースフル リスタート機能はイネーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	**exit-peer-session** 例： `Device(config-router-stmp)# exit-peer-session`	セッション テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 7	**template peer-session** *session-template-name* 例： `Device(config-router)# template peer-session S2`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。 • この例では、S2 という名前のピア セッション テンプレートが作成されます。
ステップ 8	**ha-mode graceful-restart** [**disable**] 例： `Device(config-router-stmp)# ha-mode graceful-restart disable`	BGP グレースフル リスタート機能と BGP NSF 認識をイネーブルにします。 • BGP グレースフル リスタート機能を無効にするには、**disable** キーワードを使用します。 • BGP セッションの確立後にこのコマンドを入力する場合は、機能を BGP ネイバーと交換するためにセッションを再開する必要があります。 • この例では、S2 という名前のピア セッション テンプレートの BGP グレースフル リスタート機能はディセーブルになっています。
ステップ 9	**exit-peer-session** 例： `Device(config-router-stmp)# exit-peer-session`	セッション テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 10	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバーのステータス変更（アップまたはダウン）のロギングとネイバーのリセットをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。
ステップ 11	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例：	指定された自律システム内の BGP ネイバーとのピアリングを設定します。

	コマンドまたはアクション	目的
	`Device(config-router)# neighbor 192.168.1.2 remote-as 40000`	• この例では、192.168.1.2 にある BGP ピアは外部 BGP ピアです。これは、BGP コンフィギュレーションが開始されているルータ（手順3を参照）とは異なる自律システム番号が指定されているためです。
ステップ 12	**neighbor** *ip-address* **inherit peer-session** *session-template-number* 例： `Device(config-router)# neighbor 192.168.1.2 inherit peer-session S1`	ピア セッション テンプレートを継承します。 • この例では、S1 という名前のピア セッション テンプレートが継承され、ネイバーは BGP グレースフル リスタートのイネーブル化を継承します。
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.3.2 remote-as 50000`	指定された自律システム内の BGP ネイバーとのピアリングを設定します。 • この例では、192.168.3.2 にある BGP ピアは外部 BGP ピアです。これは、BGP コンフィギュレーションが開始されているルータ（手順3を参照）とは異なる自律システム番号が指定されているためです。
ステップ 14	**neighbor** *ip-address* **inherit peer-session** *session-template-number* 例： `Device(config-router)# neighbor 192.168.3.2 inherit peer-session S2`	ピア セッション テンプレートを継承します。 • この例では、S2 という名前のピア セッション テンプレートが継承され、ネイバーは BGP グレースフル リスタートのディセーブル化を継承します。
ステップ 15	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 16	**show ip bgp template peer-session** [*session-template-number*] 例： `Device# show ip bgp template peer-session`	（任意）ローカル設定のピアセッションテンプレートを表示します。 • *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

	コマンドまたはアクション	目的
ステップ 17	**show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]] 例： `Device# show ip bgp neighbors 192.168.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このルータとグレースフル リスタート機能を交換したネイバーごとに「Graceful Restart Capability: advertised」が表示されます。 • この例では、192.168.1.2 にある BGP ピアに関する情報を表示するように出力がフィルタリングされます。

例

次に、192.168.1.2（上の図のルータ A）にある BGP ピアに対する **show ip bgp neighbors** コマンドの部分的な出力例を示します。グレースフル リスタートはイネーブルになっていると表示されます。リスタート タイマーと失効パス タイマーのデフォルト値をメモします。これらのタイマーは、**bgp graceful-restart** コマンドを使用した場合だけ設定できます。

```
Device# show ip bgp neighbors 192.168.1.2

BGP neighbor is 192.168.1.2,  remote AS 40000, external link
 Inherits from template S1 for session parameters
  BGP version 4, remote router ID 192.168.1.2
  BGP state = Established, up for 00:02:11
  Last read 00:00:23, last write 00:00:27, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    Graceful Restart Capability: advertised
    Multisession Capability: advertised and received
!
Address tracking is enabled, the RIB does have a route to 192.168.1.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 secs
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

次に、192.168.3.2（上の図のルータ E）にある BGP ピアに対する **show ip bgp neighbors** コマンドの部分的な出力例を示します。グレースフル リスタートはディセーブルになっていると表示されます。

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
```

```
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
!
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

BGP ピア グループの BGP グレースフル リスタートのディセーブル化

この作業は、BGP ピア グループの BGP グレースフル リスタートをディセーブルにする場合に実行します。この作業では、BGP ピア グループが作成され、そのピア グループのグレースフル リスタートがディセーブルにされます。その後、BGP ネイバー（上の図の 172.16.1.2 にあるルータ D）が識別されてピア グループ メンバとして追加され、ピア グループと関連付けられた設定を継承します。この例では、BGP グレースフル リスタートは無効化されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** *peer-group-name* **remote-as** *autonomous-system-number*
7. **neighbor** *peer-group-name* **ha-mode graceful-restart** [**disable**]
8. **neighbor** *ip-address* **peer-group** *peer-group-name*
9. **end**
10. **show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics**| **received prefix-filter** | **policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレスファミリを指定します。デフォルトでは、**unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router-af)# neighbor PG1 peer-group`	BGP ピア グループを作成します。 • この例では、PG1 という名前のピア グループが作成されます。
ステップ 6	**neighbor** *peer-group-name* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor PG1 remote-as 45000`	指定された自律システム内の BGP ピア グループとのピアリングを設定します。 • この例では、PG1 という名前の BGP ピア グループが、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加されます。
ステップ 7	**neighbor** *peer-group-name* **ha-mode graceful-restart** [**disable**] 例： `Device(config-router-af)# neighbor PG1 ha-mode graceful-restart disable`	BGP ネイバーの BGP グレースフル リスタート機能をイネーブルにします。 • BGP グレースフル リスタート機能を無効にするには、**disable** キーワードを使用します。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。

	コマンドまたはアクション	目的
		• この例では、PG1 という名前の BGP ピア グループの BGP グレースフル リスタート機能はディセーブルになっています。
ステップ 8	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 172.16.1.2 peer-group PG1`	BGP ネイバーの IP アドレスをピア グループに割り当てます。 • この例では、172.16.1.2 にある BGP ネイバーピアが、PG1 という名前のピア グループのメンバとして設定されます。
ステップ 9	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics**| **received prefix-filter** | **policy** [**detail**]]] 例： `Device# show ip bgp neighbors 172.16.1.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、172.16.1.2 にある BGP ピアに関する情報を表示するように出力がフィルタ処理され、「Graceful-Restart is disabled」行には、このネイバーのグレースフル リスタート機能が無効化されていることが示されます。

例

次に、172.16.1.2 にある BGP ピアに対する **show ip bgp neighbors** コマンドの部分的な出力例を示します。グレースフル リスタートはディセーブルになっていると表示されます。リスタート タイマーと失効パス タイマーのデフォルト値をメモします。これらのタイマーは、グローバル **bgp graceful-restart** コマンドを使用した場合だけ設定できます。

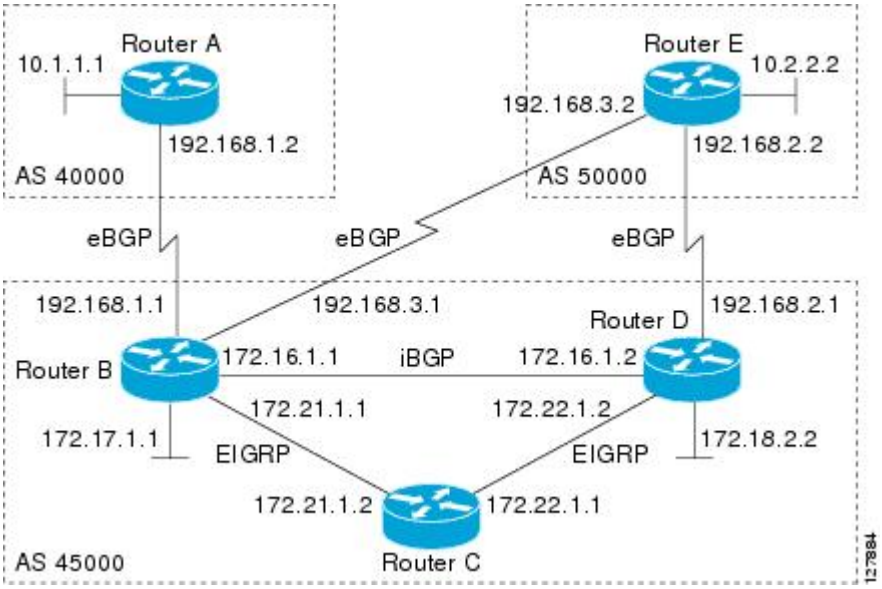
```
Device# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
 Member of peer-group PG1 for session parameters
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Neighbor sessions:
    0 active, is multisession capable
!
Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Connections established 0; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
```

ネイバーごとの BGP グレースフル リスタートの設定例

例：ネイバーごとの BGP グレースフル リスタートの有効化と無効化

個別の BGP ネイバー、ピア グループ、またはピア セッション テンプレートの BGP グレースフル リスタート機能を有効または無効にする機能が導入されました。次の例は、下の図のルータ B での設定で、S1 という名前の BGP ピア セッション テンプレートの BGP グレースフル リスタート機能を有効にして、S2 という名前の BGP ピア セッション テンプレートの BGP グレースフル リスタート機能を無効にします。ルータ A（192.168.1.2）にある外部 BGP ネイバーは、ピア セッション テンプレート S1 を継承し、このネイバーの BGP グレースフル リスタート機能は有効になります。ルータ E（192.168.3.2）にある別の外部 BGP ネイバーは、ピア セッション テンプレート S2 の継承後に、BGP グレースフル リスタート機能が無効化された状態で設定されます。

図 *45 : BGP* グレースフル リスタートについて *BGP* ネイバーを示すネットワーク トポロジ



個別の内部 BGP ネイバー（172.21.1.2 にあるルータ C）では BGP グレースフル リスタート機能は有効になっているのに対して、ルータ D（172.16.1.2）にある BGP ネイバーでは BGP グレースフル リスタートは無効になっています。これは、ピア グループ PG1 のメンバであるためです。BGP グレースフル リスタートのディセーブル化は、ピア グループ PG1 のすべてのメンバについて設定されます。リスタート タイマーと失効パス タイマーは変更され、BGP セッションがリセットされます。

```
router bgp 45000
 template peer-session S1
 remote-as 40000
 ha-mode graceful-restart
 exit-peer-session
 template peer-session S2
```

```
 remote-as 50000
 ha-mode graceful-restart disable
 exit-peer-session
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 150
 bgp graceful-restart stalepath-time 400
 address-family ipv4 unicast
 neighbor PG1 peer-group
 neighbor PG1 remote-as 45000
 neighbor PG1 ha-mode graceful-restart disable
 neighbor 172.16.1.2 peer-group PG1
 neighbor 172.21.1.2 remote-as 45000
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 ha-mode graceful-restart
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 inherit peer-session S1
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 inherit peer-session S2
 end
clear ip bgp *
```

BGP グレースフル リスタート機能の最後の設定インスタンスが適用される方法を示すには、次の例では、最初にすべての BGP ネイバーについて BGP グレースフル リスタート機能をグローバルにイネーブルにできます。BGP ピア グループである PG2 は、BGP グレースフル リスタート機能がディセーブルにされた状態で設定されます。個別の外部 BGP ネイバー（上の図の 192.168.1.2 にあるルータ A）は、ピア グループ PG2 のメンバとして設定されます。最後のグレースフル リスタート設定インスタンスが適用されます。この場合は、ネイバー 192.168.1.2 が、ピア グループ PG2 から設定インスタンスを継承し、このネイバーの BGP グレースフル リスタート機能は無効化されます。

```
router bgp 45000
 bgp log-neighbor-changes
 bgp graceful-restart
 address-family ipv4 unicast
 neighbor PG2 peer-group
 neighbor PG2 remote-as 40000
 neighbor PG2 ha-mode graceful-restart disable
 neighbor 192.168.1.2 peer-group PG2
 end
clear ip bgp *
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 4724	『*Graceful Restart Mechanism for BGP*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

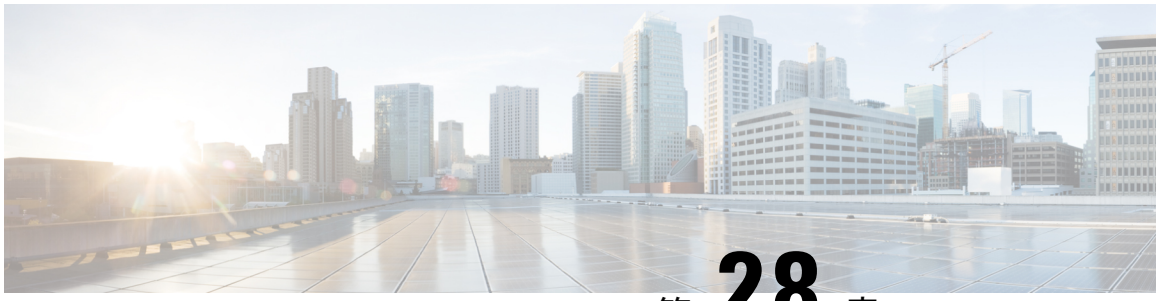
ネイバーごとのBGPグレースフルリスタートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *43 :* ネイバーごとの *BGP* グレースフル リスタートの機能情報

機能名	リリース	機能情報
ネイバーごとの BGP グレースフル リスタート		ネイバーごとの BGP グレースフル リスタート機能は、ピア セッション テンプレートと BGP ピア グループを含む個別の BGP ネイバーの BGP グレースフル リスタート機能をイネーブルまたはディセーブルにします。 この機能により、次のコマンドが導入されました。**ha-mode graceful-restart**、**neighbor ha-mode graceful-restart** この機能により、**show ip bgp neighbors** コマンドが変更されました。



第 28 章

BFD に対する BGP サポート

双方向フォワーディング検出（BFD）は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFDはネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用して、さまざまなルーティング プロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワークプロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。BGP 用の BFD を実装する主な利点は、再コンバージェンス時間が非常に短いことです。

- 機能情報の確認 （607 ページ）
- BFD に対する BGP サポートに関する情報 （608 ページ）
- BFD を使用した BGP コンバージェンス時間の短縮方法 （608 ページ）
- その他の参考資料 （612 ページ）
- BFD に対する BGP サポートの機能情報 （613 ページ）

機能情報の確認

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

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

BFD に対する BGP サポートに関する情報

BGP の BFD

双方向フォワーディング検出（BFD）は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFDはネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用して、さまざまなルーティング プロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワークプロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。BGP 用の BFD を実装する主な利点は、再コンバージェンス時間の著しい短縮です。

「BGP ネイバー セッション オプションの設定」の章の「BGP IPv6 ネイバーの BFD の設定」の項も参照してください。

BFD の詳細については、『*Cisco IOS IP Routing: BFD Configuration Guide*』を参照してください。

BFD を使用した BGP コンバージェンス時間の短縮方法

前提条件

- 関与するすべてのルータで Cisco Express Forwarding（CEF）と IP ルーティングをイネーブルにする必要があります。
- BFD を配置する前に、ルータで BGP を設定する必要があります。使用しているルーティングプロトコルの高速コンバージェンスを実装する必要があります。高速コンバージェンスの設定については、お使いのバージョンの Cisco IOS ソフトウェアの IP ルーティングのマニュアルを参照してください。

機能制限

- Cisco IOS Release15.1(1)SG での BGP に対する BFD サポートのシスコによる実装に関しては、非同期モードのみがサポートされています。非同期モードでは、どちらの BFD ピアも BFD セッションを開始できます。
- IPv6 カプセル化がサポートされています。
- BFD マルチホップがサポートされています。

BFD を使用した BGP コンバージェンス時間の短縮

インターフェイスで BFD を設定して、BFD プロセスを開始します。BFD プロセスの開始時に、隣接データベースにはエントリは作成されません。言い換えれば、BFD制御パケットは送受信されません。適用可能なルーティング プロトコルの BFD サポートを設定すると、隣接作成が実行されます。BGP コンバージェンス時間を短縮するために BGP に対する BFD サポートを実装するには、最初の 2 つの作業を設定する必要があります。3 番目の作業は、BFD のモニタまたはトラブルシューティングに役立つ任意の作業です。

「BGP ネイバー セッション オプションの設定」モジュールの「BGP IPv6 ネイバーの BFD の設定」の項も参照してください。

インターフェイスでの BFD セッション パラメータの設定

この手順では、インターフェイスで基本BFDセッションパラメータを設定することによって、インターフェイスで BFD を設定する方法を示します。BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface FastEthernet 6/0`	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	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*	インターフェイスで BFD 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： `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	
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 モードを終了します。

BGP に対する BFD サポートの設定

この作業は、BGP が BFD に登録済みのプロトコルになり、BFD から転送パス検出障害メッセージを受信するように、BGP に対する BFD サポートを設定する場合に実行します。

始める前に

- BGP は、関連するすべてのルータで実行する必要があります。
- BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **fall-over bfd**
5. **end**
6. **show bfd neighbors** [**details**]
7. **show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp tag1`	BGP プロセスを指定し、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	**neighbor** *ip-address* **fall-over bfd** 例： `Router(config-router)# neighbor 172.16.10.2 fall-over bfd`	フェールオーバーに対する BFD サポートをイネーブルにします。
ステップ 5	**end** 例： `Router(config-router)# end`	ルータを特権 EXEC モードに戻します。
ステップ 6	**show bfd neighbors** [**details**] 例： `Router# show bfd neighbors detail`	BFD ネイバーがアクティブになっていることを確認し、BFD が登録されているルーティング プロトコルを表示します。
ステップ 7	**show ip bgp neighbors** [*ip-address* [**received-routes** | **routes** | **advertised-routes** | **paths** [*regexp*] | **dampened-routes** | **flap-statistics** | **received prefix-filter** | **policy** [**detail**]]] 例： `Router# show ip bgp neighbors`	ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

BFD のモニタリングとトラブルシューティング

BFD のモニタリングまたはトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

手順の概要

1. **enable**
2. **show bfd neighbors** [**details**]
3. **debug bfd** [**event** | **packet** | **ipc-error** | **ipc-event** | **oir-error** | **oir-event**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show bfd neighbors** [**details**] 例： `Router# show bfd neighbors details`	（任意）BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。
ステップ 3	**debug bfd** [**event** | **packet** | **ipc-error** | **ipc-event** | **oir-error** | **oir-event**] 例： `Router# debug bfd packet`	（任意）BFD パケットのデバッグ情報を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BFD コマンド	『Cisco IOS IP Routing: Protocol Independent Command Reference』
別のルーティング プロトコルに対する BFD サポートの設定	『IP Routing: BFD Configuration Guide』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

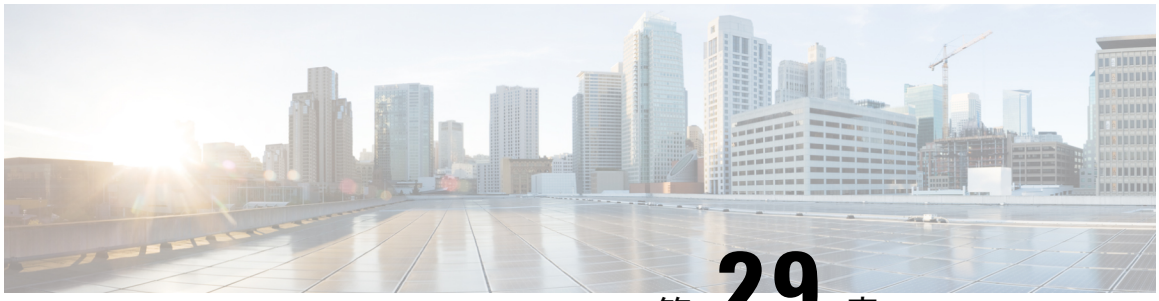
BFD に対する BGP サポートの機能情報

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、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *44 : BFD* に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
BFD に対する BGP サポート		双方向フォワーディング検出（BFD）は、すべてのメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、さまざまなルーティング プロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。BGP 用の BFD を実装する主な利点は、再コンバージェンス時間が非常に短いことです。 この機能により、次のコマンドが導入または変更されました。**bfd**、**neighbor fall-over**、**show bfd neighbors**、**show ip bgp neighbors**



第 29 章

MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタート

- 機能情報の確認 （615 ページ）
- MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートに関する情報（616 ページ）
- MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定方法（616 ページ）
- MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定例 （617 ページ）
- その他の参考資料 （618 ページ）
- MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの機能情報（619 ページ）

機能情報の確認

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

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

MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートに関する情報

MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート

グレースフル リスタート機能は、IPv6 BGP ユニキャスト、IPv6 BGP マルチキャスト、および VPNv6 アドレス ファミリでサポートされており、BGP IPv6 用の Cisco ノンストップ フォワーディング（NSF）機能をイネーブルにします。BGP グレースフル リスタート機能を使用すると、TCP 状態を維持することなく、BGP ルーティング テーブルをピアから回復できます。

NSF では、ルーティング プロトコルのコンバージェンス時にも引き続きパケットが転送されるため、スイッチオーバー時のルート フラップが回避されます。転送は、アクティブ RP とスタンバイ RP 間で FIB を同期することで維持されます。スイッチオーバー時、転送は FIB を使用して維持されます。RIB の同期は維持されないため、RIB はスイッチオーバー時に空になります。RIB は、ルーティング プロトコルによって再入力され、次に、NSF_RIB_CONVERGED レジストリ コールを使用して RIB コンバージェンスに関する情報を FIB に伝えますFIB テーブルは、RIB から更新され、古いエントリが削除されます。RIB は、ルーティング プロトコルが RIB のコンバージェンスの通知に失敗した場合、RP スイッチオーバー時にフェールセーフ タイマーを開始します。

Cisco BGP Address Family Identifier（AFI）モデルは、モジュラ式でスケーラブルな設計となっており、複数の AFI 設定および Subsequent Address Family Identifier（SAFI）設定をサポートするように設計されています。

MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定方法

IPv6 BGP グレースフル リスタート機能の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] 例： `Device(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定します。
ステップ 5	**bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**] 例： `Device(config-router-af)# bgp graceful-restart`	BGP グレースフル リスタート機能をイネーブルにします。

MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの設定例

例：IPv6 BGP グレースフル リスタート機能の設定

次の例では、BGP グレースフル リスタート機能が有効になっています。

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv6
Device(config-router-af)# bgp graceful-restart
```

次の例では、再起動タイマーが 130 秒に設定されています。

```
Device# configure terminal
Device(config)# router bgp 65000
```

```
Device(config-router)# address-family ipv6
Device(config-router-af)# bgp graceful-restart restart-time 130
```

次の例では、stalepath タイマーが 350 秒に設定されています。

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv6
Device(config-router-af)# bgp graceful-restart stalepath-time 350
```

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 Command List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MB	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

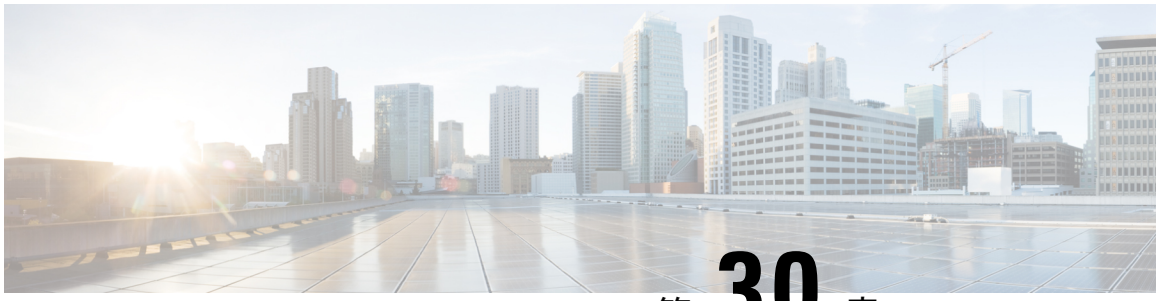
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタートの機能情報

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 *45 : MP-BGP IPv6* アドレス ファミリの *IPv6 NSF* およびグレースフル リスタートの機能情報

機能名	リリース	機能情報
MP-BGP IPv6 アドレス ファミリの IPv6 NSF およびグレースフル リスタート	Cisco IOS XE Release 3.1	グレースフル リスタート機能は、Pv6 BGP ユニキャスト、マルチキャスト、および VPNv6 アドレス ファミリでサポートされ、BGP IPv6 で Cisco NSF 機能を実現しています。BGP グレースフル リスタート機能を使用すると、TCP 状態を維持することなく、BGP ルーティング テーブルをピアから回復できます。



第 30 章

BGP パーシステンス

BGP パーシステンスにより、ルータは、ネイバー セッションがダウンしている場合でも、設定されたネイバーから学習したルートを保持できます。BGP パーシステンスは、長期的グレースフル リスタート（LLGR）とも呼ばれます。LLGR は、グレースフル リスタート（GR）の終了後に有効になります。

- BGP パーシステンスの制約事項 （621 ページ）
- BGP パーシステンスの概要 （621 ページ）
- BGP パーシステンスの設定方法 （623 ページ）
- BGP パーシステンスの確認 （624 ページ）
- BGP パーシステンスの機能情報 （626 ページ）

BGP パーシステンスの制約事項

- マルチキャスト アドレスファミリでは、LLGR はサポートされていません。

BGP パーシステンスの概要

ネイバーから受信した BGP パスは、セッションがダウンしていることが検出されるとすぐに削除されます。この動作は、現在のネットワーク状態に合わせて BGP テーブルと転送テーブルを最新の状態に保つことを目的としています。結果として、これにより、トラフィック ブラックホールやルーティング ループの発生を防ぐことができます。ただし、シナリオによっては、コントロール プレーンの障害時にルートを長期間保持することで、IP の影響を受けにくいサービスを中断なしにより長い期間継続できるようになります。次のシナリオでは、BGP ネイバーの障害時に BGP ルートが長期間保存されていても、トラフィック フローが影響を受けることはありません。

- ルート アドバタイズメント パスが転送パスと異なる場合（つまり、MPLS トンネル経由）。たとえば、VPN ルートなどです。

- ルートアドバタイズメントの目的が設定をプッシュすることである場合（つまり、ルータ上でのフィルタプログラミング）。たとえば、フロースペック、ルートターゲットなどです。
- ルート アドバタイズメントが自動検出に使用される場合。たとえば、VPLS などです。

BGP パーシステンスにより、ローカル ルータは、ネイバー セッションがダウンしている場合でも、設定されたネイバーから学習したルートを保持できます。BGP パーシステンスは、長期的グレースフル リスタート（LLGR）とも呼ばれます。LLGR は、グレースフル リスタート（GR）の終了後に有効になります。LLGR は、LLGR の失効タイマーが期限切れになったとき、またはネイバーがルートを送信した後に End-of-RIB マーカーを送信したときに終了します。ネイバーの LLGR が終了すると、そのネイバーからのルートのうち、LLGR の失効状態のままであるルートはすべて削除されます。LLGR 機能は、BGP OPEN メッセージでネイバーに通知されます（設定されている場合）。BGP パーシステンスでは、パスは非常に長い期間（数日）保持され、グレースフル リスタートの動作とは異なり、パスのプリファレンス設定が解除されるため、非失効パスが失効パスよりも優先して選択されます。

BGP スピーカーは、LLGR を使用して設定されたすべてのアドレスファミリを含む LLGR 機能をアドバタイズします。LLGR の失効時間はアドレスファミリごとに設定されます。BGP パーシステンス機能は、次のアドレス ファミリ インジケータ（AFI）でサポートされています。

- VPNv4 と VPNv6
- フロー スペック（IPv4、IPv6、VPNv4、VPNv6）

BGP パーシステンスでは、パスは非常に長い期間（数日）保持され、基本的なグレースフル リスタートの動作とは異なり、パスのプリファレンス設定が解除されるため、常に非失効パスが失効パスよりも優先して選択されます。ネイバーがダウンすると、まず、次の手順で構成される従来のグレースフル リスタートが実行されます。

- グレースフル リスタート タイマーを開始する
- そのネイバーからのプレフィックスを失効としてマークする

パーシステンスは、グレースフル リスタートの完了後にのみ、ヘルパー ルータによって実行されます。パーシステンスは、ネイバーが End-of-Row（EoR; エンドオブロー）を送信したとき、またはパーシステンス タイマーが期限切れになったときに終了します。

リスタート ルータ

パーシステンスを設定するためのパーシステンス（LLGR）ネイバー設定ノブをサポートするには、グレースフル リスタート設定が必須です。パーシステンス タイマーに指定できる値の範囲は 0 ～ 4294967 です。

ヘルパー ルータ

ヘルパー ルータは、グレースフル リスタートが完了するとパーシステンスを実行します。次の作業を行います。

- パーシステンス タイマーを開始します。
- ネイバーから学習したプレフィックスを **long-lived stale path** としてマークします。
- ベスト パス計算を実行して、存続期間の長い失効パスのプリファレンス設定を解除します。存続期間の長い失効パスしかルートにない場合は、そのパスがベストパスとして選択されます。存続期間の長い失効パスがルートに複数ある場合は、ベストパスを見つけるために通常のタイブレーク処理が実行されます。
- LLGR 対応として設定されたすべてのネイバーに対して、存続期間の長い失効パスを、LLGR_STALE（65535:6）コミュニティ属性付きのベスト パスまたは追加パスとして再アドバタイズします。
- 非 LLGR 対応のネイバーから存続期間の長い失効ルートを取り消します。

ヘルパー ルータのピア

ヘルパー ルータのネイバーは、LLGR 対応である場合、受信した LLGR_STALE コミュニティ属性付きのルートについて以下を実行します。

- 受信したLLGR_STALEコミュニティ属性付きルートのプリファレンス設定を解除します。
- LLGR_STALE コミュニティ属性付きのパスを、ベスト パスまたは追加パスとして、同じ LLGR_STALE 属性が付加された LLGR 対応ルータに再アドバタイズします。
- ルート取り消しメッセージを非 LLGR 対応のルータに送信します。

BGP パーシステンスの設定方法

BGP パーシステンスの設定

```
Device# configure terminal
Device(config)# router bgp AS
Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor neighbor -id
Device(config-router-af-nbr)# bgp long-lived-graceful-restart {stale-time send time accept time}
```

- **bgp long-lived-graceful-restart**：ネイバーに対して長期的グレースフル リスタートのサポートを有効にします。
- **stale-time**：存続期間の長い失効ルートを消去するまでの最大待機時間を指定します。ネイバー ルータがこの機能についてネゴシエートし、accept ノブがローカルで設定されている場合は、これらの 2 つの値のうち、より小さい値が、存続期間の長さによる失効時間として使用されます。

- **send** ***time***：機能で送信される失効時間（stale-time）を指定します。指定範囲は 0 ～ 4294967 秒です。
- **accept** ***time***：ネイバーから受け入れ可能な最大失効時間を指定します。指定範囲は 0 ～ 4294967 秒です。BGP スピーカーは、LLGR 対応ネイバーのヘルパーとして機能します。ただし、accept ノブの設定により、非 LLGR 対応ネイバーのヘルパーとして機能することもできます。その場合は、このノブで設定された値が、存続期間の長さによる失効時間として使用されます。

次に、例を示します。

```
router bgp 1
 address-family vpnv4
  neighbor 1.1.1.1
   long-lived-graceful-restart stale-time send 300 accept 300
   long-lived-graceful-restart stale-time accept 300
```

BGP パーシステンスの確認

1. LLGR機能のアドバタイズおよび受信ステータスを確認するには、**show ip bgp vpnv4 unicast neighbors** *neighbor-id* コマンドを使用します。

```
show ip bgp vpn4 unicast neighbors 1.1.1.1
……
BGP neighbor is 1.1.1.1,  remote AS 1, internal link
 Description: test1
 …….
Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 10 seconds
      Address families advertised by peer:
        none
      Address families advertised by peer before restart:
        none
    Long-lived Graceful Restart Capability:
        VPNv4 Unicast: advertised and received(was preserved)
        VPNv6 Unicast: received(was preserved)
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1

For address family: VPNv4 Unicast
  Session: 1.1.1.1
……
……
Long-lived Graceful-Restart(was preserved)
    Stalepath-time: sent 2000s, received 50s, accepted 2000s, used 50s
```

2. ピアの再起動を確認するには、**show ip bgp vpnv4 unicast neighbors** *neighbor-id* コマンドを使用します。

```
show ip bgp vpn4 unicast neighbors 1.1.1.1
..............
 BGP neighbor is 1.1.1.1,  remote AS 1, internal link
 Description: test1
..............
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active, down for 00:00:23
  Configured hold time is 15, keepalive interval is 5 seconds
  Minimum holdtime from neighbor is 0 seconds
  Neighbor sessions:
    0 active, is not multisession capable (disabled)
    Stateful switchover support enabled: NO for session 0
  Message statistics:
    InQ depth is 0
…….
…….
For address family: VPNv4 Unicast
  Session: 1.1.1.1
……
……
Long-lived Graceful-Restart
    Stalepath-time: sent 2000s, accepted 2000s, used 2000s
    Stalepath-timer running 37s remaining
```

3. 存続期間の長い失効ルートとしてマークされたルートを確認するには、**show ip bgp vpnv4 all** コマンドを使用します。

```
Device# show ip bgp vpnv4 all
BGP table version is 33, local router ID is 19.19.19.19
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
        L long-lived-stale-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 2:2 (default for vrf example)
 *L>i 20.0.0.0/16      1.1.88.1                 0    100      0 81 ?
 *Li  38.1.1.0/24      1.1.88.1                 0    100      0 81 ?
 *L>i 180.180.180.180/32
                       1.1.88.1                 0    100      0 81 ?

Router#show ip bgp vpnv4 all 20.0.0.0/16
BGP routing table entry for 2:2:20.0.0.0/16, version 9
Paths: (1 available, best #1, table example)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  81 (long-lived-stale), imported path from 5:5:20.0.0.0/16 (global)
    1.1.88.1 (metric 40) (via default) from 1.1.1.188 (1.1.1.188)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Community: 100:100
      Extended Community: RT:1:1
      Originator: 1.1.88.1, Cluster list: 1.1.1.188
      mpls labels in/out nolabel/44
      rx pathid: 0, tx pathid: 0x0
```

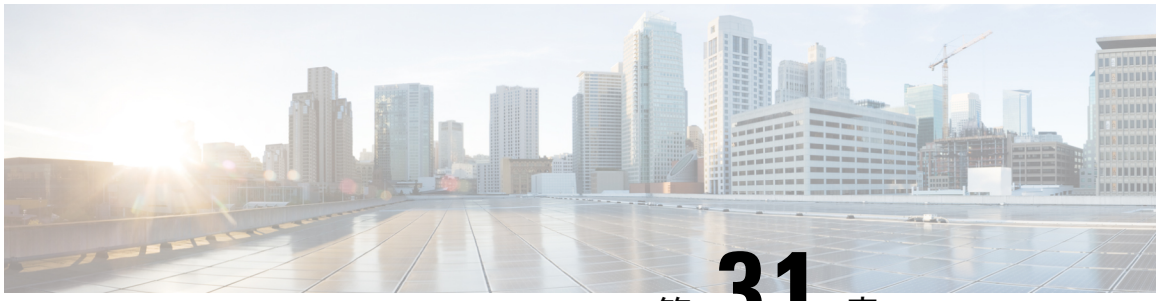
BGP パーシステンスの機能情報

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

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

表 *46 : BGP* パーシステンスの機能情報

機能名	リリース	機能の設定情報
BGP パーシステンス	Cisco IOS XE Fuji 16.7.1	BGP パーシステンスにより、ルータは、ネイバーセッションがダウンした後でも、設定されたネイバーから学習したルートを保持できます。BGP パーシステンスは、長期的グレースフル リスタート（LLGR）とも呼ばれます。 次のコマンドが変更されました。**address-family vpnv4**、**bgp long-lived-graceful-restart** {*stale-time send time accept time*}、 **neighbor** *neighbor-id*、**router bgp** *AS*、**show ip bgp vpnv4 all**、**show ip bgp vpnv4 unicast neighbors** <*neighbor-id*>



第 31 章

BGP リンク帯域幅

ボーダー ゲートウェイ プロトコル（BGP）リンク帯域幅機能は、拡張コミュニティとして自律システムの出口リンクの帯域幅をアドバタイズするために使用されます。この機能は、直接接続された外部 BGP（eBGP）ネイバー間のリンクに設定されます。このリンク帯域幅拡張コミュニティ リンク属性は、拡張コミュニティ交換がイネーブルなとき、内部 BGP（iBGP）ピアに伝播します。この機能は、BGP マルチパス機能とともに帯域幅が異なるリンクのロードバランシングを設定するために使用されます。

- 機能情報の確認 （627 ページ）
- BGP リンク帯域幅の前提条件 （628 ページ）
- BGP リンク帯域幅の制約事項 （628 ページ）
- BGP リンク帯域幅に関する情報 （628 ページ）
- BGP リンク帯域幅の設定法 （629 ページ）
- BGP リンク帯域幅の設定例 （631 ページ）
- その他の参考資料 （635 ページ）
- BGP リンク帯域幅の機能情報 （637 ページ）

機能情報の確認

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

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

BGP リンク帯域幅の前提条件

- BGP ロードバランシングまたはマルチパス ロードバランシングは、BGP リンク帯域幅機能をイネーブルにする前に設定する必要があります。
- リンク帯域幅属性のアドバタイズ先の iBGP ネイバー間で、BGP 拡張コミュニティ交換がイネーブルになっている必要があります。
- 関係するルータすべてで、Cisco Express Forwarding または分散型 Cisco Express Forwarding が有効になっている必要があります。

BGP リンク帯域幅の制約事項

- BGP リンク帯域幅機能は、IPv4 および VPNv4 アドレス ファミリ セッションだけで設定できます。
- BGP は、eBGP ネイバーに直接接続されたリンクにだけ、リンク帯域幅コミュニティを発信できます。
- iBGP および eBGP ロードバランシングは、IPv4 および VPNv4 アドレス ファミリでサポートされます。ただし、eiBGP ロード バランシングは VPNv4 アドレス ファミリだけでサポートされます。

BGP リンク帯域幅に関する情報

BGP リンク帯域幅の概要

BGP リンク帯域幅機能は、帯域幅容量の異なる外部リンクのマルチパス ロード バランシングをイネーブルにするために使用されます。この機能は、IPv4 または VPNv4 アドレス ファミリで、**bgp dmzlink-bw** コマンドを入力すると有効になります。この機能は、iBGP、eBGP マルチパス ロードバランシングおよびマルチプロトコル ラベル スイッチング（MPLS）の VPN での eiBGP マルチパス ロードバランシングをサポートしています。この機能がイネーブルなとき、直接接続された外部ネイバーから学習したルートは、発信元外部リンクの帯域幅を持つ内部 BGP（iBGP）ネットワークを通じて伝播します。

リンク帯域幅拡張コミュニティは、帯域幅に関して自律システム出口リンクを優先します。**neighbor dmzlink-bw** コマンドを入力することにより、直接接続された eBGP ピア間の外部リンクにこの拡張コミュニティが適用されます。リンク帯域幅拡張コミュニティ属性は、**neighbor send-community** コマンドで拡張コミュニティ交換が有効化されたとき、iBGP ピアに伝播します。

リンク帯域幅拡張コミュニティの属性

リンク帯域幅拡張コミュニティの属性は 4 バイトの値で、2 つのシングル ホップ eBGP ピアを接続する非武装地帯（DMZ）インターフェイスのリンクを設定します。リンク帯域幅拡張コミュニティの属性は、トラフィックがフォワーディングされる際、他のパスに相対的なトラフィック共有値として使用されます。重み、ローカル プリファレンス、as-path 長、Multi Exit Discriminator（MED）、および内部ゲートウェイ プロトコル（IGP）のコストが同一である場合、2 つのパスはロード バランシングが等しいとされます。

BGP リンク帯域幅機能の利点

BGP リンク帯域幅機能により、iBGP または eBGP が学習した複数のパス全体にトラフィックを送信するように BGP を設定することができます。ここで、送信されるトラフィックは自律システムを終了するために使用されるリンクの帯域幅に比例します。この機能の設定を eBGP および iBGP マルチパス機能とともに使用し、複数のリンク全体にわたる、同等でないコスト ロード バランシングをイネーブルにすることができます。BGP リンク帯域幅機能が追加されるまで、BGP では、同等でない帯域幅にわたる同等でないコスト ロード バランシングは不可能でした。

BGP リンク帯域幅の設定法

BGP リンク帯域幅の設定

BGP リンク帯域幅機能を設定するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]
5. **bgp dmzlink-bw**
6. **neighbor** *ip-address* **dmzlink-bw**
7. **neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**]
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	**enable** 例：	特権 EXEC モードなど、高位の権限レベルを有効にします。

	コマンドまたはアクション	目的
	`Router> 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： `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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 50000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**] 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。 • BGP リンク帯域幅機能は、IPv4 および VPNv4 アドレス ファミリだけでサポートされます。
ステップ 5	**bgp dmzlink-bw** 例： `Router(config-router-af)# bgp dmzlink-bw`	リンクの帯域幅に比例してトラフィックを配分するように BGP を設定します。 • このコマンドは、マルチパス ロード バランシングに使用される外部インターフェイスを含むルータごとに入力する必要があります。

ステップ 6	**neighbor** *ip-address* **dmzlink-bw**
	例：
	`Router(config-router-af)#`
	`neighbor 172.16.1.1 dmzlink-bw`
		外部インターフェイスが指定したIPアドレスから学習したルートのリンク帯域幅属性を含めるように BGP を設定します。
		• このコマンドは、マルチパスとして設定する eBGP リンクごとに設定する必要があります。このコマンドをイネーブルにすることにより、リンク帯域幅拡張コミュニティを通じて外部リンクの帯域幅を伝播することができます。

ステップ 7	**neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**] 例： `Router(config-router-af)# neighbor 10.10.10.1 send-community extended`	（任意）コミュニティまたは拡張コミュニティ、あるいはその両方が指定されたネイバーを交換できるようにします。 • このコマンドは、リンク帯域幅拡張コミュニティの属性が伝播する iBGP ピア用に設定する必要があります。
ステップ 8	**end** 例：	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-router-af)# end`	

BGP リンク帯域幅設定の確認

BGP リンク帯域幅機能を確認するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **show ip bgp** *ip-address* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*mask-length*]]
3. **show ip route** [[*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*] | [**static download**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp** *ip-address* [**longer-prefixes** [**injected**]	**shorter-prefixes** [*mask-length*]] 例： `Router# show ip bgp 10.0.0.0`	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。 • 出力として、リンク帯域幅設定のステータスを表示します。リンクの帯域幅の単位はキロバイト（KB）です。
ステップ 3	**show ip route** [[*ip-address* [*mask*] [**longer-prefixes**]]	[*protocol* [*process-id*]]	[**list** *access-list-number*	*access-list-name*]	[**static download**]] 例： `Router# show ip route 10.0.0.0`	ルーティングテーブルの現在の状態を表示します。 • 出力として、トラフィック シェア値を表示します。これには、各リンクの帯域幅に比例してトラフィックを誘導するために使用される、リンクの重み付けも含まれます。

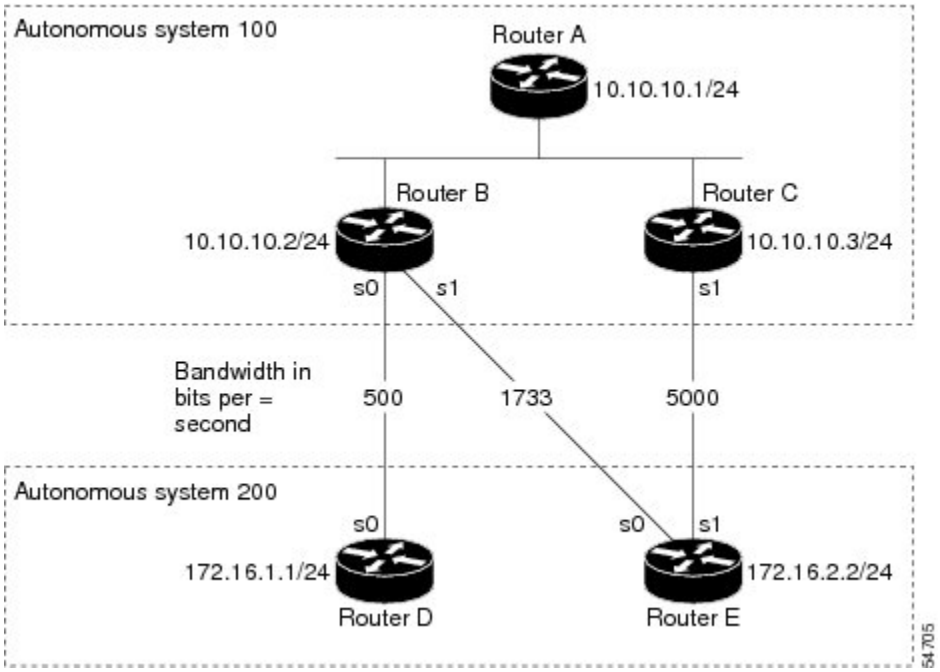
BGP リンク帯域幅の設定例

BGP リンク帯域幅設定の例

次の例では、BGP が各外部リンクの帯域幅に比例したトラフィックを配分するように BGP リンク帯域幅機能を設定します。下の図に、それぞれ帯域幅の異なる 3 つのリンク（コストが同

等でないリンク）で結合された 2 つの外部自律システムを示します。マルチパス ロード バランシングが有効になっており、トラフィックに比例してバランスされています。

図 *46 : BGP* リンク帯域幅の設定



ルータ A の設定

次の例では、iBGP マルチパス ロードバランシングをサポートし、BGP 拡張コミュニティ属性を iBGP ネイバーと交換するようにルータ A を設定します。

```
Router A(config)# router bgp 100

Router A(config-router)# neighbor 10.10.10.2 remote-as 100

Router A(config-router)# neighbor 10.10.10.2 update-source Loopback 0

Router A(config-router)# neighbor 10.10.10.3 remote-as 100

Router A(config-router)# neighbor 10.10.10.3 update-source Loopback 0

Router A(config-router)# address-family ipv4

Router A(config-router)# bgp dmzlink-bw
Router A(config-router-af)# neighbor 10.10.10.2 activate

Router A(config-router-af)# neighbor 10.10.10.2 send-community both

Router A(config-router-af)# neighbor 10.10.10.3 activate

Router A(config-router-af)# neighbor 10.10.10.3 send-community both

Router A(config-router-af)# maximum-paths ibgp 6
```

ルータ B の設定

次の例では、マルチパス ロード バランシングをサポートし、ルータ D およびルータ E にそれぞれのリンクの帯域幅に比例したトラフィックを配分し、これらのリンクの帯域幅を拡張コミュニティの iBGP ネイバーにアドバタイズするようにルータ B を設定します。

```
Router B(config)# router bgp 100

Router B(config-router)# neighbor 10.10.10.1 remote-as 100

Router B(config-router)# neighbor 10.10.10.1 update-source Loopback 0

Router B(config-router)# neighbor 10.10.10.3 remote-as 100

Router B(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router B(config-router)# neighbor 172.16.1.1 remote-as 200

Router B(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router B(config-router)# neighbor 172.16.2.2 remote-as 200

Router B(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router B(config-router)# address-family ipv4

Router B(config-router-af)# bgp dmzlink-bw

Router B(config-router-af)# neighbor 10.10.10.1 activate

Router B(config-router-af)# neighbor 10.10.10.1 next-hop-self

Router B(config-router-af)# neighbor 10.10.10.1 send-community both

Router B(config-router-af)# neighbor 10.10.10.3 activate

Router B(config-router-af)# neighbor 10.10.10.3 next-hop-self

Router B(config-router-af)# neighbor 10.10.10.3 send-community both

Router B(config-router-af)# neighbor 172.16.1.1
 activate
Router B(config-router-af)# neighbor 172.16.1.1 dmzlink-bw

Router B(config-router-af)# neighbor 172.16.2.2 activate
Router B(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router B(config-router-af)# maximum-paths ibgp 6
Router B(config-router-af)# maximum-paths 6
```

ルータ C の設定

次の例では、マルチパス ロード バランシングをサポートし、ルータ E から拡張コミュニティとしての iBGP ネイバーへのリンクの帯域幅をアドバタイズするようにルータ C を設定します。

```
Router C(config)# router bgp 100
Router C(config-router)# neighbor 10.10.10.1 remote-as 100
Router C(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router C(config-router)# neighbor 10.10.10.2 remote-as 100
Router C(config-router)# neighbor 10.10.10.2 update-source Loopback 0
Router C(config-router)# neighbor 172.16.3.30 remote-as 200
```

```
Router C(config-router)# neighbor 172.16.3.30 ebgp-multihop 1
Router C(config-router)# address-family ipv4
Router C(config-router-af)# bgp dmzlink-bw

Router C(config-router-af)# neighbor 10.10.10.1 activate
Router C(config-router-af)# neighbor 10.10.10.1 send-community both
Router C(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router C(config-router-af)# neighbor 10.10.10.2 activate
Router C(config-router-af)# neighbor 10.10.10.2 send-community both
Router C(config-router-af)# neighbor 10.10.10.2 next-hop-self
Router C(config-router-af)# neighbor 172.16.3.3 activate
Router C(config-router-af)# neighbor 172.16.3.3 dmzlink-bw

Router C(config-router-af)# maximum-paths ibgp 6
Router C(config-router-af)# maximum-paths 6
```

BGP リンク帯域幅の確認

ここで、ルータ A およびルータ B でこの機能を確認する例を示します。

ルータ B

次の例では、**show ip bgp** コマンドをルータ B で入力し、BGP ルーティング テーブルにコストが同等でないベストパスがインストールされていることを確認します。各リンクの帯域幅は、各ルートとともに表示されます。

```
Router B# show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 48
Paths: (2 available, best #2)
Multipath: eBGP
  Advertised to update-groups:
     1          2
  200
    172.16.1.1 from 172.16.1.2 (192.168.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
      Extended Community: 0x0:0:0
      DMZ-Link Bw 278 kbytes
  200
    172.16.2.2 from 172.16.2.2 (192.168.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
      Extended Community: 0x0:0:0
      DMZ-Link Bw 625 kbytes
```

ルータ A

次の例では、**show ip bgp** コマンドをルータ A で入力して、iBGP を通じてリンク帯域幅拡張コミュニティがルータ A に伝播していることを確認します。出力には、BGP のルーティング テーブルのベスト パスとして、（ルータ B およびルータ C に関する）各出口リンクから自律システム 200 へのルートがインストールされていることが表示されます。

```
Router A# show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 48
Paths: (3 available, best #3)
Multipath: eBGP
  Advertised to update-groups:
```

```
   1          2
200
  172.16.1.1 from 172.16.1.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath
    Extended Community: 0x0:0:0
    DMZ-Link Bw 278 kbytes
200
  172.16.2.2 from 172.16.2.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 625 kbytes
200
  172.16.3.3 from 172.16.3.3 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 2500 kbytes
```

ルータ A

次の例では、**show ip route** コマンドをルータ A に入力し、アドバタイズされたマルチパス ルートおよび関連するトラフィック共有値を確認します。

```
Router A# show ip route 192.168.1.0
Routing entry for 192.168.1.0/24
  Known via "bgp 100", distance 200, metric 0
  Tag 200, type internal
  Last update from 172.168.1.1 00:01:43 ago
  Routing Descriptor Blocks:
  * 172.168.1.1, from 172.168.1.1, 00:01:43 ago
      Route metric is 0, traffic share count is 13
      AS Hops 1, BGP network version 0
      Route tag 200
    172.168.2.2, from 172.168.2.2, 00:01:43 ago
      Route metric is 0, traffic share count is 30
      AS Hops 1, BGP network version 0
      Route tag 200
    172.168.3.3, from 172.168.3.3, 00:01:43 ago
      Route metric is 0, traffic share count is 120
      AS Hops 1, BGP network version 0
      Route tag 200
```

その他の参考資料

次のセクションには、BGP リンク帯域幅機能に関連する参考資料があります。

関連資料

関連項目	マニュアル タイトル
BGP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』

関連項目	マニュアル タイトル
MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	「MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング」
iBGP のマルチパス ロード シェアリング	「iBGP マルチパス ロード シェアリング」
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格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

シスコのテクニカル サポート

説明	リンク
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

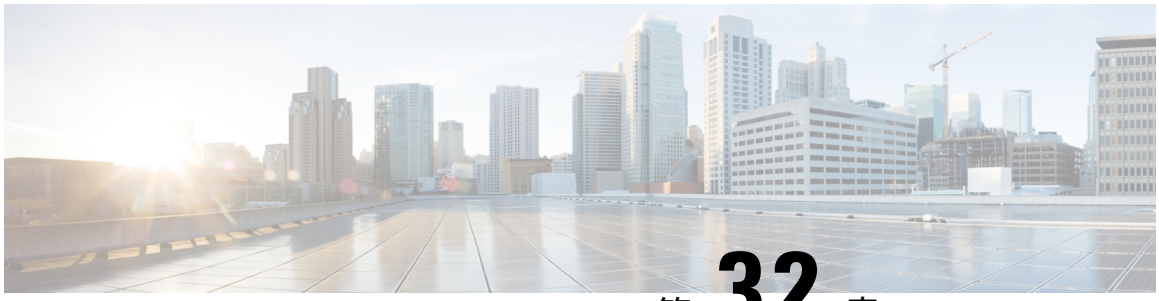
BGP リンク帯域幅の機能情報

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 *47 : BGP* リンク帯域幅の機能情報

機能名	リリース	機能情報
BGP リンク帯域幅	Cisco IOS XE リリース 2.1	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。 この機能により、**bgp dmzlink-bw, neighbor dmzlink-bw** コマンドが導入または変更されました。



第 32 章

ボーダー ゲートウェイ プロトコル リンクステート

ボーダー ゲートウェイ プロトコル リンクステート（BGP-LS）は、BGP ルーティング プロトコルを介して内部ゲートウェイ プロトコル（IGP）リンクステート データベースを伝送するために定義されたアドレス ファミリ識別子（AFI）およびサブアドレス ファミリ識別子（SAFI）です。BGP-LSは、ネットワーク トポロジ情報をトポロジ サーバおよびアプリケーション層トラフィック最適化（ALTO）サーバに提供します。BGP-LS では、集約、情報の非表示、および抽象化に対するポリシーベースの制御が可能です。BGP-LS は IS-IS および OSPFv2 サポートしています。

- 機能情報の確認 （639 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートに関する情報 （640 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートを使用した OSPF の設定方法 （644 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定方法 （645 ページ）
- ボーダー ゲートウェイ プロトコル リンクステート設定の確認 （647 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートの debug コマンド （650 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートに関する追加情報 （650 ページ）
- ボーダー ゲートウェイ プロトコル リンクステートの機能情報 （651 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。

ボーダー ゲートウェイ プロトコル リンクステートに関する情報

ボーダー ゲートウェイ プロトコルのリンクステート情報の概要

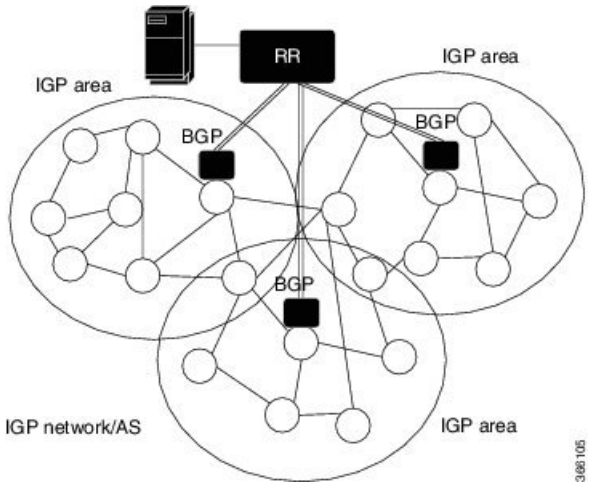
多くの環境では、ネットワークの外部にあるコンポーネントは、ネットワーク トポロジおよびネットワーク内の接続の現在の状態（トラフィック エンジニアリング（TE）情報を含む）に基づいて計算を実行するために呼び出されます。この情報は、通常、ネットワーク内の内部ゲートウェイ プロトコル（IGP）ルーティング プロトコルによって配布されます。

このモジュールでは、IGP のリンクステート（LS）およびトラフィック エンジニアリング（TE）情報をネットワークから収集し、BGP ルーティング プロトコルを使用してその情報を新しい BGP ネットワーク層到達可能性情報（NLRI）エンコード形式で外部コンポーネントと共有するためのメカニズムについて説明します。このメカニズムは、物理リンクと仮想リンクの両方に適用できます。この手法の用途には、ネットワークの外部にあるがネットワークの状態に関するリアルタイム情報を必要とする、アプリケーション層トラフィック最適化（ALTO）サーバやパス計算要素（PCE）が含まれます。たとえば、ネットワーク全体の各 IGP ノード（OSPF または IS-IS）のリンクステート データベース情報などです。

IGP エリア全体または自律システム（AS）全体におけるトポロジの可視性を必要とする用途に対応するために、BGP でリンクステート情報を伝送できるよう BGP-LS アドレスファミリまたはサブアドレスファミリが定義されています。各リンクステート オブジェクト（ノード、リンク、プレフィックスなど）の識別キーは NLRI でエンコードされ、オブジェクトのプロパティは BGP-LS 属性でエンコードされます。

下の図は、BGP-LS を利用するネットワークの一般的な展開シナリオを示しています。各 IGP エリアで、1 つ以上のノードが BGP-LS を使用して設定されています。これらの BGP スピーカーは、1 つ以上のルートリフレクタに接続することによって IBGP メッシュを形成します。このようにして、すべての BGP スピーカー（特にルートリフレクタ（RR））は、すべての IGP エリア（および EBGP ピアのその他の AS）からリンクステート情報を取得します。外部コンポーネントは、ルートリフレクタに接続してこの情報を取得します（多くの場合は、どのような情報が外部コンポーネントにアドバタイズされるかに関するポリシーによって管理されます）。その後、外部コンポーネント（コントローラなど）は、IGP エリアまたは AS 全体の「ノースバウンド」方向でこの情報を収集し、エンドツーエンドの転送のために着信パケットに適用されるエンドツーエンドのパス（とその関連付けられた SID）を生成できます。

図 *47 : IGP* ノードと *BGP* の関係



ボーダー ゲートウェイ プロトコルのリンクステート情報の伝送

リンクステート情報の伝送には、次の 2 つの部分があります。

- IGP リンクステート情報を構成するリンク、ノード、およびプレフィックスを表す新しい BGP NLRI の定義
- リンク、ノード、およびプレフィックスのプロパティと属性（リンクおよびプレフィックス メトリックやノードの補助ルータ ID など）を伝送する新しい BGP-LS 属性の定義

TLV 形式

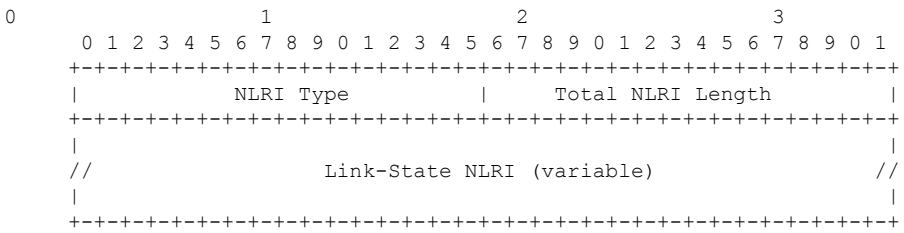
新しいリンクステート NLRI および属性の情報は、タイプ/長さ/値（TLV）というトリプレットでエンコードされます。この TLV 形式を下の図に示します。

```
0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |              Type             |             Length            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     //                       Value (variable)                      //
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Length（長さ）フィールドは、値部分の長さをオクテット単位で定義します（したがって、値部分がない TLV の長さは 0 になります）。

リンクステート NLRI

MP_REACH_NLRI および MP_UNREACH_NLRI 属性は、不透明な情報を伝送するための BGP のコンテナです。各リンクステート ネットワーク層到達可能性情報（NLRI）は、ノード、リンク、プレフィックスのいずれかを表します。NLRI の本体は、タイプ/長さ/値（TLV）トリプレットのセットであり、オブジェクトを識別するデータを含んでいます。



NLRI タイプ

Total NLRI Length（NLRI の合計長）フィールドには、NLRI タイプ フィールドまたはそれ自体を含まない、NLRI の残りの部分を合計した長さ（オクテット単位）が格納されます。

図 *48 : NLRI* タイプ

Type	NLRI Type
1	Node NLRI
2	Link NLRI
3	IPv4 Topology Prefix NLRI
4	IPv6 Topology Prefix NLRI

NLRI タイプを以下の図に示します。

図 *49 :* ノード *NLRI* 形式

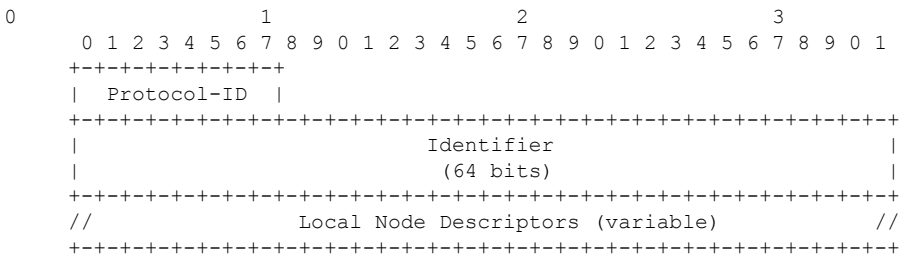
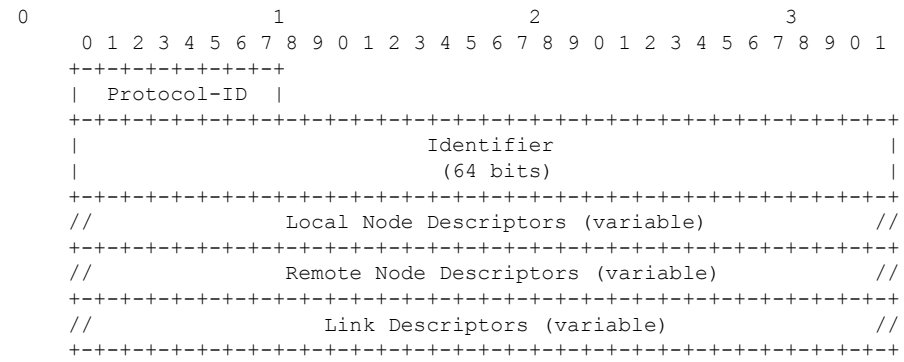
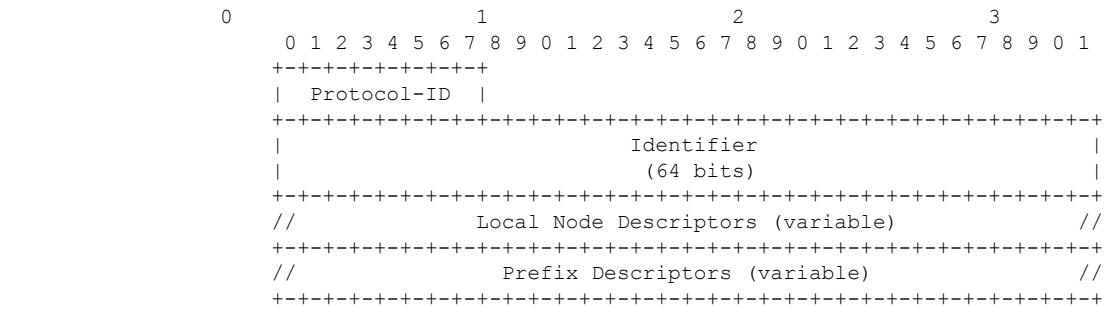


図 *50 :* リンク *NLRI* 形式



次の図に示すように、IPv4 および IPv6 プレフィックス NLRI（NLRI タイプ = 3 およびタイプ = 4）では同じ形式が使用されています。

図 *51 : IPv4/IPv6* トポロジのプレフィックス *NLRI* 形式



ノード記述子

各リンクは、基になる IGP で使用されるルータ ID のペア、つまり、IS-IS 用の 48 ビット ISO システム ID と OSPFv2 および OSPFv3 用の 32 ビット ルータ ID によって固定されます。IGP では、主にトラフィック エンジニアリングの目的で、1 つ以上の補助ルータ ID を追加で使用する場合があります。たとえば、IS-IS には 1 つ以上の IPv4 TE ルータ ID と IPv6 TE ルータ ID がある場合があります。これらの補助ルータ ID は、リンク属性に含める必要があります。

リンク記述子

Link Descriptors（リンク記述子）フィールドは、タイプ/長さ/値（TLV）トリプレットのセットです。リンク記述子の TLV は、アンカー ルータのペア間における複数のパラレル リンクから 1 つのリンクを一意に識別します。リンク記述子の TLV によって表されるリンクは、実際には「ハーフリンク」であり、論理リンクの単一方向の表現です。1 つの論理リンクを完全に表すために、2 つの発信側ルータがそれぞれハーフリンクをアドバタイズします。つまり、1 つのポイントツーポイント リンクについて 2 つのリンク NLRI がアドバタイズされます。

プレフィックス記述子

Prefix Descriptors（プレフィックス記述子）フィールドは、タイプ/長さ/値（TLV）トリプレットのセットです。プレフィックス記述子の TLV は、ノードによって発信された IPv4 または IPv6 プレフィックスを一意に識別します。

BGP-LS 属性

BGP-LS 属性は、リンク、ノード、およびプレフィックスのパラメータと属性を伝送するために使用される、任意の推移的な BGP 属性です。これは、タイプ/長さ/値（TLV）トリプレットのセットとして定義されます。この属性は、リンクステート NLRI にのみ含める必要があります。この属性は、他のすべてのアドレス ファミリでは無視する必要があります。

ボーダー ゲートウェイ プロトコル リンクステートを使用した OSPF の設定方法

OSPF は、BGP へのトポロジを LS キャッシュに挿入する IGP プロトコルの 1 つです。リンクステート情報は、次の 2 つの方法で BGP に渡すことができます。

- OSPF と BGP 間の新しい通信が確立されている場合、または BGP-LS 機能が OSPF で最初に有効にされている場合、すべての LSA 情報は LS ライブラリを介して BGP にダウンロードされます。
- 新しい LSA 情報が処理またはリモート OSPF ノードから受信されると、この情報は BGP に追加または BGP で更新されます。

ボーダー ゲートウェイ プロトコル リンクステートを使用した OSPF の設定

BGP-LS を使用して OSPF を設定するには、次の手順を実行します。

1. OSPF ルーティング プロトコルを有効にし、ルータ コンフィギュレーション モードを開始します。

   ```
   router ospf
   ```

   次に例を示します。

   ```
   Device(config-router)# router ospf 10
   ```

2. BGP リンクステートを配布します。

   ```
    distribute link-state
   ```

   次に例を示します。

   ```
   Device(config-router)# distribute link-state instance-id <instid>
   Device(config-router)# distribute link-state throttle <time>
   ```

   instance-id（任意）：LS 配布のインスタンス ID を設定します。デフォルト値は 0 です。範囲は 32 ～ 2^32-1 です。

   throttle（任意）：LS 配布キューを処理するスロットル時間を設定します。デフォルト値は 5 秒です。範囲は 1 ～ 3600 秒です。

（注） すべてのエリアが削除されるシナリオでは、スロットル タイマーは適用されません。キューは OSPF によって完全にウォークされ、すべてのエリアに対するアップデートが BGP に送信されます。

インスタンス ID とスロットルの値を指定しなかった場合は、デフォルト値が使用されます。

例：

```
#show run | sec router ospf
router ospf 10
distribute link-state instance-id 33 throttle 6
```

（注） 2 つの OSPF インスタンスで同じインスタンス ID を使用することはできません。使用すると、インスタンス ID がすでに使用されているというエラーがスローされます。

ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定方法

IS-IS は、ルーティング情報を BGP に配布します。IS-IS は、LSP データベース内のルーティング情報を処理し、関連するオブジェクトを抽出します。IS-IS のノード、リンク、プレフィックス情報およびそれらの属性が BGP にアドバタイズされます。IS-IS から BGP へのこのアップデートは、ローカルルータまたはリモートルータに属している LSP フラグメントで変更があった場合にのみ発生します。

ボーダー ゲートウェイ プロトコル リンクステートを使用した IS-IS の設定

BGP-LS を使用して IS-IS を設定するには、次の手順を実行します。

1. IS-IS ルーティング プロトコルを有効にし、ルータ コンフィギュレーション モードを開始します。

   ```
   router isis
   ```

   次に例を示します。

   ```
   Device(config-router)# router isis
   ```

2. BGP リンクステートを配布します。

   ```
    distribute link-state
   ```

   次に例を示します。

   ```
   Device(config-router)# distribute link-state instance-id <instid>
   ```

   ```
   Device(config-router)# distribute link-state throttle <time>
   ```

   instance-id（任意）：LS 配布のインスタンス ID を設定します。範囲は 32 ～ 4294967294 です。

throttle（任意）：LS 配布キューを処理するスロットル時間を設定します。範囲は 5 ～ 20 秒です。

BGP の設定

BGP-LS を使用して BGP を設定するには、次の手順を実行します。

1. BGP ルーティング プロトコルを有効にし、ルータ コンフィギュレーション モードを開始します。

   ```
   router bgp
   ```

   次に例を示します。

   ```
   Device(config-if)# router bgp 100
   ```

2. アドレスファミリ リンクステートを設定します。

   ```
   address-family link-state link-state
   ```

   次に例を示します。

   ```
   Device(config-router)# address-family link-state link-state
   ```

3. アドレスファミリを終了します。

   ```
   exit-address-family
   ```

   次に例を示します。

   ```
   Device(config-router)# exit-address-family
   ```

例：ボーダーゲートウェイプロトコルリンクステートを使用したIS-IS の設定

例：IS-IS の設定

```
router isis 1
 net 49.0001.1720.1600.1001.00
 is-type level-1
 metric-style wide
 distribute link-state level-1
 segment-routing mpls
 segment-routing prefix-sid-map advertise-local
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1

interface GigabitEthernet2/2/2
 ip address 172.16.0.1 255.255.0.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
```

例：BGP の設定

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.4 remote-as 100
 !
 address-family ipv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.4 activate
 exit-address-family
 !
 address-family link-state link-state
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.4 activate
 exit-address-family
```

ボーダー ゲートウェイ プロトコル リンクステート設定の確認

BGP-LS 設定のステータスを確認するには、以下の show コマンドを任意の順序で使用します。

show ip ospf ls-distribution

LS 配布のステータスを表示します。

```
Device# show ip ospf ls-distribution

            OSPF Router with ID (10.0.0.6) (Process ID 10)
          OSPF LS Distribution is Enabled
                         Instance Id: 0
                      Throttle time: 5
                  Registration Handle: 0x0
                               Status:Ready Active
    Num DBs Queued for LSCache Update: 0
     Num of DBs with Unresolved Links: 0
```

show ip ospf database dist-ls-pending

BGP に送信される、保留中の LSA を表示します。

```
 Sample Output:
Device# show ip ospf database dist-ls-pending

            OSPF Router with ID (10.0.0.6) (Process ID 10)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
 10.0.0.7         10.0.0.6         4           0x80000006 0x009678 1
 172.16.0.6         172.16.0.6         1110        0x80000018 0x00CAF9 2
(Has-unresolved-links)
```

show isis distribute-ls [level-1 | level-2]

BGP に配布される IS-IS の内部 LS キャッシュ情報を表示します。

```
Device# sh isis distribute-ls

 ISIS distribute link-state: configured
 distls_levels:0x3, distls_initialized:1,
 distls_instance_id:0, distls_throttle_delay:10
 LS DB: ls_init_started(0) ls_initialized(1) ls_pending_delete(0)
 distls_enabled[1]:1
 distls_enabled[2]:1
 Level 1:
Node System ID:0003.0003.0003 Pseudonode-Id:0 ls_change_flags:0x0
   LSP: lspid(0003.0003.0003.00-00), lsptype(0) lsp_change_flags(0x0)
    Node Attr: name(r3) bitfield(0xD1) node_flags(0x0)
     area_len/area_addr(2/33) num_mtid/mtid(0/0) ipv4_id(172.16.0.9)
     num_alg/sr_alg(0/0) num_srgb/srgb(1/(start:16000, range:8000)
     srgb_flags(0x80)
     opaqe_len/opaqe(0/0x0)
    ISIS LS Links:
     mtid(0): nid:0002.0002.0002.00, {0, 0}, {6.6.6.1, 6.6.6.6}
     Link Attr: bitbfield:0x940F, local_ipv4_id:6.6.6.1, remote_ipv4_id:172.16.0.8,
      max_link_bw:10000, max_resv_bw:10000,
     num_unresv_bw/unresv_bw:8/
      [0]:    10000 kbits/sec, [1]:     8000 kbits/sec
      [2]:     8000 kbits/sec, [3]:     8000 kbits/sec
      [4]:     8000 kbits/sec, [5]:     8000 kbits/sec
      [6]:     8000 kbits/sec, [7]:     8000 kbits/sec,
      admin_group:0, protect_type:0, mpls_proto_mask:0x0,
      te_metric:0, metric:0, link_name:,
      num_srlg/srlg:0/
      num_adj_sid/adjsid:2/
    Adjacency SID Label:16 F:0 B:0 V:1 L:1 S:0 weight:0
    Adjacency SID Label:17 F:0 B:1 V:1 L:1 S:0 weight:0
      opaque_len/opaque_data:0/0x0
    Address-family ipv4 ISIS LS Prefix:
     mtid(0): 1.1.1.0/24
     Prefix Attr: bitfield:0x0, metric:10, igp_flags:0x0,
      num_route_tag:0, route_tag:0
      num_pfx_sid:0, pfx_sid:
      pfx_srms:
      opaque_len:0, opaque_data:0x0
     mtid(0): 172.16.0.8/24
     Prefix Attr: bitfield:0x0, metric:10, igp_flags:0x0,
      num_route_tag:0, route_tag:0
      num_pfx_sid:0, pfx_sid:
      pfx_srms:
      opaque_len:0, opaque_data:0x0
```

show bgp link-state link-state

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Prefix codes:E link, V node, T4 IPv4 reachable route, T6 IPv6 reachable route, I
Identifier,
              N local node, R remote node, L link, P prefix,
              L1/L2 ISIS level-1/level-2, O OSPF, a area-ID, l link-ID,
              t topology-ID, s ISO-ID, c confed-ID/ASN, b bgp-identifier,
              r router-ID, i if-address, n nbr-address, o OSPF Route-type,
              p IP-prefix, d designated router address, u/U Unknown,
              x/X Unexpected, m/M Malformed

     Network          Next Hop            Metric LocPrf Weight Path
```

```
 *>   [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.1001.00]]
                       15.0.0.1                 0             0 100 i
 *>   [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]]
                       15.0.0.1                 0             0 100 i
 *>   [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]]
                       15.0.0.1                 0             0 100 i
 *>   [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]]
                       15.0.0.1                 0             0 100 i
 *>   [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]]
                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.1001.00]][R[c100][b0.0.0.0][s1720.1600.2002.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][R[c100][b0.0.0.0][s1720.1600.1001.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][R[c100][b0.0.0.0][s1720.1600.3003.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][R[c100][b0.0.0.0][s1720.1600.4004.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]][R[c100][b0.0.0.0][s1720.1600.2002.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]][R[c100][b0.0.0.0][s1720.1600.5005.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]][R[c100][b0.0.0.0][s1720.1600.2002.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]][R[c100][b0.0.0.0][s1720.1600.5005.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][R[c100][b0.0.0.0][s1720.1600.3003.00]][L]

                       15.0.0.1                 0             0 100 i
 *>
[E][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][R[c100][b0.0.0.0][s1720.1600.4004.00]][L]

                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.1001.00]][P[p10.0.0.0/24]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.1001.00]][P[p7.7.7.7/32]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][P[p10.0.0.0/24]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][P[p11.0.0.0/24]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][P[p12.0.0.0/24]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.2002.00]][P[p5.5.5.5/32]]
                       15.0.0.1                 0             0 100 i
 *>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]][P[p11.0.0.0/24]]
                       15.0.0.1                 0             0 100 i
```

```
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]][P[p13.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.3003.00]][P[p3.3.3.3/32]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]][P[p12.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]][P[p14.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]][P[p15.15.15.15/32]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][P[p13.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][P[p14.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][P[p15.0.0.0/24]]
                    15.0.0.1                 0             0 100 i
*>   [T4][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.5005.00]][P[p16.16.16.16/32]]
                    15.0.0.1                 0             0 100 i
```

show bgp link-state link-state nlri <nlri string>

```
BGP routing table entry for [V][L1][I0x43][N[c100][b0.0.0.0][s1720.1600.4004.00]], version
 95
Paths: (1 available, best #1, table link-state link-state)
  Not advertised to any peer
  Refresh Epoch 4
  Local
    16.16.16.16 (metric 30) from 15.15.15.15 (15.15.15.15)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 16.16.16.16, Cluster list: 15.15.15.15
      LS Attribute: Node-name: R4, ISIS area: 49.12.34
      rx pathid: 0, tx pathid: 0x0
```

ボーダー ゲートウェイ プロトコル リンクステートの debug コマンド

- **debug ip ospf dist-ls [detail]**

  OSPF で LS 配布関連のデバッグをオンにします。

- **debug isis distribute-ls**

  IS-IS から BGP にアドバタイズされている項目を表示します。

ボーダー ゲートウェイ プロトコル リンクステ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 Commands List, All Releases』

MIB

MIB	MIB のリンク
• CISCO-BGP-LS-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

RFC

RFC	タイトル
• RFC 7752	『*Link-State Info Distribution Using BGP*』

シスコのテクニカル サポート

説明	リンク
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

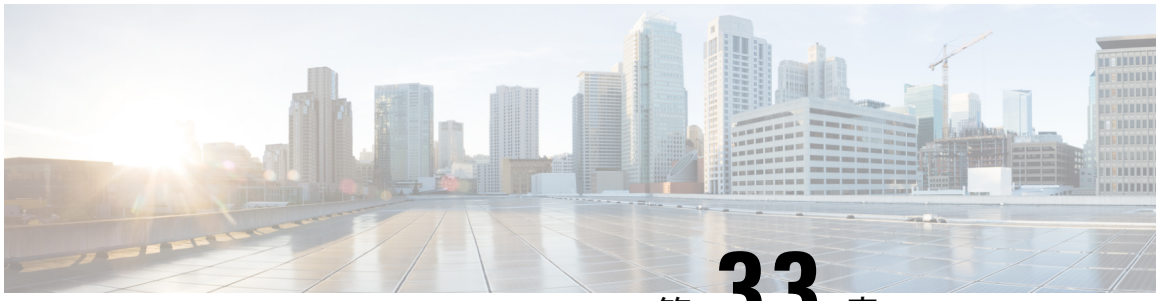
ボーダー ゲートウェイ プロトコル リンクステートの機能情報

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 *48 : BGP-LS* の機能情報

機能名	リリース	機能情報
ボーダー ゲートウェイ プロトコル リンクステート	Cisco IOS XE Everest 16.4.1	BGP リンクステート（LS）は、BGP を介して内部ゲートウェイ プロトコル（IGP）リンクステート データベースを伝えるために定義されたアドレス ファミリ識別子（AFI）およびサブアドレス ファミリ識別子（SAFI）です。次のコマンドが導入または変更されました。 **address-family link-state link-state**、**distribute link-state**、**show bgp link-state link-state**、**show bgp link-state link-state nlri** *nlri string*、**show ip ospf database dist-ls-pending**、**show ip ospf ls-distribution**、 **show isis distribute-ls**



第 33 章

iBGP マルチパス ロード シェアリング

このフィーチャ モジュールでは、iBGP のマルチパス ロード シェアリング機能について説明します。この機能を使用すると、BGP スピーキング ルータが宛先へのベスト パスとして複数の iBGP パスを選択できます。次に、このベスト パスまたはマルチパスが、このルータの IP ルーティング テーブルに組み込まれます。

- 機能情報の確認 （653 ページ）
- iBGP マルチパス ロード シェアリングの概要 （653 ページ）
- iBGP のマルチパス ロード シェアリングの設定方法 （656 ページ）
- 設定例 （659 ページ）
- その他の参考資料 （661 ページ）
- iBGP のマルチパス ロード シェアリングの機能情報 （662 ページ）

機能情報の確認

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

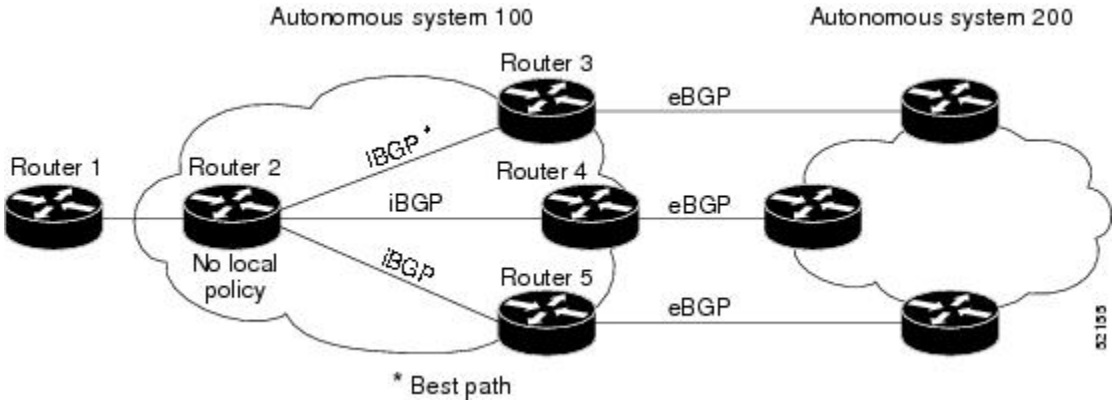
プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

iBGP マルチパス ロード シェアリングの概要

ローカル ポリシーが設定されていないボーダー ゲートウェイ プロトコル（BGP）対応ルータが複数のネットワーク層到着達可能性情報（NLRI）を同じ宛先の内部 BGP（iBGP）から受信すると、このルータは 1 つの iBGP パスをベスト パスとして選択します。次に、このベスト パスが、このルータの IP ルーティング テーブルに組み込まれます。たとえば、下の図では、自

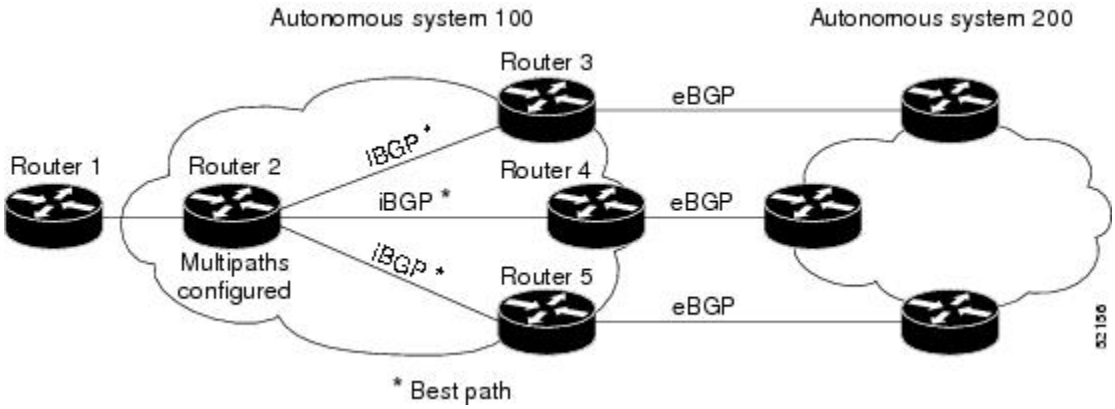
律システム 200 へのパスは 3 つありますが、ルータ 2 は、自律システム 200 へのパスの 1 つをベスト パスであると判断し、このパスだけを使用して自律システム 200 に到達します。

図 *52 : 1* つのベスト パスを持つ非マルチプロトコル ラベル スイッチング（*MPLS*）トポロジ



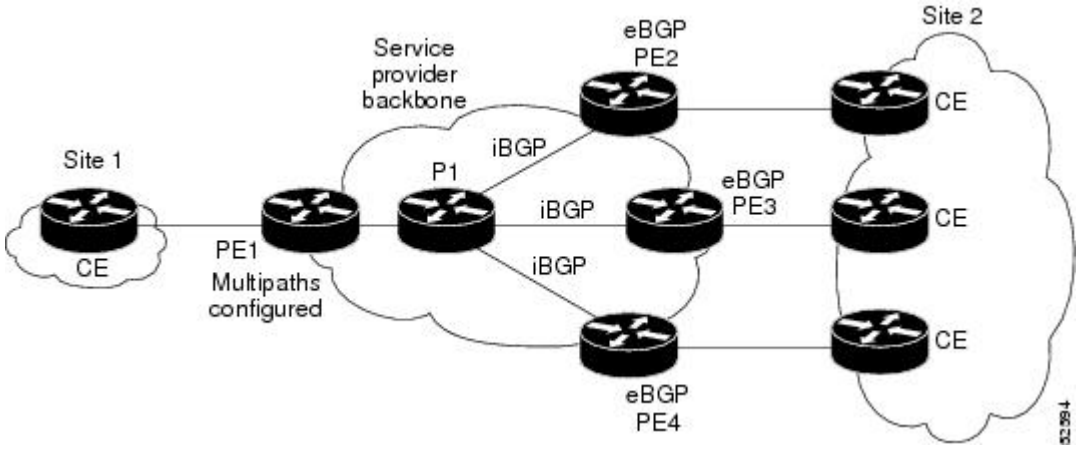
iBGP のマルチパス ロード シェアリング機能を使用すると、BGP 対応ルータでは、複数の iBGP パスを宛先へのベストパスとして選択できます。次に、このベストパスまたはマルチパスが、このルータの IP ルーティング テーブルに組み込まれます。たとえば、下の図のルータ 2 で、ルータ 3、4、および 5 へのパスがマルチパスとして設定され、自律システム 200 に到達するために使用でき、結果として自律システム 200 への負荷が均等に負担されます。

図 *53 : 3* つのマルチパスを持つ非 *MPLS* トポロジ



iBGP のマルチパス ロード シェアリング機能は、サービス プロバイダー バックボーンを持つマルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）と同様に機能します。たとえば、下の図のルータ PE1 では、ルータ PE2、PE3、および PE4 へのパスをマルチパスとして選択でき、サイト 2 への負荷を均等に負担するために使用できます。

図 *54 : 3* つのマルチパスを持つ *MPLS VPN*



同じ宛先への複数のパスをマルチパスと見なすには、次の基準を満たす必要があります。

- すべての属性が同じである必要があります。属性には、加重、ローカルプリファレンス、自律システム パス（長さだけでなく属性全体）、発信元コード、Multi Exit Discriminator（MED）、および内部ゲートウェイ プロトコル（IGP）距離が含まれます。
- 各マルチパスのネクスト ホップ ルータが異なっている必要があります。

基準を満たしていて、複数のパスがマルチパスと見なされても、BGP 対応ルータは、引き続きマルチパスの 1 つをベスト パスに指定し、このベスト パスをそのネイバーにアドバタイズします。

iBGP マルチパス ロード シェアリングの利点

複数の iBGP のベスト パスを設定すると、ルータでは、特定のサイトを宛先とするトラフィックを均等に負担できるようになります。

iBGP マルチパス ロード シェアリングに関する制約事項

ルート リフレクタの制限事項

ルーティング テーブルに複数の iBGP パスがインストールされている場合、ルート リフレクタは 1 つのパス（1 つのネクスト ホップ）だけをアドバタイズします。

メモリ消費の制約事項

複数の iBGP パスがある BGP プレフィックス用の各 IP ルーティング テーブル エントリは、約 350 バイトの追加メモリを使用します。ルータの使用可能なメモリが少なく、特にルータがフル インターネット ルーティング テーブルを備えている場合は、この機能の使用を推奨しません。

iBGP のマルチパス ロード シェアリングの設定方法

iBGP マルチパス ロード シェアリングの設定

iBGP マルチパス ロード シェアリング機能を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Device(config-router)# maximum-paths ibgp maximum-number`	ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

iBGP のマルチパス ロード シェアリングの確認

iBGP のマルチパス ロード シェアリング機能が正しく設定されていることを確認するには、次の手順を実行します。

手順の概要

1. **show ip bgp** *network-number* EXEC コマンドを入力して、非 MPLS トポロジのネットワークの属性を表示するか、**show ip bgp vpnv4 all** *ip-prefix* EXECコマンドを入力して、MPLS VPN のネットワークの属性を表示します。
2. **show ip bgp** *network-number* EXEC コマンドまたは **show ip bgp vpnv4 all** *ip-prefix* EXEC コマンドを入力して得られる表示で、目的のマルチパスが「multipath」としてマークされていることを確認します。マルチパスの 1 つが「best」としてマークされていることに留意してください。
3. **show ip route** *ip-address* EXEC コマンドを入力して、非 MPLS トポロジのネットワークのルーティング情報を表示するか、**show ip route vrf** *vrf-name ip-prefix* EXEC コマンドを入力して、MPLS VPN のネットワークのルーティング情報を表示します。
4. **show ip bgp** *ip-prefix* EXEC コマンドまたは **show ip bgp vpnv4 all** *ip-prefix* EXEC コマンドを入力して得られる表示で、「multipath」としてマークされたパスがルーティング情報に含まれていることを確認します（ルーティング情報は、手順 3 の実行後に表示されます）。

手順の詳細

ステップ 1 **show ip bgp** *network-number* EXEC コマンドを入力して、非 MPLS トポロジのネットワークの属性を表示するか、**show ip bgp vpnv4 all** *ip-prefix* EXECコマンドを入力して、MPLS VPN のネットワークの属性を表示します。

例：

```
Device# show ip bgp 10.22.22.0
```

```
BGP routing table entry for 10.22.22.0/24, version 119
Paths:(6 available, best #1)
Multipath:iBGP
Flag:0x820
  Advertised to non peer-group peers:
  10.1.12.12
  22
    10.2.3.8 (metric 11) from 10.1.3.4 (100.0.0.5)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Originator:100.0.0.5, Cluster list:100.0.0.4
  22
    10.2.1.9 (metric 11) from 10.1.1.2 (100.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.9, Cluster list:100.0.0.2
  22
    10.2.5.10 (metric 11) from 10.1.5.6 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.6
  22
    10.2.4.10 (metric 11) from 10.1.4.5 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.5
  22
    10.2.6.10 (metric 11) from 10.1.6.7 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.7

Device# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 100:1:10.22.22.0/24, version 50
Paths:(6 available, best #1)
Multipath:iBGP
  Advertised to non peer-group peers:
  200.1.12.12
  22
    10.22.7.8 (metric 11) from 10.11.3.4 (100.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Extended Community:RT:100:1
      Originator:100.0.0.8, Cluster list:100.1.1.44
  22
    10.22.1.9 (metric 11) from 10.11.1.2 (100.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.9, Cluster list:100.1.1.22
  22
    10.22.6.10 (metric 11) from 10.11.6.7 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.7
  22
    10.22.4.10 (metric 11) from 10.11.4.5 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.5
  22
    10.22.5.10 (metric 11) from 10.11.5.6 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.6
```

ステップ 2 **show ip bgp** *network-number* EXEC コマンドまたは **show ip bgp vpnv4 all** *ip-prefix* EXEC コマンドを入力して得られる表示で、目的のマルチパスが「multipath」としてマークされていることを確認します。マルチパスの 1 つが「best」としてマークされていることに留意してください。

ステップ 3 **show ip route** *ip-address* EXEC コマンドを入力して、非 MPLS トポロジのネットワークのルーティング情報を表示するか、**show ip route vrf** *vrf-name ip-prefix* EXEC コマンドを入力して、MPLS VPN のネットワークのルーティング情報を表示します。

例：

```
Device# show ip route 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.2.6.10 00:00:03 ago
  Routing Descriptor Blocks:
  * 10.2.3.8, from 10.1.3.4, 00:00:03 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.2.1.9, from 10.1.1.2, 00:00:03 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.2.5.10, from 10.1.5.6, 00:00:03 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.2.4.10, from 10.1.4.5, 00:00:03 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.2.6.10, from 10.1.6.7, 00:00:03 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1

Device# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

ステップ 4 **show ip bgp** *ip-prefix* EXEC コマンドまたは **show ip bgp vpnv4 all** *ip-prefix* EXEC コマンドを入力して得られる表示で、「multipath」としてマークされたパスがルーティング情報に含まれていることを確認します（ルーティング情報は、手順 3 の実行後に表示されます）。

iBGP のマルチパス ロード シェアリングのモニタリングおよびメンテナンス

iBGP のマルチパス ロード シェアリング情報を表示するには、必要に応じて EXEC モードで次のコマンドを使用します。

コマンド	目的
`Device# show ip bgp ip-prefix`	非 MPLS トポロジのネットワークの属性およびマルチパスを表示します。
`Device# show ip bgp vpnv4 all ip-prefix`	MPLS VPN のネットワークの属性およびマルチパスを表示します。
`Device# show ip route ip-prefix`	非 MPLS トポロジのネットワークのルーティング情報を表示します。
`Device# show ip route vrf vrf-name ip-prefix`	MPLS VPN のネットワークのルーティング情報を表示します。

設定例

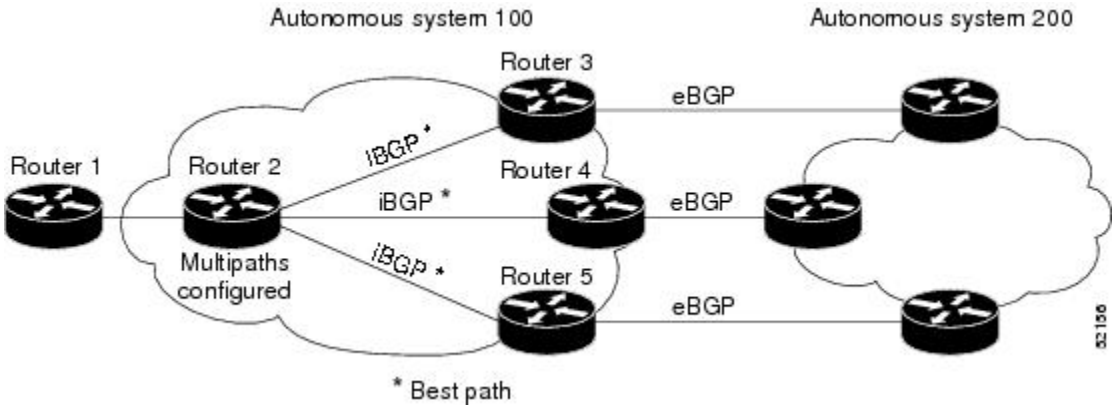
設定例は両方とも、各パスの適切な属性が等しく、各マルチパスのネクスト ホップ ルータが異なっていることを前提としています。

例：非 MPLS トポロジでの iBGP のマルチパス ロード シェアリング

設定例は両方とも、各パスの適切な属性が等しく、各マルチパスのネクスト ホップ ルータが異なっていることを前提としています。

次の例は、非 MPLS トポロジで iBGP のマルチパス ロード シェアリング機能をセットアップする方法を示します（下の図を参照）。

図 *55 : 非 MPLS* トポロジの例



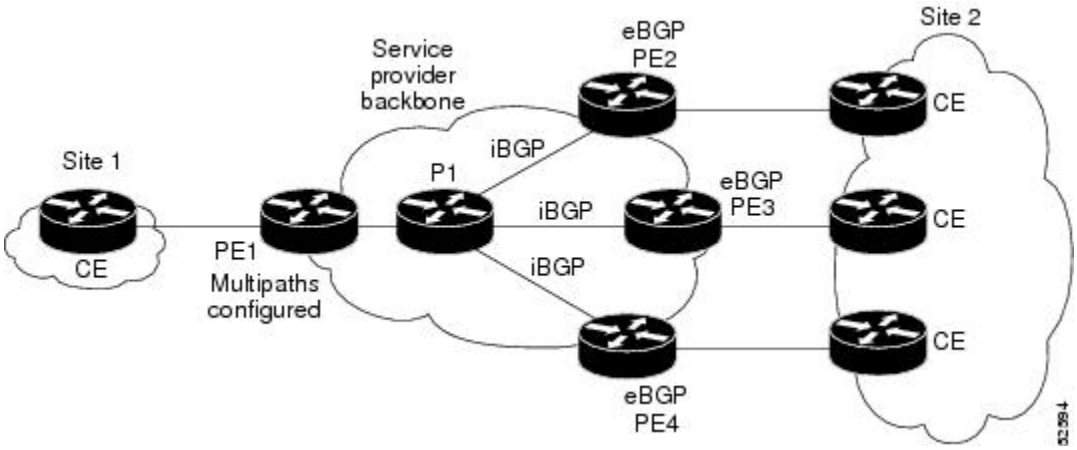
ルータ 2 の設定

```
router bgp 100
maximum-paths ibgp 3
```

例：MPLS VPN トポロジでの iBGP のマルチパス ロード シェアリング

次の例は、MPLS VPN トポロジで iBGP のマルチパス ロード シェアリング機能をセットアップする方法を示します（下の図を参照）。

図 *56 : MPLS VPN* トポロジの例



ルータ PE1 の設定

```
router bgp 100
address-family ipv4 unicast vrf site2
 maximum-paths ibgp 3
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング」モジュール
自律システムの出口リンクの帯域幅の拡張コミュニティとしてのアドバタイズ	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP リンク帯域幅」モジュール

標準

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

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS 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	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

テクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

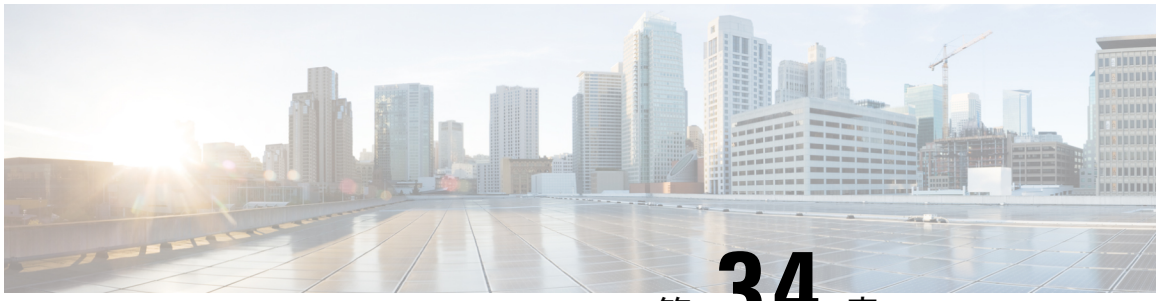
iBGP のマルチパス ロード シェアリングの機能情報

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

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 *49 : iBGP* のマルチパス ロード シェアリングの機能情報

機能名	リリース	機能情報
iBGP のマルチパス ロード シェアリング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。 この機能により、次のコマンドが変更されました。**maximum paths ibgp**、**show ip bgp**、 **show ip bgp vpnv4**、 **show ip route**、 **show ip route vrf**



第 34 章

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

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

- 機能情報の確認 （663 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの前提条件 （664 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの制約事項 （664 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングについて （665 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの設定方法 （667 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの設定例 （670 ページ）
- 次の作業 （671 ページ）
- その他の参考資料 （671 ページ）
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの機能情報 （673 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および

ご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

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

ロード バランシングの設定に CEF を使用

Cisco Express Forwarding（CEF）または distributed CEF（dCEF）が、参加するすべてのルータでイネーブルになっている必要があります。

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

アドレス ファミリのサポート

この機能は、VPN ルーティング/転送（VRF）インスタンス単位で設定されます。この機能は IPv4 VRF アドレス ファミリだけで設定できます。

メモリ消費の制約事項

各 BGP マルチパス ルーティング テーブル エントリでは、追加のメモリを使用します。使用できるメモリが少ないルータや、特にフル インターネット ルーティング テーブルを送受信するルータでは、この機能を使用しないことを推奨します。

ルート リフレクタの制限事項

ルーティング テーブルに複数の iBGP パスがインストールされている場合、ルート リフレクタは 1 つのパス（ネクスト ホップ）だけをアドバタイズします。ルータがルート リフレクタの背後にある場合、マルチホーム サイトに接続されているすべてのルータは、別のルート識別子が VRF ごとに設定されない限りアドバタイズされません。

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

eBGP と iBGP 間のマルチパス ロード シェアリング

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

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

マルチパス全体でのロード バランシングは CEF によって実行されます。CEF ロード バランシングは、パケット単位のラウンドロビンまたはセッション単位（送信元と宛先のペア）を基準として設定されます。CEF については、『Cisco Express Forwarding Overview』のマニュアルを参照してください。

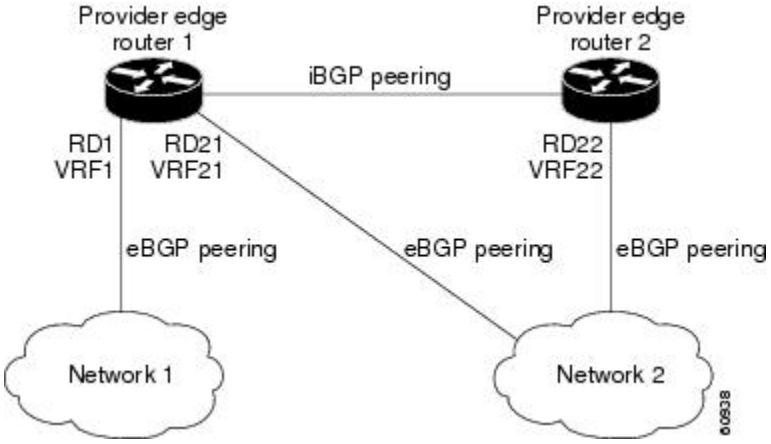
MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能は、IPv4 VRF アドレス ファミリ コンフィギュレーション モードだけでイネーブルにされます。この機能が有効にされると、VRF にインポートされた eBGP パスまたは iBGP パスあるいはその両方でロードバランシングを実行できます。マルチパスの数は VRF 単位で設定されます。別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。

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

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

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

図 *57:* サービス プロバイダー *BGP MPLS* ネットワーク

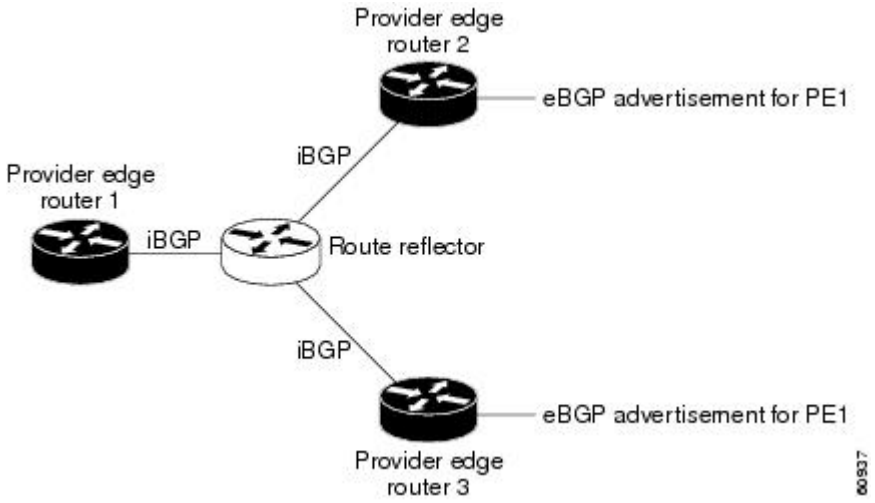


PE ルータ 1 には、MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能が設定でき、これによって、iBGP パスと eBGP パスの両方をマルチパスとして選択し、ネットワーク 1 の VRF にインポートできます。マルチパスは CEF によって使用され、ロード バランシングが実行されます。ネットワーク 2 から PE ルータ 1 および PE ルータ 2 に送信される IP トラフィックは、eBGP パスを経由して IP トラフィックとして送信されます。iBGP パスを経由して送信される IP トラフィックは MPLS トラフィックとして送信され、eBGP パスを経由して送信される MPLS トラフィックは IP トラフィックとして送信されます。ネットワーク 2 からアドバタイズされるすべてのプレフィックスは、ルート識別子（RD）21 および RD 22 を経由して PE ルータ 1 によって受信されます。RD 21 を経由するアドバタイズメントは IP パケットとして送受信され、RD 22 を経由するアドバタイズメントは MPLS パケットとして送受信されます。両方のパスを VRF1 のマルチパスとして選択でき、VRF1 の RIB にインストールできます。

ルート リフレクタを使用した eBGP および iBGP のマルチパス ロード シェアリング

下の図に、3 つの PE ルータとルート リフレクタを含むトポロジを示します。これらすべてには、iBGP ピアリングが設定されています。PE ルータ 2 および PE ルータ 3 はそれぞれ、PE ルータ 1 への等価プリファレンス eBGP パスをアドバタイズします。デフォルトでは、ルート リフレクタは 1 つのパスだけを選択し、PE ルータ 1 にアドバタイズします。

図 *58 :* ルート リフレクタを使用したトポロジ



PE ルータ 1 への等価プリファレンス パスのすべてがルート リフレクタを経由してアドバタイズされるためには、異なる RD を使用して各 VRF を設定する必要があります。ルート リフレクタによって受信されるプレフィックスは別々に認識され、PE ルータ 1 にアドバタイズされます。

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

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

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

eBGP および iBGP に対する BGP マルチパス ロード シェアリングの設定

この機能を設定するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*

4. **address-family ipv4 vrf** *vrf-name*
5. **maximum-paths eibgp** *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	**enable** 例： `Device> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf RED`	ルータをアドレス ファミリ コンフィギュレーション モードにします。 • 別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。
ステップ 5	**maximum-paths eibgp** *number* 例： `Device(config-router-af)# maximum-paths eibgp 6`	ルーティング テーブルにインストールできるパラレルの iBGP ルートおよび eBGP ルートの数を設定します。 （注） **maximum-paths eibgp** コマンドは IPv4 VRF アドレス ファミリ コンフィギュレーション モードだけで設定でき、他のすべてのアドレス ファミリ コンフィギュレーション モードでは設定できません。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

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

手順の概要

1. **enable**
2. **show ip bgp neighbors** [*neighbor-address*[**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*regexp*] | **received** *prefix-filter* | **received-routes** | **routes**]]
3. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}
4. **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	**enable** 例： `Device> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp neighbors** [*neighbor-address*[**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*regexp*] | **received** *prefix-filter* | **received-routes** | **routes**]] 例： `Device# show ip bgp neighbors`	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。
ステップ 3	**show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} 例： `Device# show ip bgp vpnv4 vrf RED`	VPN アドレス情報を BGP テーブルから表示します。このコマンドは、VRF が BGP によって受信されたことを確認するために使用します。
ステップ 4	**show ip route vrf** *vrf-name* 例： `Device# show ip route vrf RED`	VRF インスタンスに関連する IP ルーティング テーブルを表示します。show ip route vrf コマンドは、該当する VRF がルーティング テーブルにあることを確認するために使用します。

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

例：eBGP および iBGP のマルチパス ロード シェアリングの設定

次の設定例では、ルータをアドレス ファミリ モードで設定して、6 つの BGP ルート（eBGP または iBGP）をマルチパスとして選択します。

```
Device(config)# router bgp 40000
 Device(config-router)# address-family ipv4 vrf RED
 Device(config-router-af)# maximum-paths eibgp 6
 Device(config-router-af)# end
```

例：eBGP および iBGP のマルチパス ロード シェアリングの確認

iBGP ルートおよび eBGP ルートがロード シェアリングについて設定されたことを確認するには、 **show ip bgp vpnv4** EXEC コマンドまたは **show ip route vrf** EXEC コマンドを使用します。

次の例では、**show ip bgp vpnv4** コマンドを入力して、VPNv4 RIB にインストールされたマルチパスを表示します。

```
Device# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10:1:22.22.22.0/24, version 19
Paths:(5 available, best #5)
Multipath:eiBGP
  Advertised to non peer-group peers:
  10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
  22
    10.0.0.2 (metric 20) from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.4
  22
    10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.5
  22
    10.0.0.2 (metric 20) from 10.0.0.2 (10.0.0.2)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1 0x0:0:0
  22
    10.0.0.2 (metric 20) from 10.0.0.3 (10.0.0.3)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.3
  22
    10.1.1.12 from 10.1.1.12 (10.22.22.12)
      Origin IGP, metric 0, localpref 100, valid, external, multipath, best
      Extended Community:RT:100:1
```

次の例では、**show ip route vrf** コマンドを入力して、VRF テーブル内のマルチパス ルートを表示します。

```
Device# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 20, metric 0
  Tag 22, type external
  Last update from 10.1.1.12 01:59:31 ago
  Routing Descriptor Blocks:
  * 10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.4, 01:59:31 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.5, 01:59:31 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.2, 01:59:31 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.3, 01:59:31 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.1.1.12, from 10.1.1.12, 01:59:31 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

次の作業

拡張コミュニティとして自律システム出口リンクの帯域幅をアドバタイズする方法については、「BGP リンク帯域幅」モジュールを参照してください。

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
BGP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『Cisco IOS IP Routing: BGP Command Reference』
総合的な BGP リンク帯域幅の設定例および作業	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP リンク帯域幅」モジュール
CEF 設定作業	『*IP Switching Cisco Express Forwarding Configuration Guide*』の「CEF Overview」モジュール

標準

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

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	プラットフォームおよび Cisco IOS Release によりサポートされている MIB のリストを入手し、MIB モジュールをダウンロードするには、Cisco.com の次のシスコ MIB Web サイトの URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC 1771	『*A Border Gateway Protocol 4（BGP4）*』
RFC 2547	『*BGP/MPLS VPNs*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

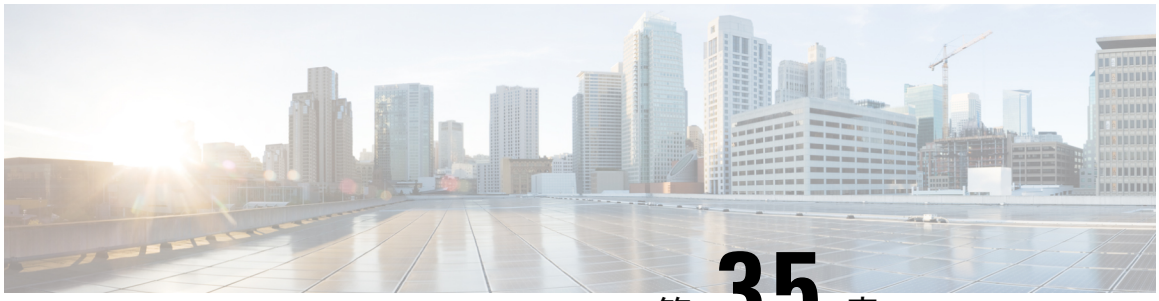
MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロード シェアリングの機能情報

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

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

機能名	リリース	機能情報
MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	Cisco IOS XE リリース 2.1	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。



第 35 章

6 つを超えるパラレル パスにおける IP パケットのロードシェアリング

ここでは、6 つを超えるパラレル パスにおける IP パケットのロードシェアリング機能について説明します。この機能により、マルチパス ロードシェアリングの目的でルーティング テーブルにインストールされるパラレル ルートの最大数を増やすことができます。

- 機能情報の確認 （675 ページ）
- 6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの概要 （676 ページ）
- その他の参考資料 （676 ページ）
- 6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの機能情報 （677 ページ）

機能情報の確認

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

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

6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの概要

6 つを超えるパラレル パスにおける IP パケットのロードシェアリング機能により、ルーティング テーブルにインストールできるパラレル ルートの最大数を増やすことができます。次のコマンドに対する最大数は、6 から 16 に増加しました。

- **maximum-paths**
- **maximum-paths eibgp**
- **maximum-paths ibgp**

show ip route summary コマンドの出力は、ルーティング テーブルでサポートされているパラレル ルートの数を表示するようにアップデートされました。

この機能の利点は次のとおりです。

- ルーティング テーブルのパラレル ルートがより柔軟なコンフィギュレーションとなる。
- より多くのリンクでマルチパス ロードシェアリングを設定する機能により、低速なリンクを使用してより高度な帯域幅集約を実現するコンフィギュレーションが可能となる。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
eBGP マルチパス ロード シェアリング	「MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング」モジュール
iBGP のマルチパス ロード シェアリング	「iBGP マルチパス ロード シェアリング」モジュール

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

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

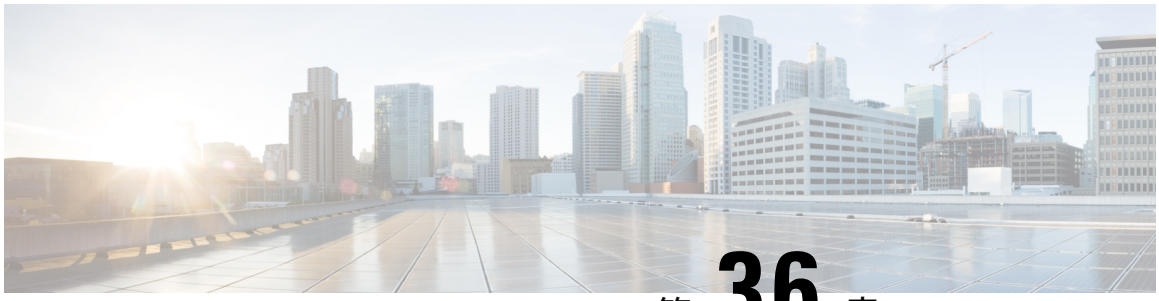
6 つを超えるパラレル パスにおける IP パケットのロードシェアリングの機能情報

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

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 *51 : 6* つを超えるパラレル パスにおける *IP* パケットのロードシェアリングの機能情報

機能名	リリース	機能情報
6つを超えるパラレルパスにおける IP パケットのロードシェアリング	Cisco IOS XE リリース 2.1	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。 この機能により、次のコマンドが変更されました。**maximum-paths**、 **maximum-paths eibgp**、**maximum-paths ibgp**、 **show ip route summary**



第 36 章

BGP ポリシー アカウンティング

ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティングは、異なるピア間で送受信される IP トラフィックを測定および分類します。ポリシー アカウンティングは入力インターフェイスでイネーブル化されます。また、コミュニティ リスト、自律システム番号、または自律システム パスなどのパラメータに基づくカウンタが割り当てられ、IP トラフィックを識別します。

- 機能情報の確認 （679 ページ）
- 前提条件 （679 ページ）
- BGP ポリシー アカウンティングに関する情報 （680 ページ）
- BGP ポリシー アカウンティングの設定方法 （681 ページ）
- BGP ポリシー アカウンティングの設定例 （685 ページ）
- その他の参考資料 （686 ページ）
- BGP ポリシー アカウンティングの機能情報 （687 ページ）

機能情報の確認

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

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

前提条件

BGP ポリシー アカウンティング機能を使用する前に、ルータで BGP および CEF または dCEF をイネーブルにする必要があります。

BGP ポリシー アカウンティングに関する情報

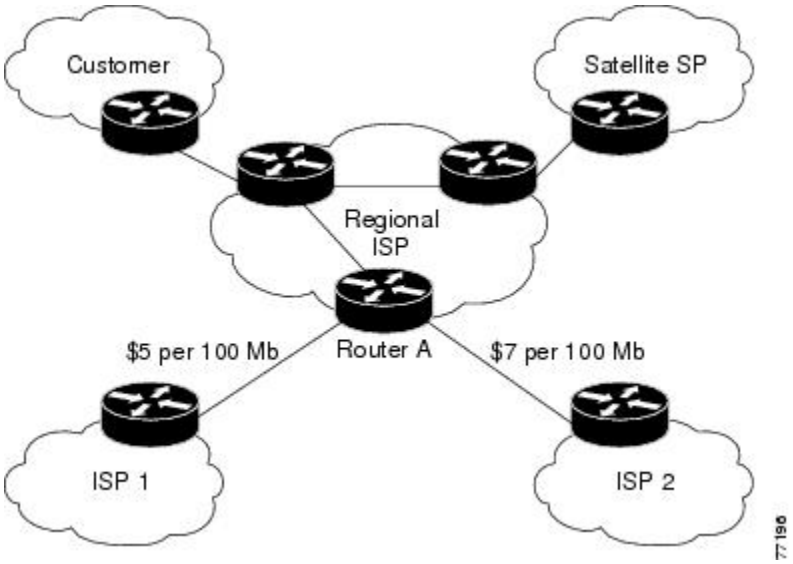
BGP ポリシー アカウンティングの概要

ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティングは、異なるピア間で送受信される IP トラフィックを測定および分類します。ポリシー アカウンティングは入力インターフェイスでイネーブル化されます。また、コミュニティ リスト、自律システム番号、または自律システム パスなどのパラメータに基づくカウンタが割り当てられ、IP トラフィックを識別します。

BGP の **table-map** コマンドを使用することで、ルーティング テーブルに追加されるプレフィックスは、BGP 属性、自律システム番号、または自律システム パス別に分類されます。パケットおよびバイト カウンタは、入力インターフェイス単位で増加します。トラフィックは、Cisco IOS ポリシーベースの分類子により、異なるトラフィック クラスを表す 8 つの可能性のあるバケットのうちの 1 つにマッピングされます。

BGP ポリシー アカウンティングを使用して、通過するルートに基づいてトラフィックのアカウンティングを行うことができます。サービス プロバイダー（SP）は、すべてのトラフィックをカスタマー別に識別してアカウンティングを行うことができ、それに応じて課金できます。下の図では、BGP ポリシー アカウンティングはルータ A で実装され、自律システム バケットにおけるパケットおよびバイト ボリュームを測定します。カスタマーは、国内、海外、または衛星経由の送信元からルーティングされたトラフィックに応じて適切に課金されます。

図 *59 : BGP* ポリシー アカウンティングのトポロジ例



自律システム番号を使用した BGP ポリシー アカウンティングは、インターネット サービス プロバイダー（ISP）間でのネットワーク回線のピアリングおよび中継の契約に関する設計を改善するために使用できます。

BGP ポリシー アカウンティングの利点

格差を付けた IP トラフィックのアカウンティング

BGP ポリシー アカウンティングは、自律システム番号、自律システム パス、またはコミュニティ リスト ストリングに基づいて IP トラフィックを分類し、パケットおよびバイト カウンタの値を増加させます。サービス プロバイダーは、ルート固有のトラフィック トラバースに基づいてトラフィックのアカウンティングを行い、請求に適用できます。

ネットワーク回線のピアリングおよび中継の契約に関する効率的な設計

BGP ポリシー アカウンティングをエッジ ルータに実装すると、ピアリングおよび中継の契約に関する設計の潜在的な改善点を明らかにすることができます。

BGP ポリシー アカウンティングの設定方法

BGP ポリシー アカウンティングの一致基準の指定

BGP ポリシー アカウンティングを設定する最初の作業は、一致する必要のある基準を指定することです。コミュニティ リスト、自律システム パス、または自律システム番号は、指定が可能で、後でルート マップを使用してマッチングできる BGP 属性の例です。

BGP ポリシー アカウンティングに使用する BGP 属性を指定し、ルート マップで一致基準を作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **ip community-list** *community-list-number* {**permit** | **deny**} *community-number*
2. Device(config)# **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. Device(config-route-map)# **match community-list** *community-list-number* [**exact**]
4. Device(config-route-map)# **set traffic-index** *bucket-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **ip community-list** *community-list-number* {**permit** | **deny**} *community-number*	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。 このステップは、指定する対象のコミュニティごとに繰り返す必要があります。
ステップ 2	Device(config)# **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]	ルート マップ コンフィギュレーション モードを開始し、ポリシー ルーティングの条件を定義します。 *map-name* 引数はルート マップを識別します。

	コマンドまたはアクション	目的
		オプションの **permit** および **deny** の各キーワードは一致基準および設定基準とともに機能し、パケットのアカウンティングを行う方法を制御します。 オプションの *sequence-number* 引数は、同一の名前ですでに設定されているルートマップのリスト内における新しいルート マップの場所を示します。
ステップ 3	Device(config-route-map)# **match community-list** *community-list-number* [**exact**]	BGP コミュニティを照合します。
ステップ 4	Device(config-route-map)# **set traffic-index** *bucket-number*	BGP ポリシー アカウンティングのルート マップの match 句を渡すパケットの出力先を示します。

IP トラフィックの分類および BGP ポリシー アカウンティングの有効化

ルート マップを定義して一致基準を指定した後、BGP ポリシー アカウンティングを有効にする前に、IP トラフィックを分類する方法を設定する必要があります。

ルーティング テーブルに追加される各プレフィックスは、**table-map** コマンドで、一致基準に基づいて BGP により分類されます。BGP ポリシー アカウンティングは、インターフェイスで **bgp-policy accounting** コマンドが設定されたときに有効化されます。

IP トラフィックを分類して BGP ポリシー アカウンティングを有効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **router bgp** *as-number*
2. Device(config-router)# **table-map** *route-map-name*
3. Device(config-router)# **network** *network-number* [**mask** *network-mask*]
4. Device(config-router)# **neighbor** *ip-address* **remote-as** *as-number*
5. Device(config-router)# **exit**
6. Device(config)# **interface** *interface-type interface-number*
7. Device(config-if)# **no ip directed-broadcast**
8. Device(config-if)# **ip address** *ip-address mask*
9. Device(config-if)# **bgp-policy accounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **router bgp** *as-number*	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Device(config-router)# **table-map** *route-map-name*	ルーティング テーブルに入力された BGP プレフィックスを分類します。
ステップ 3	Device(config-router)# **network** *network-number* [**mask** *network-mask*]	BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。
ステップ 4	Device(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	BGP ルーティング テーブルにエントリを追加して、BGP ピアを指定します。
ステップ 5	Device(config-router)# **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	Device(config)# **interface** *interface-type interface-number*	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 7	Device(config-if)# **no ip directed-broadcast**	ブロードキャストよりもインターフェイスが添付されたサブネットを宛先とする、誘導されたブロードキャストをドロップするようにインターフェイスを設定します。これはセキュリティの問題です。
ステップ 8	Device(config-if)# **ip address** *ip-address mask*	IP アドレスを使用してインターフェイスを設定します。
ステップ 9	Device(config-if)# **bgp-policy accounting**	インターフェイスに対して、BGP ポリシー アカウンティングを有効にします。

BGP ポリシー アカウンティングの確認

BGP ポリシー アカウンティングが動作しているかを確認するために、次の手順を実行します。

手順の概要

1. **detail** キーワードを指定して **show ip cef** EXEC コマンドを入力し、指定されたプレフィックスに割り当てられているアカウンティング バケットを調べます。
2. 手順 1 で使用したのと同じプレフィックス（192.168.5.0）について **show ip bgp** EXEC コマンドを入力し、このプレフィックスに割り当てられているコミュニティを調べます。
3. **show cef interface policy-statistics** EXEC コマンドを入力し、インターフェイス単位のトラフィック統計情報を表示します。

手順の詳細

ステップ 1 **detail** キーワードを指定して **show ip cef** EXEC コマンドを入力し、指定されたプレフィックスに割り当てられているアカウンティング バケットを調べます。

この例では、プレフィックス 192.168.5.0 についての出力が表示されます。この例では、アカウンティング バケット番号「4」（traffic_index 4）がこのプレフィックスに割り当てられていることが示されています。

例：

```
Device# show ip cef 192.168.5.0 detail

192.168.5.0/24, version 21, cached adjacency to POS7/2
0 packets, 0 bytes, traffic_index 4
  via 10.14.1.1, 0 dependencies, recursive
   next hop 10.14.1.1, POS7/2 via 10.14.1.0/30
   valid cached adjacency
```

ステップ 2 手順 1 で使用したのと同じプレフィックス（192.168.5.0）について **show ip bgp** EXEC コマンドを入力し、このプレフィックスに割り当てられているコミュニティを調べます。

この例では、プレフィックス 192.168.5.0 についての出力が表示されます。この例では、コミュニティ「100:197」がこのプレフィックスに割り当てられていることが示されています。

例：

```
Device# show ip bgp 192.168.5.0

BGP routing table entry for 192.168.5.0/24, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
  100
    10.14.1.1 from 10.14.1.1 (32.32.32.32)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 100:197
```

ステップ 3 **show cef interface policy-statistics** EXEC コマンドを入力し、インターフェイス単位のトラフィック統計情報を表示します。

この例では、各アカウンティング バケットに割り当てられているパケットおよびバイトの数が出力に表示されます。

例：

```
Device# show cef interface policy-statistics

POS7/0 is up (if_number 8)
Bucket    Packets               Bytes
1          0                      0
2          0                      0
3          50                     5000
4          100                    10000
5          100                    10000
6          10                     1000
7          0                      0
8          0                      0
```

BGP ポリシー アカウンティングのモニタリングおよびメンテナンス

コマンド	目的
Device# **show cef interface** [*type number*] **policy-statistics**	（任意）すべてのインターフェイスに対する CEF ポリシー統計情報の詳細を表示します。
Device# **show ip bgp** [*network*] [*network mask*] [**longer-prefixes**]	（任意）BGP ルーティング テーブルのエントリを表示します。
Device# **show ip cef** [*network* [*mask*]] [**detail**]	（任意）転送情報ベース（FIB）のエントリまたは FIB の概要を表示します。

BGP ポリシー アカウンティングの設定例

例：BGP ポリシー アカウンティングの一致基準の指定

次の例では、BGP コミュニティがコミュニティ リストに指定され、set_bucket という名前のルート マップが、**set traffic-index** コマンドを使用して、各コミュニティ リストが特定のアカウンティング バケットに一致するように設定されます。

```
ip community-list 30 permit 100:190
ip community-list 40 permit 100:198
ip community-list 50 permit 100:197
ip community-list 60 permit 100:296
!
route-map set_bucket permit 10
match community 30
set traffic-index 2
!
route-map set_bucket permit 20
match community 40
set traffic-index 3
!
route-map set_bucket permit 30
match community 50
set traffic-index 4
!
route-map set_bucket permit 40
match community 60
set traffic-index 5
```

例：IP トラフィックの分類および BGP ポリシー アカウンティングの有効化

次に、POS インターフェイス 7/0 で BGP ポリシー アカウンティングが有効化され、**table-map** コマンドにより IP ルーティング テーブルが BGP で学習されたルートによりアップデートされたときに、バケット番号が変更される例を示します。

```
router bgp 65000
 table-map set_bucket
 network 10.15.1.0 mask 255.255.255.0
 neighbor 10.14.1.1 remote-as 65100
!
ip classless
ip bgp-community new-format
!
interface POS7/0
 ip address 10.15.1.2 255.255.255.0
 no ip directed-broadcast
 bgp-policy accounting
 no keepalive
 crc 32
 clock source internal
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
Cisco Express Forwarding（CEF）および分散型 CEF（dCEF）	『Cisco IOS IP Switching Command Reference』
Cisco Express Forwarding（CEF）および分散型 CEF（dCEF）の設定情報	『*Cisco IOS Switching Services Configuration Guide*』の「CEF Overview」モジュール

MIB

MIB	MIB のリンク
• CISCO-BGP-POLICY-ACCOUNTING-MIB （注） CISCO-BGP-POLICY-ACCOUNTING-MIB は、Cisco IOS Release 12.0(9)S、12.0(17)ST、およびそれ以降のリリースだけで使用可能です。この MIB は、いずれのメインラインおよび T トレイン リリースでも使用できません。	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 ポリシー アカウン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 *52 : BGP* ポリシー アカウンティングの機能情報

機能名	リリース	機能情報
BGP ポリシー アカウンティング	12.0(9)S 12.0(17)ST 12.2(13)T 15.0(1)S 12.2(50)SY Cisco IOS XE Release 3.8S	ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティングは、異なるピア間で送受信される IP トラフィックを測定および分類します。ポリシー アカウンティングは入力インターフェイスでイネーブル化されます。また、コミュニティ リスト、自律システム番号、または自律システム パスなどのパラメータに基づくカウンタが割り当てられ、IP トラフィックを識別します。 次のコマンドが導入または変更されました。 • **bgp-policy** • **set traffic-index** • **show cef interface policy-statistics** • **show ip bgp** • **show ip cef**

第 37 章

BGP ポリシーアカウンティング出力インターフェイス アカウンティング

ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティング（PA）では、異なるピア間で送受信される IP トラフィックを測定および分類します。ポリシーアカウンティングは、以前は入力インターフェイスだけで使用可能でした。BGP ポリシー アカウンティング出力インターフェイス アカウンティング機能により、BGP PA を出力インターフェイスでイネーブルにし、インターフェイスの入力トラフィックおよび出力トラフィックの両方の送信元アドレスに基づくアカウンティングを組み込むための複数の拡張機能が追加されます。IP トラフィックを識別するために、コミュニティ リスト、自律システム番号、または自律システム パスなどのパラメータに基づくカウンタが割り当てられます。

- 機能情報の確認 （689 ページ）
- BGP PA 出力インターフェイス アカウンティングの前提条件 （690 ページ）
- BGP PA 出力インターフェイス アカウンティングに関する情報 （690 ページ）
- BGP PA 出力インターフェイス アカウンティングの設定方法 （692 ページ）
- BGP PA 出力インターフェイス アカウンティングの設定例 （698 ページ）
- その他の参考資料 （699 ページ）
- BGP ポリシーアカウンティング出力インターフェイス アカウンティングの機能情報 （701 ページ）
- 用語集 （702 ページ）

機能情報の確認

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

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

BGP PA 出力インターフェイス アカウンティングの前提条件

BGP ポリシーアカウンティング出力インターフェイスアカウンティング機能を使用する前に、BGP および Cisco Express Forwarding（CEF）または分散型 CEFをルータで有効にする必要があります。

BGP PA 出力インターフェイス アカウンティングに関する情報

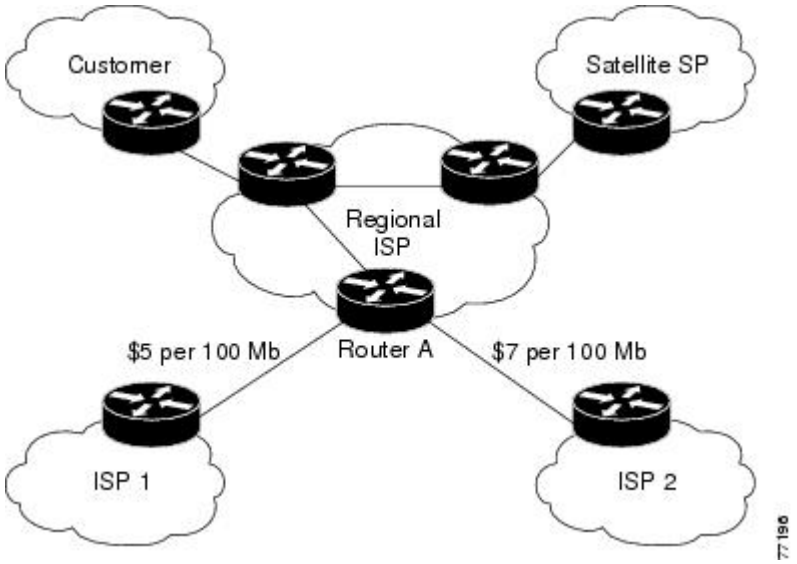
BGP PA 出力インターフェイス アカウンティング

BGP を使用したポリシー アカウンティングでは、異なるピア間で送受信される IP トラフィックを測定および分類します。BGP PA は元々、入力インターフェイスだけで使用可能でした。BGP PA 出力インターフェイス アカウンティングでは、BGP PA を出力インターフェイスでイネーブルにし、インターフェイスの入力トラフィックおよび出力トラフィックの両方の送信元アドレスに基づくアカウンティングを組み込むための複数の拡張機能が導入されています。IP トラフィックを識別するために、コミュニティ リスト、自律システム番号、または自律システム パスなどのパラメータに基づくカウンタが割り当てられます。

BGP の **table-map** コマンドを使用することで、ルーティング テーブルに追加されるプレフィックスは、BGP 属性、自律システム番号、または自律システム パス別に分類されます。パケット カウンタおよびバイト カウンタは、入力インターフェイスまたは出力インターフェイス単位で増加します。シスコのポリシーベースの分類機能によって、トラフィックは異なるトラフィック クラスを表す 8 つのうちいずれか 1 つのバケットにマッピングされます。

BGP PA を使用することで、トラフィックの発信元またはトラフィックが通過したルートに応じてトラフィックのアカウンティングを行うことができます。サービス プロバイダー（SP）は、すべてのトラフィックをカスタマー別に識別してアカウンティングを行うことができ、それに応じて課金できます。下の図では、BGP PA はルータ A で実装され、自律システム バケットにおけるパケットおよびバイト ボリュームを測定します。カスタマーは、国内、海外、または衛星経由の送信元からルーティングされたトラフィックに応じて適切に課金されます。

図 *60 : BGP* ポリシー アカウンティングのトポロジ例



自律システム番号を使用したBGPポリシーアカウンティングは、インターネットサービスプロバイダー（ISP）間でのネットワーク回線のピアリングおよび中継の契約に関する設計を改善するために使用できます。

BGP PA 出力インターフェイス アカウンティングの利点

格差を付けた IP トラフィックのアカウンティング

BGP ポリシー アカウンティングは、自律システム番号、自律システム パス、またはコミュニティ リスト ストリングに基づいてIPトラフィックを分類し、パケットおよびバイト カウンタの値を増加させます。ポリシーアカウンティングは、送信元アドレスを基本とすることもできます。サービスプロバイダーはトラフィックのアカウンティングを行い、トラフィックの発信元または特定のトラフィックが通過したルートに応じた課金を適用できます。

ネットワーク回線のピアリングおよび中継の契約に関する効率的な設計

BGP ポリシー アカウンティングをエッジ ルータに実装すると、ピアリングおよび中継の契約に関する設計の潜在的な改善点を明らかにすることができます。

BGP PA 出力インターフェイス アカウンティングの設定方法

BGP PA の一致基準の指定

BGP PA を設定する最初の作業は、一致させる必要がある基準を指定することです。コミュニティ リスト、自律システムパス、または自律システム番号は、指定が可能で、後でルートマップを使用してマッチングできる BGP 属性の例です。BGP PA に使用する BGP 属性を指定し、ルート マップ内の一致基準を作成するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip community-list** {*standard-list-number* | *expanded-list-number* [*regular-expression*] | {**standard** | **expanded**} *community-list-name*} {**permit** | **deny**} {*community-number* | *regular-expression*}
4. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
5. **match community-list** *community-list-number* [**exact**]
6. **set traffic-index** *bucket-number*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 community-list** {*standard-list-number* | *expanded-list-number* [*regular-expression*] | {**standard** | **expanded**} *community-list-name*} {**permit** | **deny**} {*community-number* | *regular-expression*} 例： `Device(config)# ip community-list 30 permit 100:190`	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。 • 指定する各コミュニティについて、このステップを繰り返します。

	コマンドまたはアクション	目的
ステップ 4	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map set_bucket permit 10`	ルート マップ コンフィギュレーション モードを開始し、ポリシールーティングの条件を定義します。 • *map-name* 引数はルート マップを識別します。 • オプションの **permit** および **deny** の各キーワードは一致基準および設定基準とともに機能し、パケットのアカウンティングを行う方法を制御します。 • オプションの *sequence-number* 引数は、同一の名前ですでに設定されているルートマップのリスト内における新しいルートマップの場所を示します。
ステップ 5	**match community-list** *community-list-number* [**exact**] 例： `Router(config-route-map)# match community-list 30`	BGP コミュニティを照合します。
ステップ 6	**set traffic-index** *bucket-number* 例： `Device(config-route-map)# set traffic-index 2`	BGP ポリシー アカウンティングのルート マップの match 句を渡すパケットの出力先を示します。
ステップ 7	**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。

IP トラフィックの分類および BGP PA の有効化

ルート マップを定義して一致基準を指定した後、BGP ポリシー アカウンティングを有効にする前に、IP トラフィックを分類する方法を設定する必要があります。

table-map コマンドを使用することで、BGP ではルーティング テーブルに追加した各プレフィックスを、一致基準に応じて分類します。BGP ポリシー アカウンティングは、インターフェイスで **bgp-policy accounting** コマンドが設定されたときに有効化されます。

IP トラフィックを分類して BGP ポリシー アカウンティングを有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *as-number*
4. **table-map** *route-map-name*
5. **network** *network-number* [**mask** *network-mask*]
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **bgp-policy accounting** [**input** | **output**] [**source**]
11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、指定されたルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、BGP 自律システム番号を識別します。
ステップ 4	**table-map** *route-map-name* 例： `Device(config-router)# table-map set_bucket`	ルーティング テーブルに入力された BGP プレフィックスを分類します。
ステップ 5	**network** *network-number* [**mask** *network-mask*] 例： `Device(config-router)# network 10.15.1.0 mask 255.255.255.0`	BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。
ステップ 6	**neighbor** *ip-address* **remote-as** *as-number* 例： `Device(config-router)# neighbor 10.14.1.1 remote-as 65100`	BGP ルーティング テーブルにエントリを追加して、BGP ピアを指定します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 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 8	**interface** *type number* 例： `Device(config)# interface POS 7/0`	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。 • *type* 引数は、インターフェイスのタイプを識別します。 • *number* 引数は、インターフェイスのスロット番号およびポート番号を識別します。インターフェイスのタイプと番号の間のスペースは任意です。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip-address 10.15.1.2 255.255.255.0`	IP アドレスを使用してインターフェイスを設定します。
ステップ 10	**bgp-policy accounting** [**input** | **output**] [**source**] 例： `Device(config-if)# bgp-policy accounting input source`	インターフェイスに対して、BGP ポリシー アカウンティングを有効にします。 • 任意の **input** または **output** キーワードを使用すると、ルータに入力または出力されるいずれかのトラフィックのアカウンティングを行うことができます。デフォルトでは、BGPポリシーアカウンティングは、ルータに入力されるトラフィックに基づきます。 • 任意の **source** キーワードを使用すると、送信元アドレスに基づいてトラフィックのアカウンティングを行うことができます。
ステップ 11	**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。

BGP ポリシー アカウンティングの確認

BGPポリシーアカウンティングが動作していることを確認するには、次の作業を実行します。

手順の概要

1. **show ip cef** [*network* [*mask*]] [**detail**]
2. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
3. **show cef interface** [*type number*] **policy-statistics** [**input** | **output**]
4. **show cef interface** [*type number*] [**statistics**] [**detail**]

手順の詳細

ステップ 1 **show ip cef** [*network* [*mask*]] [**detail**]

detail キーワードを指定して **show ip cef** コマンドを入力し、指定されたプレフィックスに割り当てられているアカウンティング バケットを調べます。

この例では、プレフィックス 192.168.5.0 についての出力が表示されます。このプレフィックスにアカウンティング バケット番号 4（traffic_index 4）が割り当てられていることが示されます。

例：

```
Device# show ip cef 192.168.5.0 detail

192.168.5.0/24, version 21, cached adjacency to POS7/2
0 packets, 0 bytes, traffic_index 4
  via 10.14.1.1, 0 dependencies, recursive
   next hop 10.14.1.1, POS7/2 via 10.14.1.0/30
   valid cached adjacency
```

ステップ 2 **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]

手順 1 で使用したのと同じプレフィックス（192.168.5.0）について **show ip bgp** コマンドを入力し、このプレフィックスに割り当てられているコミュニティを調べます。

この例では、プレフィックス 192.168.5.0 についての出力が表示されます。この例では、コミュニティ「100:197」がこのプレフィックスに割り当てられていることが示されています。

例：

```
Device# show ip bgp 192.168.5.0

BGP routing table entry for 192.168.5.0/24, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
  100
    10.14.1.1 from 10.14.1.1 (32.32.32.32)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 100:197
```

ステップ 3 **show cef interface** [*type number*] **policy-statistics** [**input** | **output**]

インターフェイス単位のトラフィック統計情報を表示します。

この例では、各アカウンティング バケットに割り当てられているパケットおよびバイトの数が出力に表示されます。

例：

```
Device# show cef interface policy-statistics input

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  BGP based Policy accounting on input is enabled
 Index         Packets          Bytes
     1            9999         999900
     2               0              0
     3               0              0
     4               0              0
     5               0              0
     6               0              0
     7               0              0
     8               0              0
     9               0              0
    10               0              0
    11               0              0
    12               0              0
    13               0              0
    14               0              0
    15               0              0
    16               0              0
    17               0              0
    18               0              0
    19               0              0
    20               0              0
    21               0              0
    22               0              0
    23               0              0
    24               0              0
    25               0              0
    26               0              0
    27               0              0
    28               0              0
    29               0              0
    30               0              0
    31               0              0
    32               0              0
    33               0              0
    34            1234         123400
    35               0              0
    36               0              0
    37               0              0
    38               0              0
    39               0              0
    40               0              0
    41               0              0
    42               0              0
    43               0              0
    44               0              0
    45            1000         100000
    46               0              0
    47               0              0
    48               0              0
    49               0              0
    50               0              0
    51               0              0
    52               0              0
    53               0              0
    54            5123        1198782
    55               0              0
    56               0              0
```

```
  57                0                0
  58                0                0
  59                0                0
  60                0                0
  61                0                0
  62                0                0
  63                0                0
  64                0                0
```

ステップ 4 **show cef interface** [*type number*] [**statistics**] [**detail**]

指定したインターフェイスの BGP ポリシー アカウンティングの状態を表示します。

この例では、BGP ポリシー アカウンティングは、ファストイーサネット インターフェイス 1/0/0 の入力トラフィックに基づいて設定されていることが出力に示されています。

例：

```
Device# show cef interface Fast Ethernet 1/0/0

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
  Hardware idb is FastEthernet1/0/0 (6)
  Software idb is FastEthernet1/0/0 (6)
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0xE8001A82 (0xE8001A82)
  IP MTU 1500
```

BGP PA 出力インターフェイス アカウンティングの設定例

BGP ポリシー アカウンティングの一致基準の指定例

次の例では、BGP コミュニティがコミュニティ リストに指定され、set_bucket という名前のルート マップが、**set traffic-index** コマンドを使用して、各コミュニティ リストが特定のアカウンティング バケットに一致するように設定されます。

```
ip community-list 30 permit 100:190
ip community-list 40 permit 100:198
ip community-list 50 permit 100:197
ip community-list 60 permit 100:296
!
route-map set_bucket permit 10
 match community-list 30
 set traffic-index 2
!
route-map set_bucket permit 20
 match community-list 40
 set traffic-index 3
!
route-map set_bucket permit 30
 match community-list 50
 set traffic-index 4
!
route-map set_bucket permit 40
 match community-list 60
 set traffic-index 5
```

IP トラフィックの分類および BGP ポリシー アカウンティングの有効化の例

次の例では、BGP ポリシー アカウンティングが POS インターフェイス 2/0/0 で有効になります。ポリシー アカウンティング基準は入力トラフィックの送信元アドレスに基づいており、**table-map** コマンドを使用して、IP ルーティング テーブルが BGP から学習したルートで更新されるときにバケット番号を変更するようにします。

```
router bgp 65000
 table-map set_bucket
 network 10.15.1.0 mask 255.255.255.0
 neighbor 10.14.1.1 remote-as 65100
!
ip classless
ip bgp-community new-format
!
interface POS2/0/0
 ip address 10.15.1.2 255.255.255.0
 bgp-policy accounting input source
 no keepalive
 crc 32
 clock source internal
```

その他の参考資料

以下の各項では、BGP ポリシー アカウンティング出力インターフェイス アカウンティング機能に関する関連資料を示します。

関連資料

関連項目	マニュアル タイトル
BGP 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、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
スイッチング 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、使用上の注意事項、および例	『*Cisco IOS IP Switching Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

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

テクニカル サポート

説明	リンク
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

BGPポリシーアカウンティング出力インターフェイスアカウン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 *53 : BGP* ポリシー アカウンティング出力インターフェイス アカウンティングの機能情報

機能名	リリース	機能情報
BGP ポリシー アカウンティング	Cisco IOS XE Release 2.1	BGP ポリシー アカウンティングは、異なるピア間で送受信される IP トラフィックを測定および分類します。 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。

機能名	リリース	機能情報
BGP ポリシーアカウンティング出力インターフェイス アカウンティング	Cisco IOS XE Release 2.1	この機能により、BGP PA を出力インターフェイスで有効にし、インターフェイスの入力トラフィックおよび出力トラフィックの両方の送信元アドレスに基づくアカウンティングを組み込むための複数の拡張機能が追加されます。 この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。 この機能により、次のコマンドが導入または変更されました。**bgp-policy**、**set traffic-index**、**show cef interface**、**show cef interface policy-statistics**
BGP ポリシーアカウンティングの SNMP サポート	Cisco IOS XE Release 2.1	CISCO-BGP-POLICY-ACCOUNTING-MIB が導入されました。 この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。

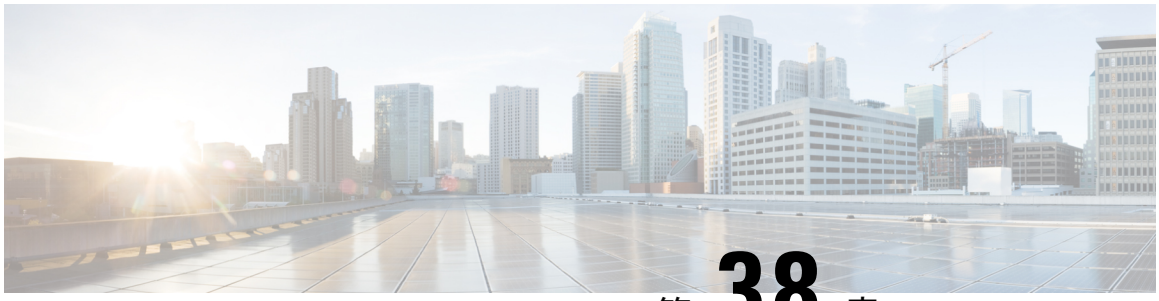
用語集

AS ：自律システム。独立した独自のルーティング ポリシーを持ち、単一権限によって管理されるルーティング ドメインを表す IP 用語です。

BGP ：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとの間で到着可能性情報を交換するドメイン間ルーティング プロトコルです。

CEF ：Cisco Express Forwarding（シスコ エクスプレス フォワーディング）。

dCEF ：distributed Cisco Express Forwarding（分散型シスコ エクスプレス フォワーディング）。



第 38 章

BGP コスト コミュニティ

BGP コスト コミュニティ機能により、コスト拡張コミュニティ属性が導入されます。コスト コミュニティとは、非推移的な拡張コミュニティ属性で、内部 BGP（iBGP）およびコンフェデレーション ピアには渡されますが、外部 BGP（eBGP）ピアには渡されません。コスト コミュニティ機能により、コスト値を特定のルートに割り当てることで、ローカル ルート プリファレンスをカスタマイズし、ベスト パス選択プロセスに反映させることができます。

Cisco IOS Release 12.0(27)S、12.3(8)T、12.2(25)S、およびそれ以降のリリースでは、VPN およびバックドア リンクを備えた多様な EIGRP MPLS VPN ネットワーク トポロジのためにサポートが導入されました。

- 機能情報の確認 （703 ページ）
- BGP コスト コミュニティ機能の前提条件 （704 ページ）
- BGP コスト コミュニティ機能の制約事項 （704 ページ）
- BGP コスト コミュニティ機能に関する情報 （704 ページ）
- BGP コスト コミュニティ機能の設定方法 （708 ページ）
- BGP コスト コミュニティ機能の設定例 （710 ページ）
- その他の参考資料 （712 ページ）
- BGP コスト コミュニティの機能情報 （714 ページ）

機能情報の確認

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

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

BGP コスト コミュニティ機能の前提条件

このマニュアルは、BGPがネットワークで設定されていること、およびピアリングが確立されていることを前提としています。

BGP コスト コミュニティ機能の制約事項

- BGPコストコミュニティ機能が設定できるのは、自律システムまたはコンフェデレーション内だけです。コスト コミュニティは非推移的な拡張コミュニティ属性で、iBGP およびコンフェデレーション ピアだけに渡され、eBGP ピアには渡されません。
- コスト コミュニティ フィルタリングを設定するには、BGP コスト コミュニティ機能がすべての自律システムまたはコンフェデレーションでサポートされている必要があります。潜在的なルーティング ループを回避するために、コスト コミュニティはローカルの自律システムまたはコンフェデレーション全体に一貫して適用される必要があります。
- 単一のルートマップ ブロックまたはシーケンスにおいて、**set extcommunity cost** コマンドで複数の cost community set 句を設定することも可能です。ただし、各 set 句は、各挿入ポイント（POI）に対し異なる ID 値（0 ～ 255）を持つよう設定する必要があります。ID 値は、その他の属性がすべて等しい場合に、プリファレンスを決定します。最も低い ID 値が優先されます。

BGP コスト コミュニティ機能に関する情報

BGP コスト コミュニティの概要

コスト コミュニティは非推移的な拡張コミュニティ属性で、iBGP およびコンフェデレーション ピアには渡されますが、eBGP ピアには渡されません。BGP コスト コミュニティ機能のコンフィギュレーションにより、ローカルの自律システムまたはコンフェデレーションにおける BGP ベスト パス選択プロセスがカスタマイズできます。

コスト コミュニティ属性は、ルート マップで **set extcommunity cost** コマンドを設定することにより、内部ルートに適用されます。cost community set 句は、コスト コミュニティ ID 番号（0 ～ 255）およびコスト番号（0 ～ 4294967295）で設定されます。コスト コミュニティ ID 番号によってパスの優先度が判断されます。最も低いコスト コミュニティ ID 番号を持つパスが優先されます。

コストコミュニティ属性で特別に設定されていないパスは、デフォルトのコスト番号値である 2147483647（0 ～ 4294967295 の中央値）が割り当てられ、ベスト パス選択プロセスにより評価されます。2 つのパスが同じコスト コミュニティ ID 番号を使用して設定されている場合、パス選択プロセスでは最も低いコスト番号のパスが優先されます。コスト拡張コミュニティ属

性は、**neighbor send-community** コマンドで拡張コミュニティ交換が有効化されたとき、iBGP ピアに伝播します。

cost community set 句で設定されたルート マップの適用に使用できるコマンドは、次のとおりです。

- **aggregate-address**
- **neighbor default-originate route-map {in | out}**
- **neighbor route-map**
- **network route-map**
- **redistribute route-map**

BGP コストコミュニティによるベスト パス選択プロセスへの影響

BGP ベスト パス選択プロセスは、挿入ポイント（POI）においてコスト コミュニティ属性の影響を受けます。デフォルトでは、POI は内部ゲートウェイ プロトコル（IGP）メトリック比較に準拠します。同一の宛先に向かう複数のパスを受信したとき、BGP はベスト パス選択プロセスを使用して、いずれのパスがベスト パスであるかを決定します。ベスト パスは BGP により自動的に決定され、ルーティング テーブルにインストールされます。複数の等価コスト パスが使用可能な場合、POI で特定のパスにプリファレンスを割り当てることができます。ローカルのベスト パス選択で POI が有効でない場合は、コスト コミュニティ属性は暗黙的に無視されます。

コスト コミュニティ属性を使用して、同一の POI に対し複数のパスを設定できます。最も低いコスト コミュニティ ID を持つパスが最優先で検討されます。つまり、特定の POI に対するすべてのコスト コミュニティ パスは、最も低いコスト コミュニティを持つパスから考慮されていきます。コストコミュニティを持たないパス（POI でコミュニティ ID が評価されるもの）には、デフォルトのコミュニティ コスト値（2147483647）が割り当てられます。コストコミュニティ値が等しい場合、コスト コミュニティ比較は、その POI で次に低いコミュニティ ID に進みます。

（注） パスにコスト コミュニティ属性が設定されていない場合、ベスト パス選択プロセスはそのパスにデフォルトのコスト値（最大値 [4294967295] の半分である 2147483647）が割り当てられているものと見なします。

POI でコストコミュニティ属性を適用することで、ローカルの自律システムまたはコンフェデレーションにおける任意の部分にあるピアを起点とするか、このピアで学習したパスに、値を割り当てることができるようになります。コスト コミュニティは、ベスト パス選択プロセス中の「タイブレーカー」として使用できます。同一の自律システムまたはコンフェデレーションにおける別個の等コスト パスに対し、コスト コミュニティのインスタンスを複数設定できます。たとえば、複数の等コスト出口ポイントがあるネットワークにおいて、特定の出口パスに、より低いコスト コミュニティ値を適用すれば、そのパスは BGP ベスト パス選択プロセス

により優先されることになります。「マルチエグジット IGP ネットワークにおけるルート プリファレンスの反映」の項に記載されているシナリオを参照してください。

集約ルートおよびマルチパスに対するコストコミュニティのサポート

BGP コストコミュニティ機能により、集約ルートおよびマルチパスがサポートされています。コストコミュニティ属性は、いずれかのルートのタイプに適用できます。コストコミュニティ属性は、コスト コミュニティ属性を伝送するコンポーネント ルートから集約ルートまたはマルチパス ルートに渡されます。伝送されるのは一意の ID だけであり、個々のコンポーネント ルートの中で最も高いコストが、ID 単位で集約に適用されます。複数のコンポーネント ルートに同一の ID が含まれる場合は、設定されている最大のコストがルートに適用されます。たとえば、次の 2 つのコンポーネント ルートにインバウンド ルート マップ経由でコスト コミュニティ属性が設定されているとします。

- 10.0.0.1 (POI=IGP, ID=1, Cost=100)
- 192.168.0.1 (POI=IGP, ID=1, Cost=200)

これらのコンポーネント ルートがマルチパスとして集約または設定された場合、コスト値 200（POI=IGP、ID=1、コスト=200）が最も高いコストとなるため、このコスト値がアドバタイズされます。

1 つ以上のコンポーネント ルートがコスト コミュニティ属性を伝送しない場合、またはこれらのコンポーネント ルートに異なる ID が設定されている場合は、デフォルト値（2147483647）が集約ルートまたはマルチパス ルートに対してアドバタイズされます。たとえば、次の 3 つのコンポーネント ルートにインバウンド ルート マップ経由でコスト コミュニティ属性が設定されているとします。ただし、これらのコンポーネント ルートには 2 つの異なる ID が設定されています。

- 10.0.0.1 (POI=IGP, ID=1, Cost=100)
- 172.16.0.1 (POI=IGP, ID=2, Cost=100)
- 192.168.0.1 (POI=IGP, ID=1, Cost=200)

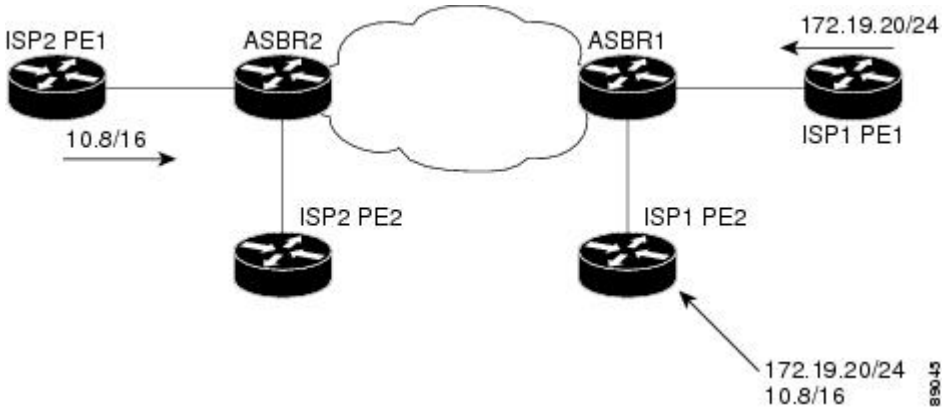
アドバタイズされる単一のパスには、次のように集約コスト コミュニティが含まれます。

- {POI=IGP, ID=1, Cost=2147483647} {POI=IGP, ID=2, Cost=2147483647}

マルチエグジット IGP ネットワークにおけるルート プリファレンスの反映

下の図に、エッジに 2 つの自律システム境界ルータ（ASBR）がある内部ゲートウェイ プロトコル（IGP）ネットワークを示します。各 ASBR は、ネットワーク 10.8/16 に対して等コスト パスを持ちます。

図 *61 :* マルチエグジット ポイント *IGP* ネットワーク



BGP では、両パスは等しいと見なされます。マルチパス ロードシェアリングが設定されている場合、両方のパスがルーティング テーブルにインストールされ、トラフィックのロード バランスに使用されます。マルチパス ロード バランシングが設定されていない場合、BGP により最初にベストパスであると学習されたパスが選択され、ルーティングテーブルにインストールされます。この動作は、一部の条件下では望ましくない場合があります。たとえば、パスは最初に ISP1 PE2 から学習されますが、ISP1 PE2 と ASBR1 間のリンクは低速リンクです。

コスト コミュニティ属性のコンフィギュレーションを使用して ASBR2 が学習したパスにより低いコスト コミュニティ値を適用することで、BGP ベスト パス選択プロセスに影響を与えることができます。たとえば、次のコンフィギュレーションは ASBR2 に適用されます。

```
route-map ISP2_PE1 permit 10
 set extcommunity cost 1 1
 match ip address 13
!
ip access-list 13 permit 10.8.0.0 0.0.255.255
```

上のルートマップでは、コスト コミュニティ番号値の 1 がルート 10.8.0.0 に適用されます。デフォルトでは、ASBR1 で学習したパスにはコスト コミュニティ値 2147483647 が割り当てられます。ASBR2 で学習したパスのコスト コミュニティ値の方が低いため、こちらのパスが優先されます。

バックドア リンクを持つ EIGRP MPLS VPN Provider Edge-Customer Edge（PE-CE）に対する BGP コスト コミュニティ サポート

EIGRP Site of Origin（SoO）BGP コスト コミュニティ サポートの導入以前は、BGP ピアが学習したルートよりもローカル ソース ルートの方が BGP により優先されました。バックドア リンクの方が先に学習された場合、BGP により EIGRP MPLS VPN トポロジにおけるバックドア リンクが優先されます。（バックドア リンクまたはルートは、遠隔地の拠点と主拠点間の VPN の外で設定される接続です。たとえば、遠隔地の拠点を企業のネットワークに接続する WAN リース ラインです）。

VPN およびバックドア リンクが混在する EIGRP VPN ネットワーク トポロジをサポートするために、BGP コスト コミュニティ機能で「プレベストパス」挿入ポイント（POI）が導入され

ました。この POI は BGP に再配布される EIGRP ルートに自動的に適用されます。「プレベストパス」POI は、EIGRP ルート タイプおよびメトリックを伝送します。この POI は、BGP がその他のあらゆる比較ステップの前にこの POI を考慮するように影響を与えておくことで、ベストパス計算プロセスに作用します。設定は必要ありません。Cisco IOS Release 12.0(27)S がプロバイダーエッジ（PE）、カスタマーエッジ（CE）、またはバック ドアルータにインストールされている場合、この機能は自動的に EIGRP VPN 拠点に対して有効になります。

EIGRP MPLS VPN の設定については、Cisco IOS Release 12.0(27)S の『MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge』マニュアルを参照してください。

EIGRP MPLS VPN PE-CE Site of Origin（SoO）機能の詳細については、Cisco IOS Release 12.0(27)S の『EIGRP MPLS VPN PE-CE Site of Origin (SoO)』機能マニュアルを参照してください。

BGP コスト コミュニティ機能の設定方法

BGP コスト コミュニティの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **ipv6** [**multicast** | **unicast**] | **vpnv4** [**unicast**]
6. **neighbor** *ip-address* **route-map** *map-name* {**in** | **out**}
7. **exit**
8. **route-map** *map-name* {**permit** | **deny**} [*sequence-number*]
9. **set extcommunity cost** [**igp**] *community-id cost-value*
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	**enable** 例： `Device> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 50000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 101`	指定したネイバーまたはピアグループとのピアリングを確立します。
ステップ 5	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **ipv6** [**multicast** | **unicast**] | **vpnv4** [**unicast**] 例： `Device(config-router)# address-family ipv4`	ルータをアドレス ファミリ コンフィギュレーション モードにします。
ステップ 6	**neighbor** *ip-address* **route-map** *map-name* {**in** | **out**} 例： `Device(config-router)# neighbor 10.0.0.1 route-map MAP-NAME in`	指定したネイバーまたはピアグループに対し着信または発信ルート マップを適用します。
ステップ 7	**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 8	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map MAP-NAME permit 10`	ルート マップ コンフィギュレーション モードを開始し、ルート マップを作成または設定します。
ステップ 9	**set extcommunity cost** [**igp**] *community-id cost-value* 例： `Device(config-route-map)# set extcommunity cost 1 100`	set 句を作成しコスト コミュニティ属性を適用します。 • 各ルート マップ ブロックまたはシーケンスで複数の cost community set 句を設定できます。各 cost community set 句には、異なる ID（0 ～ 255）を持たせる必要があります。その他すべての属性が等しい場合、最も低い *cost-value* を持つ cost community set 句がベスト パス選択プロセスにより優先されます。

	コマンドまたはアクション	目的
		• コスト コミュニティ属性が設定されていないパスにはデフォルトの *cost-value* が割り当てられます。この値は最大値（4294967295）の半分である 2147483647 です。
ステップ 10	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP コスト コミュニティの設定確認

BGP コスト コミュニティ コンフィギュレーションは、ローカルまたは特定のネイバーに対して確認できます。コスト コミュニティのローカル コンフィギュレーションを確認するには、**show route-map** または **show running-config** コマンドを使用します。

特定のネイバーがコスト コミュニティを伝送することを確認するには、**show ip bgp** *ip-address* コマンドを使用します。これらのコマンドの出力により、POI（IGP はデフォルトの POI）、設定された ID、および設定されたコストが表示されます。大きなコスト コミュニティ値に対しては、これらのコマンドからの出力は設定されたコストとデフォルトのコストの差異を+または - の値で表示します。出力例については、「例：BGP コスト コミュニティ検証」の項を参照してください。

トラブルシューティングのヒント

bgp bestpath cost-community ignore コマンドでコスト コミュニティ属性の評価を無効にし、BGP ベスト パス選択に関連する問題の隔離およびトラブルシューティングに役立てることができます。

debug ip bgp updates コマンドは BGP アップデート メッセージを印刷する際に使用できます。コストコミュニティ拡張コミュニティ属性をネイバーから受信した際に、このコマンドの出力で表示することができます。外部ピアから非推移的な拡張コミュニティを受信した場合も、メッセージが表示されます。

BGP コスト コミュニティ機能の設定例

例：BGP コスト コミュニティ設定

次の例では、コスト コミュニティ ID「1」、コスト コミュニティ値「100」がルート マップで許可されたルートに適用されます。このコンフィギュレーションでは、このルート マップ シーケンスで許可されていないその他の等コスト パスよりもこのルートが、ベスト パス選択プロセスにより優先されます。

```
Device(config)# router bgp 50000
Device(config-router)# neighbor 10.0.0.1 remote-as 50000
Device(config-router)# neighbor 10.0.0.1 update-source Loopback 0
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 route-map COST1 in
Device(config-router-af)# neighbor 10.0.0.1 send-community both
Router(config-router-af)# exit
Device(config)# route-map COST1 permit 10
Device(config-route-map)# match ip-address 1
Device(config-route-map)# set extcommunity cost 1 100
```

例：BGP コスト コミュニティ検証

BGP コスト コミュニティ コンフィギュレーションは、ローカルまたは特定のネイバーに対して確認できます。コスト コミュニティのローカル コンフィギュレーションを確認するには、**show route-map** または **show running-config** コマンドを使用します。特定のネイバーがコスト コミュニティを伝送することを確認するには、**show ip bgp** *ip-address* コマンドを使用します。

show route-map コマンドの出力では、ローカルで設定されたルート マップ、match 句、set 句、continue 句、およびコスト コミュニティ属性のステータスおよび属性が表示されます。次の出力例は、表示される出力に類似しています。

```
Device# show route-map

route-map COST1, permit, sequence 10
  Match clauses:
    as-path (as-path filter): 1
  Set clauses:
    extended community Cost:igp:1:100
  Policy routing matches: 0 packets, 0 bytes
route-map COST1, permit, sequence 20
  Match clauses:
    ip next-hop (access-lists): 2
  Set clauses:
    extended community Cost:igp:2:200
  Policy routing matches: 0 packets, 0 bytes
route-map COST1, permit, sequence 30
  Match clauses:
    interface FastEthernet0/0
    extcommunity (extcommunity-list filter):300
  Set clauses:
    extended community Cost:igp:3:300
  Policy routing matches: 0 packets, 0 bytes
```

次に、ローカルで設定された大きいコスト コミュニティ値を持つルートの例を示します。

```
Device# show route-map

route-map set-cost, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:1:1 RT:2:2 RT:3:3 RT:4:4 RT:5:5 RT:6:6 RT:7:7
      RT:100:100 RT:200:200 RT:300:300 RT:400:400 RT:500:500 RT:600:600
      RT:700:700 additive
    extended community Cost:igp:1:4294967295 (default+2147483648)
      Cost:igp:2:200 Cost:igp:3:300 Cost:igp:4:400
```

```
      Cost:igp:5:2147483648 (default+1) Cost:igp:6:2147484648 (default+1001)
      Cost:igp:7:2147284648 (default-198999)
  Policy routing matches: 0 packets, 0 bytes
```

show running config コマンドの出力では、ルート マップ内で設定された match 句、set 句、continue 句が表示されます。次に、実行中のコンフィギュレーションのうち、関連する部分だけをフィルタリングして表示した出力例を示します。

```
Device# show running-config | begin route-map

route-map COST1 permit 20
 match ip next-hop 2
 set extcommunity cost igp 2 200
!
route-map COST1 permit 30
 match interface FastEthernet0/0
 match extcommunity 300
 set extcommunity cost igp 3 300
.
.
.
```

show ip bgp *ip-address* コマンドの出力は、特定のネイバーがコスト コミュニティ属性を設定したパスを伝送するかどうかを確認する際に使用できます。コスト コミュニティ属性情報は、[Extended Community] フィールドに表示されます。POI、コスト コミュニティ ID、およびコスト コミュニティ番号値が表示されます。次に、ネイバー 172.16.1.2 が、ID「1」、コスト「100」のコスト コミュニティを伝送している出力例を示します。

```
Device# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
  2 2 2
    172.16.1.2 from 172.16.1.2 (172.16.1.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: Cost:igp:1:100
```

指定されたネイバーにデフォルトのコスト コミュニティ番号値が設定されている場合、またはコスト コミュニティ評価のためにデフォルト値が自動的に割り当てられている場合は、出力ではコスト コミュニティ番号値の後ろに + および - の値を伴った「default」が表示されます。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

関連項目	マニュアル タイトル
EIGRP MPLS VPN PE-CE Site of Origin（SoO）	『*IP Routing: EIGRP Configuration Guide*』の「EIGRP MPLS VPN PE-CE Site of Origin (SoO)」の項

標準

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

MIB

MIB	MIB のリンク
—	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

RFC

RFC	タイトル
draft-retana-bgp-custom-decision-00.txt	『BGP Custom Decision Process』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

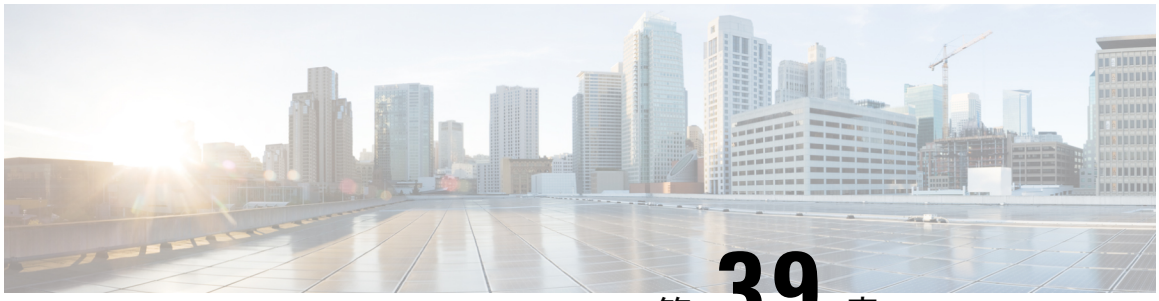
BGP コスト コミュニティの機能情報

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 *54 : BGP* コスト コミュニティの機能情報

機能名	リリース	機能情報
BGP コスト コミュニティ	12.0(24)S 12.3(2)T 12.2(18)S 12.2(27)SBC 15.0(1)S	BGP コスト コミュニティ機能により、コスト拡張コミュニティ属性が導入されます。コスト コミュニティとは、非推移的な拡張コミュニティ属性で、内部 BGP（iBGP）およびコンフェデレーション ピアには渡されますが、外部 BGP（eBGP）ピアには渡されません。コスト コミュニティ機能により、コスト値を特定のルートに割り当てることで、ローカル ルート プリファレンスをカスタマイズし、ベスト パス選択プロセスに反映させることができます。 次のコマンドが導入または変更されました。**bgp bestpath cost-community ignore**、**debug ip bgp updates**、**set extcommunity cost**
バックドア リンクを持つ EIGRP MPLS VPN Provider Edge-Customer Edge（PE-CE）に対する BGP コスト コミュニティ サポート	12.0(27)S 12.3(8)T 12.2(25)S	バックドア リンクの方が先に学習された場合、BGP により EIGRP MPLS VPN トポロジにおけるバックドア リンクが優先されます。VPN およびバックドア リンクが混在する EIGRP VPN ネットワーク トポロジをサポートするために、BGP コスト コミュニティ機能で「プレベストパス」挿入ポイント（POI）が導入されました。この POI は BGP に再配布される EIGRP ルートに自動的に適用されます。この POI は、BGP がその他のあらゆる比較ステップの前にこの POI を考慮するように影響を与えておくことで、最良パス計算プロセスに影響します。設定は必要ありません。Cisco IOS Release 12.0(27)S、12.3(8)T、12,2(25)S、およびそれ以降のリリースが PE、CE、またはバックドア ルータにインストールされている場合、この機能は自動的に EIGRP VPN 拠点に対して有効になります。 追加または変更されたコマンドはありません。



第 39 章

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィックスをグローバル ルーティング テーブルから VPN ルーティング/転送（VRF）インスタンス テーブルにインポートする機能が追加されます。

- 機能情報の確認 （715 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの前提条件 （716 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの制限事項 （716 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポートに関する情報 （717 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート方法 （718 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの設定例 （725 ページ）
- 内部 BGP 機能に関する追加情報 （726 ページ）
- グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの機能情報 （728 ページ）

機能情報の確認

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

リースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの前提条件

- ボーダー ゲートウェイ プロトコル（BGP）ピアリング セッションが確立されている必要があります。
- （分散プラットフォーム用の）CEF または dCEF が、参加しているすべてのルータで有効になっている必要があります。

グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの制限事項

- この機能で VRF にインポートできるのは、IPv4 ユニキャストおよびマルチキャストのプレフィックスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィックスをインポートするために、ルータごとに最大 5 つの VRF インスタンスを作成できます。
- この機能を使用して VRF にインポートされた IPv4 プレフィックスは、VPNv4 VRF にインポートできません。
- グローバル プレフィックスは、この機能で BGP VRF テーブルにインポートできるように、BGP テーブル内にある必要があります。
- この機能を使用して VRF にインポートされた IPv4 プレフィックスは、2 番目の VPNv4 VRF にはインポートできません。

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポートに関する情報

IPv4 プレフィックスから VRF へのインポート

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィックスをグローバル ルーティング テーブルからバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンス テーブルにインポートする機能が追加されます。この機能により VRF インポート マップ設定の機能が拡張され、標準コミュニティに基づいて IPv4 プレフィックスを VRF にインポートできるようになります。IPv4 ユニキャスト プレフィックスおよび IPv4 マルチキャスト プレフィックスの両方がサポートされています。マルチプロトコル ラベル スイッチング（MPLS）またはルート ターゲット（インポートまたはエクスポート）コンフィギュレーションは不要です。

IP プレフィックスは、標準のシスコ フィルタリング メカニズムでインポート マップの一致基準として定義されます。たとえば、IP アクセス リスト、IP プレフィックス リスト、または IP as-path フィルタを作成して IP プレフィックスまたは IP プレフィックス範囲を定義した後、ルート マップ内で 1 つ以上のプレフィックスに match 句の処理が行われます。ルート マップを通過するプレフィックスは、インポート マップ コンフィギュレーションごとに指定された VRF にインポートされます。

ブラック ホール ルーティング

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、ブラック ホール ルーティング（BHR）をサポートするように設定できます。BHR は、管理者が、トラフィックをデッド インターフェイスや調査用の情報を収集するように設計されたホストにダイナミック ルーティングを行い、ネットワークへの攻撃の影響を軽減することによって、不正な送信元からのトラフィックやサービス妨害（DoS）攻撃により生成されたトラフィックなどの望ましくないトラフィックをブロックできる方法です。プレフィックスが検索され、許可されていない送信元から届いたパケットが ASIC によってライン レートでブラックホール化されます。

グローバル トラフィックの分類

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、実際の位置またはサービス クラスに基づいてグローバル IP トラフィックを分類するために使用できます。トラフィックは、管理ポリシーに基づいて分類された後、異なる VRF にインポートされます。たとえば、大学のキャンパスでは、ネットワーク トラフィックは、大学ネットワークと寄宿舎ネットワークのトラフィック、学生ネットワークと学部ネットワーク、またはマルチキャスト トラフィック専用のネットワークに分割できます。管理ポリシーに従ってトラフィックが分割された後、ルーティング決定は、ポリシーベース ルーティン

グを使用した MPLS VPN--VRF 選択機能、または送信元 IP アドレスに基づく MPLS VPN--VRF 選択機能で設定できます。

ユニキャスト リバース パス フォワーディング

ユニキャスト リバース パス転送（ユニキャスト RPF）は、グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポートを使用して任意で設定できます。ユニキャスト RPF は、送信元アドレスが転送情報ベース（FIB）内にあることを確認するために使用されます。**ip verify unicast vrf** コマンドはインターフェイス コンフィギュレーション モードで設定され、各 VRF で有効化されます。このコマンドには、ユニキャスト RPF 確認の後にトラフィックが転送されるかドロップされるかを判断するために使用される **permit** キーワードおよび **deny** キーワードがあります。

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート方法

インポートする IPv4 IP プレフィックスの定義

IPv4 ユニキャストまたは IPv4 マルチキャストのプレフィックスは、標準のシスコ フィルタリング メカニズムを使用して、インポート ルート マップの一致基準として定義されます。この作業では、IP アクセス リストおよび IP プレフィックス リストを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
4. **ip prefix-list** *prefix-list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 50 permit 10.1.1.0 0.0.0.255`	アクセス リストを作成して、VRF テーブルにインポートする IP プレフィックスの範囲を定義します。 • この例では、50 の番号が付けられた標準アクセス 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 アドレスを持つホストからのトラフィックを許可します。
ステップ 4	**ip prefix-list** *prefix-list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] 例： `Device(config)# ip prefix-list COLORADO permit 10.24.240.0/22`	プレフィックス リストを作成して、VRF テーブルにインポートする IP プレフィックスの範囲を定義します。 • この例では、COLORADO という名前の IP プレフィックス リストを作成しています。このフィルタは、10.24.240.0/22 サブネット内の IP アドレスを持つホストからのトラフィックを許可します。

VRF およびインポート ルート マップの作成

インポートに対して定義された IP プレフィックスは、その後、ルート マップ内で match 句の処理が行われます。ルート マップを通過する IP プレフィックスは、VRF にインポートされます。グローバル ルーティング テーブルから IPv4 プレフィックスをインポートするために、ルータごとに最大 5 つの VRF を設定できます。デフォルトでは、VRF あたり最大 1000 プレフィックスをインポートできます。この制限は、VRF ごとに 1 ～ 2,147,483,647 プレフィックスの範囲で変更できます。プレフィックス インポート制限を 1000 よりも大きくする場合は注意してください。ルータが過剰な量のプレフィックスをインポートするように設定すると、正常なルータの正常な動作が中断する場合があります。

MPLS コンフィギュレーションもルート ターゲット（インポートまたはエクスポート）コンフィギュレーションも必要ありません。

インポート アクションは、新しいルーティング アップデートが受信されたとき、またはルートが除去されたときにトリガーされます。最初の BGP アップデート期間中は、BGP がコンバージェンスをより迅速に実行できるように、インポート アクションが延期されます。BGP がコンバージェンスを実行すると、インクリメンタル BGP アップデートがただちに評価されて、認定されたプレフィックスが受信と同時にインポートされます。

次の syslog メッセージが、グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能で導入されました。このメッセージは、ユーザ定義の制限よりも多くのプレフィックスがインポートで使用できる場合に表示されます。

```
00:00:33: %BGP-3-AFIMPORT_EXCEED: IPv4 Multicast prefixes imported to multicast vrf
exceed the limit 2
```

プレフィックス制限を増やすか、またはインポート ルート マップ フィルタを微調整すると、候補ルートの数を削減できます。

（注）
- この機能で VRF にインポートできるのは、IPv4 ユニキャストおよびマルチキャストのプレフィックスだけです。
- グローバル ルーティング テーブルから IPv4 プレフィックスをインポートするために、ルータごとに最大 5 つの VRF インスタンスを作成できます。
- この機能を使用して VRF にインポートされた IPv4 プレフィックスは、VPNv4 VRF にインポートできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **import ipv4** {**unicast** | **multicast**} [*prefix-limit*] **map** *route-map*
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
8. **match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf GREEN`	VRF ルーティング テーブルを作成し、VRF の名前（またはタグ）を指定します。 • **ip vrf** *vrf-name* コマンドは VRF ルーティング テーブルおよびCEFテーブルを作成し、その両方のテーブルに、*vrf-name* 引数を使用して名前が付けられます。この両方のテーブルには、デ

	コマンドまたはアクション	目的
		フォルトのルート識別子の値が関連付けられています。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 100:10`	VRF インスタンスのためのルーティング テーブルおよびフォワーディング テーブルを作成します。 • ルート識別子の引数を設定するには、2 つの形式があります。例で示されているような as-number:network number（ASN:nn）の形式、または IP address:network number（IP-address:nn）の形式で設定できます。
ステップ 5	**import ipv4** {**unicast** | **multicast**} [*prefix-limit*] **map** *route-map* 例： `Router(config-vrf)# import ipv4 unicast 1000 map UNICAST`	IPv4 プレフィックスを、指定したルート マップでフィルタ処理して、グローバル ルーティング テーブルから VRF テーブルにインポートします。 • ユニキャスト プレフィックスまたはマルチキャスト プレフィックスを指定します。 • デフォルトでは、最大 1000 のプレフィックスがインポートされます。1 ～ 2,147,483,647 のプレフィックスの制限を指定するには、*prefix-limit* 引数を使用します。 • この例では、通過した最大 1000 のユニキャスト プレフィックスをインポートするルート マップを参照しています。
ステップ 6	**exit** 例： `Router(config-vrf)# exit`	VRF 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 モードを開始します。
ステップ 7	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map UNICAST 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 マップ名は、ステップ 5 で指定されたルート マップと一致する必要があります。 • この例では、UNICAST という名前のルート マップを作成しています。
ステップ 8	**match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}	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

	コマンドまたはアクション	目的
	例： `Router(config-route-map)# match ip address 50`	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 リストと IP プレフィックス リストの両方がサポートされています。 • この例では、標準アクセス リスト 50 を使用して一致基準を定義するようにルートマップを定義しています。
ステップ 9	**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。

入力インターフェイスのフィルタリング

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能は、グローバルに、またはインターフェイス単位で設定できます。性能を最大限に高めるために、この機能を入力インターフェイスだけに適用することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip verify unicast vrf** *vrf-name* {**deny** | **permit**}
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* [*name-tag*] 例： `Router(config)# interface Ethernet0/0`	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： `Router(config-if)# ip policy route-map UNICAST`	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。 • この例では、UNICAST という名前のルートマップをインターフェイスに接続しています。
ステップ 5	**ip verify unicast vrf** *vrf-name* {**deny** | **permit**} 例： `Router(config-if)# ip verify unicast vrf GREEN permit`	（任意）指定された VRF のユニキャスト Reverse Path Forwarding の確認をイネーブルにします。 • この例では、GREEN という名前の VRF の確認をイネーブルにしています。確認を通過したトラフィックは転送されます。
ステップ 6	**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 モードに戻ります。

グローバル IP プレフィックス インポートの確認

グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能で設定された VRF に関する情報を表示し、指定した VRF テーブルにグローバル IP プレフィックスがインポートされていることを確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}
3. **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*]

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device# enable
```

ステップ 2 **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}

VPN アドレス情報を BGP テーブルから表示します。出力には、インポート ルート マップ、トラフィック タイプ（ユニキャストまたはマルチキャスト）、デフォルトまたはユーザ定義のプレフィックス インポート制限、インポートされた実際のプレフィックスの数、および個別のインポート プレフィックス エントリが表示されます。

例：

```
Device# show ip bgp vpnv4 all

BGP table version is 15, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf academic)
Import Map: ACADEMIC, Address-Family: IPv4 Unicast, Pfx Count/Limit: 6/1000
*> 10.50.1.0/24     172.17.2.2                             0 2 3 ?
*> 10.50.2.0/24     172.17.2.2                             0 2 3 ?
*> 10.50.3.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.1.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.2.0/24     172.17.2.2                             0 2 3 ?
*> 10.60.3.0/24     172.17.2.2                             0 2 3 ?
Route Distinguisher: 200:1 (default for vrf residence)
Import Map: RESIDENCE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.30.1.0/24     172.17.2.2                  0          0 2 i
*> 10.30.2.0/24     172.17.2.2                  0          0 2 i
*> 10.30.3.0/24     172.17.2.2                  0          0 2 i
Route Distinguisher: 300:1 (default for vrf BLACKHOLE)
Import Map: BLACKHOLE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.40.1.0/24     172.17.2.2                  0          0 2 i
*> 10.40.2.0/24     172.17.2.2                  0          0 2 i
*> 10.40.3.0/24     172.17.2.2                  0          0 2 i
Route Distinguisher: 400:1 (default for vrf multicast)
Import Map: MCAST, Address-Family: IPv4 Multicast, Pfx Count/Limit: 2/2
*> 10.70.1.0/24     172.17.2.2                  0          0 2 i
*> 10.70.2.0/24     172.17.2.2                  0          0 2 i
```

ステップ 3 **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*]

定義された VRF、および関連付けられたインターフェイスを表示します。出力には、インポート ルート マップ、トラフィック タイプ（ユニキャストまたはマルチキャスト）、およびデフォルトまたはユーザ定義のプレフィックス インポート リミットが表示されています。次の例では、UNICAST という名前のインポート ルート マップが IPv4 ユニキャスト プレフィックスをインポートしており、プレフィックス インポート リミットが 1000 であることを示します。

例：

```
Device# show ip vrf detail

VRF academic; default RD 100:10; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:10
  Import VPN route-target communities
    RT:100:10
```

```
Import route-map for ipv4 unicast: UNICAST (prefix limit: 1000)
No export route-map
```

グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP サポートの設定例

例：グローバル テーブルから VRF テーブルへの IP プレフィックスのインポート

次に、IP プレフィックス リストとルート マップを使用して、ユニキャスト プレフィックスを、*green* という名前の VRF にインポートする例を示します。

この例は、グローバル コンフィギュレーション モードで開始します。

```
!
ip prefix-list COLORADO seq 5 permit 10.131.64.0/19
ip prefix-list COLORADO seq 10 permit 172.31.2.0/30
ip prefix-list COLORADO seq 15 permit 172.31.1.1/32
!
ip vrf green
 rd 200:1
 import ipv4 unicast map UNICAST
 route-target export 200:10
 route-target import 200:10
!
 exit
!
route-map UNICAST permit 10
 match ip address prefix-list COLORADO
!
 exit
```

例：VRF テーブルへの IP プレフィックス インポートの確認

show ip vrf コマンドまたは **show ip bgp vpnv4** コマンドを使用すると、プレフィックスがグローバル ルーティング テーブルから VRF テーブルにインポートされていることを確認できます。

次の出力例では、UNICAST という名前のインポート ルート マップが IPv4 ユニキャスト プレフィックスをインポートしており、プレフィックス インポート制限が 1000 であることを示します。

```
Device# show ip vrf detail

VRF green; default RD 200:1; default VPNID <not set>
  Interfaces:
    Se2/0
VRF Table ID = 1
  Export VPN route-target communities
```

```
    RT:200:10
  Import VPN route-target communities
    RT:200:10
  Import route-map for ipv4 unicast: UNICAST (prefix limit: 1000)
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
VRF red; default RD 200:2; default VPNID <not set>
  Interfaces:
    Se3/0
VRF Table ID = 2
  Export VPN route-target communities
    RT:200:20
  Import VPN route-target communities
    RT:200:20
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

次の出力例は、インポート ルート マップ名、プレフィックス インポート制限、インポートされたプレフィックスの実際の数、および個別のインポート エントリを示します。

```
Device# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.131.127.252
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:1 (default for vrf green)
Import Map: UNICAST, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
*>i10.131.64.0/19   10.131.95.252            0    100      0 i
*> 172.16.1.1/32    172.16.2.1               0         32768 i
*> 172.16.2.0/30    0.0.0.0                  0         32768 i
*>i172.31.1.1/32    10.131.95.252            0    100      0 i
*>i172.31.2.0/30    10.131.95.252            0    100      0 i
Route Distinguisher: 200:2 (default for vrf red)
*> 172.16.1.1/32    172.16.2.1               0         32768 i
*> 172.16.2.0/30    0.0.0.0                  0         32768 i
*>i172.31.1.1/32    10.131.95.252            0    100      0 i
*>i172.31.2.0/30    10.131.95.252            0    100      0 i
```

内部 BGP 機能に関する追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概要	「Cisco BGP 概要」モジュール
基本的な BGP 設定作業	「基本 BGP ネットワークの設定」モジュール

関連項目	マニュアル タイトル
iBGP のマルチパス ロード シェアリング	「iBGP マルチパス ロード シェアリング」モジュール
サービス プロバイダーへの接続	「外部 BGP を使用したサービス プロバイダーとの接続」モジュール
複数の IP ルーティング プロトコルに適用する機能の設定	『*IP Routing: Protocol-Independent Configuration Guide*』

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4893	『*BGP Support for Four-octet AS Number Space*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

グローバル テーブルから VRF テーブルへの IP プレフィックス インポートに対する BGP 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 *55 :* グローバル テーブルから *VRF* テーブルへの *IP* プレフィックス インポートに対する *BGP* サポートの機能情報

機能名	リリース	機能情報
グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート	Cisco IOS XE Release 2.1	グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート機能により、インポート ルート マップを使用して、IPv4 ユニキャスト プレフィックスをグローバル ルーティング テーブルから VPN ルーティング/転送（VRF）インスタンス テーブルにインポートする機能が追加されます。 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。 この機能により、次のコマンドが導入または変更されました。**debug ip bgp import**、**import ipv4**、**ip verify unicast vrf**

第 40 章

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに対する BGP サポート

この機能により、ネットワーク管理者は VRF テーブルからグローバル ルーティング テーブルに IP プレフィックスをエクスポートできます。

- 機能情報の確認 （729 ページ）
- VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに関する情報（730 ページ）
- VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート方法 （732 ページ）
- VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの設定例 （738 ページ）
- その他の参考資料 （739 ページ）
- VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの機能情報（740 ページ）

機能情報の確認

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

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

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに関する情報

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの利点

- グローバル テーブルに存在するネットワーク管理ノードを使用して、VRF 内の一部のネットワーク リソースを管理できます。
- インターネット パブリック IP アドレス空間を所有しながら、それらの IP アドレスを管理するための VRF を保持できます。

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの仕組み

マルチプロトコル BGP（MP-BGP）を使用した MPLS VPN は、非常に柔軟でありながらセキュアな VPN プロビジョニング メカニズムをサービス プロバイダーやお客様に提供します。ただし、お客様によっては、VRF でもグローバル ルーティング テーブルでも特定のプレフィックスに同様に到達できるように、境界を緩和することを望む場合があります。

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに対する BGP サポート機能よりも前に、BGP では、グローバルから VRF へのプレフィックスのインポートをすでにサポートしていました。この機能の詳細については、「グローバル テーブルから *VRF* テーブルへの *IP* プレフィックスのインポートに対する *BGP* サポート」モジュールを参照してください。また、このインポート機能とエクスポート機能は、L3VPN ダイナミック ルート リークを提供します。

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに対する BGP サポート機能は、前述のインポート機能とは逆のメカニズムを提供します。つまり、VRF テーブルからグローバル ルーティング テーブルへのプレフィックスのエクスポートに対応しています。この機能は、VRF テーブルからグローバル ルーティング テーブルにエクスポートするプレフィックスを制御するためのルート マップを指定する **export {ipv4 | ipv6} {unicast | multicast} map** コマンドによって実現されます。

⚠

注意 VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポート機能は、VRF ルートをグローバル BGP ルーティング テーブルにリークします。これらのルートは、IPv4 または IPv6 ルーティング テーブルにインストールされます。ネットワークを設計する際は、このようなリークが通常のインターネット ルーティングに影響しないように細心の注意を払ってください。

エクスポートアクションは、新しいルーティングアップデートが受信されたとき、またはルートが取り消されたときにトリガーされます。最初の BGP アップデート期間中は、BGP がコンバージェンスをより迅速に実行できるように、エクスポートアクションが延期されます。BGP がコンバージェンスを実行すると、インクリメンタル BGP アップデートがただちに評価されて、認定されたプレフィックスが受信と同時にエクスポートされます。

各 VRF では、IPv4（ユニキャストまたはマルチキャスト）のグローバル トポロジの 1 つにのみエクスポートでき、IPv6（ユニキャストまたはマルチキャスト）のグローバル トポロジの 1 つにのみエクスポートできます。

IPv4 または IPv6 プレフィックスをグローバル ルーティング テーブルにエクスポートするように設定できるルータあたりの VRF 数に制限はありません。

デフォルトでは、エクスポートできるプレフィックス数は VRF あたり最大 1000 プレフィックスに制限されます。この制限は、VRF ごとに 1 ～ 2,147,483,647 プレフィックスの範囲内の値に変更できます。プレフィックス制限を 1000 よりも大きくする場合は注意してください。過剰な量のプレフィックスをエクスポートするようにデバイスを設定すると、正常なルータの動作を妨げる可能性があります。

この機能では、次の **match** および **set** コマンドがサポートされています。

- **match as-path**
- **match community** [**exact-match**]
- **match extcommunity**
- **match ip address** [**prefix-list**]
- **match ip next-hop**
- **match ip route-source**
- **match ipv6 address** [**prefix-list**]
- **match ipv6 route-source**
- **match ipv6 next-hop**
- **match policy-list**
- **match route-type**
- **set as-path prepend** [**last-as**]
- **set community additive**
- **set extcommunity** [**cost** | **rt**]
- **set extcomm-list delete**
- **set ip next-hop**
- **set ipv6 next-hop**
- **set local-preference**
- **set metric**

- **set origin**
- **set weight**

（注） この機能では、**set ip vrf next-hop** および **set ipv6 vrf next-hop** コマンドはサポートされていません。

VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート方法

VRF およびアドレス ファミリ用エクスポート ルート マップの作成

エクスポートに対して定義された IP プレフィックスは、ルート マップ内で match 句によって処理されます。ルート マップを通過した IP プレフィックスはグローバル ルーティング テーブルにインポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **export** {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix-limit*] **map** *map-name*
7. **route-target import** *route-target-ext-community*
8. **route-target export** *route-target-ext-community*
9. **exit**
10. **exit**
11. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
12. **match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vpn1`	VRF ルーティング テーブルを作成し、VRF の名前（またはタグ）を指定します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:100`	VRF インスタンスのためのルーティング テーブルおよびフォワーディング テーブルを作成します。 • 引数を設定する形式が 2 つあります。例で示されている *as-number*:*network number*（*ASN*:*nn*）の形式、または *IP address*:*network number*（*IP-address*:*nn*）の形式で設定できます。
ステップ 5	**address-family** {**ipv4** | **ipv6**} 例： `Device(config-vrf)# address-family ipv4`	IPv4 または IPv6 アドレス ファミリを設定します。
ステップ 6	**export** {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix-limit*] **map** *map-name* 例： `Device(config-vrf-af)# export ipv4 unicast 500 map UNICAST`	IPv4 または IPv6 プレフィックスを、指定したルート マップでフィルタ処理して、VRF テーブルからグローバル ルーティング テーブルにエクスポートします。 • 手順 5 で指定した **ipv4** または **ipv6** を指定します。この例では、IPv4 ユニキャスト プレフィックスをエクスポートします。 • この例に基づく場合、500 を超えるプレフィックスはエクスポートされません。 • エクスポートされるプレフィックスは、ルート マップを通過したプレフィックスです。
ステップ 7	**route-target import** *route-target-ext-community* 例： `Device(config-vrf-af)# route-target import 100:100`	VRF インスタンス用にルート ターゲット拡張コミュニティを作成します。 • route-target import または route-target export については、『*MPLS: Layer 3 VPNs Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 8	**route-target export** *route-target-ext-community* 例： `Device(config-vrf-af)# route-target export 100:100`	VRFインスタンス用にルートターゲット拡張コミュニティを作成します。
ステップ 9	**exit** 例： `Device(config-vrf-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、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 10	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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 11	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map UNICAST permit 10`	ポリシー ルーティングを有効にします。 • この例では、UNICAST という名前のルート マップを作成しています。
ステップ 12	**match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]} 例： `Device(config-route-map)# match ip address 50`	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 リストと IP プレフィックス リストの両方がサポートされています。 • この例では、標準アクセス リスト 50 を使用して一致基準を定義するようにルート マップを定義しています。 • アクセス リストを定義します（この作業では示されていません）。たとえば、access-list 50 permit 192.168.1.0 255.255.255.0 などです。
ステップ 13	**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。

VRF および VRF 用エクスポート ルート マップの作成（IPv4 のみ）

エクスポートに対して定義された IP プレフィックスは、ルート マップ内で match 句によって処理されます。ルート マップを通過した IP プレフィックスはグローバル ルーティング テーブルにインポートされます。

（注）
- この作業で示すように、**ip vrf** コマンド下で VRF テーブルからグローバル ルーティング テーブルにエクスポートできるのは IPv4 ユニキャストおよびマルチキャスト プレフィックスだけです。IPv6 プレフィックスをエクスポートするには、IPv6 アドレス ファミリで行う必要があります。「VRF およびアドレス ファミリ用エクスポート ルート マップの作成」の項を参照してください。
- この機能を使用してグローバル ルーティング テーブルにエクスポートされた IPv4 プレフィックスは、VPNv4 VRF にエクスポートできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **export ipv4** {**unicast** | **multicast**} [*prefix-limit*] **map** *map-tag*
6. **route-target import** *route-target-ext-community*
7. **route-target export** *route-target-ext-community*
8. **exit**
9. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
10. **match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}
11. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 GREEN`	VRF ルーティング テーブルを作成し、VRF の名前（またはタグ）を指定します。 • **ip vrf** *vrf-name* コマンドは VRF ルーティング テーブルおよび CEF テーブルを作成し、その両方のテーブルに、*vrf-name* 引数を使用して名前が付けられます。この両方のテーブルには、デフォルトのルート識別子の値が関連付けられています。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:10`	VRF インスタンスのためのルーティング テーブルおよびフォワーディング テーブルを作成します。 • 引数を設定する形式が 2 つあります。例で示されている *as-number*:*network number*（*ASN*:*nn*）の形式、または *IP-address*:*network number*（*IP-address*:*nn*）の形式で設定できます。
ステップ 5	**export ipv4** {**unicast** | **multicast**} [*prefix-limit*] **map** *map-tag* 例： `Device(config-vrf)# export ipv4 unicast 500 map UNICAST`	IPv4 プレフィックスを、指定したルート マップでフィルタ処理して、VRF テーブルからグローバル ルーティング テーブルにエクスポートします。 • ユニキャスト プレフィックスまたはマルチキャスト プレフィックスを指定します。 • デフォルトでは、最大 1000 プレフィックスをエクスポートできます。1 ～ 2,147,483,647 のプレフィックスの制限を指定するには、*prefix-limit* 引数を使用します。 • この例では、UNICAST という名前のルート マップを通過した最大 500 のユニキャスト プレフィックスをエクスポートするエクスポート マップを作成しています。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:100`	VRF インスタンス用にルート ターゲット拡張コミュニティを作成します。 • route-target import または route-target export については、『*MPLS: Layer 3 VPNs Configuration Guide*』を参照してください。
ステップ 7	**route-target export** *route-target-ext-community* 例：	VRF インスタンス用にルート ターゲット拡張コミュニティを作成します。

	コマンドまたはアクション	目的
	`Device(config-vrf)# route-target export 100:100`	
ステップ 8	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map UNICAST 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 ルーティングを有効にします。 • ルート マップ名は、ステップ 5 で指定されたルート マップと一致する必要があります。 • この例では、UNICAST という名前のルート マップを作成しています。
ステップ 10	**match ip address** {*acl-number* [*acl-number* | *acl-name*] | *acl-name* [*acl-name* | *acl-number*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]} 例： `Device(config-route-map)# match ip address 50`	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 リストと IP プレフィックス リストの両方がサポートされています。 • この例では、標準アクセス リスト 50 を使用して一致基準を定義するようにルート マップを定義しています。
ステップ 11	**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。

VRF からグローバル テーブルへの IP プレフィックス エクスポートに関する情報の表示

VRF テーブルからグローバル テーブルにエクスポートされたプレフィックスに関する情報を表示するには、この作業のいずれかの手順を実行します。

手順の概要

1. **enable**
2. **show ip bgp** {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix*]

3. **debug ip bgp import event**
4. **debug ip bgp import update**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp** {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix*] 例： `Device# show ip bgp ipv4 unicast 192.168.1.1`	VRF からグローバル テーブルにインポートされたパスに関する情報を表示します。
ステップ 3	**debug ip bgp import event** 例： `Device# debug ip bgp import event`	IPv4 プレフィックス インポート イベントに関連するメッセージを表示します。
ステップ 4	**debug ip bgp import update** 例： `Device# debug ip bgp import update`	IPv4 プレフィックス インポート アップデートに関連するメッセージを表示します。

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの設定例

例：IPv6 アドレス ファミリを使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート

```
vrf definition X
  rd 100:100
   address-family ipv6
    export ipv6 unicast map OnlyNet2000
    route-target import 100:100
    route-target export 100:100
!
 ipv6 prefix-list net2000 permit 2000::/16
!
route-map OnlyNet2000 permit 10
 match ipv6 address prefix-list net2000
```

例：IPv4 アドレス ファミリを使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート

```
vrf definition X
  rd 100:100
   address-family ipv4
    export ipv4 unicast map OnlyNet200
    route-target import 100:100
    route-target export 100:100
!
 ip prefix-list net200 permit 200.0.0.0/8
!
route-map OnlyNet200 permit 10
 match ip address prefix-list net200
```

例：IP VRF を使用した VRF テーブルからグローバル テーブルへの IP プレフィックスのエクスポート（IPv4 のみ）

```
 ip vrf vrfname
  rd 100:100
  export ipv4 unicast map OnlyNet200
  route-target import 100:100
  route-target export 100:100
!
 ip prefix-list net200 permit 200.0.0.0/8
!
route-map OnlyNet200 permit 10
 match ip address prefix-list net200
```

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』
BGP コマンド	『Cisco IOS BGP Command Reference』
route-target import および route-target export の使用	『*MPLS: Layer 3 VPNs Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートの機能情報

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 *56 : VRF* テーブルからグローバル テーブルへの *IP* プレフィックス エクスポートに対する *BGP* サポートの機能情報

機能名	リリース	機能情報
VRF テーブルからグローバル テーブルへの IP プレフィックス エクスポートに対する BGP サポート		この機能により、ネットワーク管理者は VRF ルーティング テーブルからグローバル ルーティング テーブルに IP プレフィックスをエクスポートできます。 **export map (VRF table to global table)** コマンドが導入されました。 次のコマンドが変更されました。**debug ip bgp import**、**show ip bgp**

第 41 章

BGP のネイバーごとの SoO 設定

ボーダーゲートウェイ プロトコル（BGP）のネイバー Site-of-Origin（SoO）ごとの設定機能を使用すると、SoO 値の設定が簡略化されます。ネイバーごとの SoO 設定により、ルータ コンフィギュレーション モードの下のサブモードで設定可能な 2 つの新しいコマンドが導入され、SoO 値が設定されます。

- 機能情報の確認 （741 ページ）
- BGP のネイバーごとの SoO 設定の前提条件 （742 ページ）
- BGP のネイバーごとの SoO 設定の制約事項 （742 ページ）
- BGP のネイバーごとの SoO の設定に関する情報 （742 ページ）
- BGP のネイバーごとの SoO の設定方法 （745 ページ）
- BGP のネイバーごとの SoO 設定の設定例 （756 ページ）
- 次の作業 （757 ページ）
- その他の参考資料 （758 ページ）
- BGP のネイバーごとの SoO 設定の機能情報 （758 ページ）

機能情報の確認

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

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

BGP のネイバーごとの SoO 設定の前提条件

この機能は、ボーダーゲートウェイプロトコル（BGP）ネットワークが設定され、Cisco Express Forwarding がご使用のネットワークで有効になっていることを前提としています。

BGP のネイバーごとの SoO 設定の制約事項

BGP ネイバーまたはピア ポリシーのテンプレート ベースの SoO 設定は、インバウンド ルートマップで設定された SoO 値よりも優先されます。

BGP のネイバーごとの SoO の設定に関する情報

Site of Origin BGP コミュニティ属性

Site-of-Origin（SoO）拡張コミュニティは、サイトを発信元とするルートを識別し、そのプレフィックスの再アドバタイズメントが送信元のサイトに戻されることを防ぐために使用される BGP 拡張コミュニティ属性です。この SoO 拡張コミュニティは、ルータがルートを学んだサイトを一意に識別します。BGP は、ルートに関連付けられた SoO 値を使用し、ルーティングループを防止できます。

ルート識別子

ルート識別子（RD）はルーティングテーブルとフォワーディングテーブルを作成し、VPN のデフォルトのルート識別子を指定します。IPv4 プレフィックスをグローバルに固有の VPN-IPv4 プレフィックスに変更するために、RD が IPv4 プレフィックスの先頭に追加されます。RD は、自律システム番号と任意番号、または IP アドレスと任意番号のいずれかで構成できます。

RD は、次のいずれかの形式で入力できます。

- 16 ビット自律システム番号、コロン、32 ビット番号を入力します。次に例を示します。

45000:3

- 32 ビット IP アドレス、コロン、16 ビット番号を入力します。次に例を示します。

192.168.10.15:1

BGP によるネイバーごとの Site of Origin の設定

BGP ネイバーに SoO 値を設定するには 3 つの方法があります。

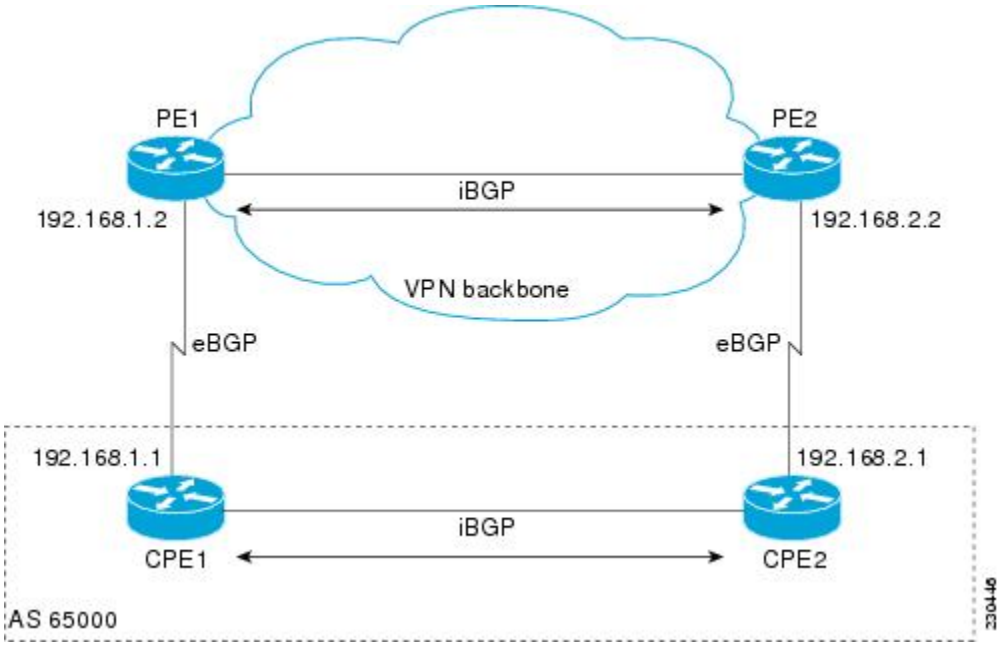
- BGP ピア ポリシー テンプレート：ピア ポリシー テンプレートが作成され、SoO 値がこのピア ポリシーの一部として設定されます。アドレス ファミリ IPv4 仮想ルーティング/転送（VRF）の下で、ネイバーが特定され、SoO 値を含むピア ポリシーを継承するように設定されます。
- BGP **neighbor** コマンド：アドレス ファミリ IPv4 VRF の下で、ネイバーが特定され、SoO 値がこのネイバーに設定されます。
- BGP ピア グループ：アドレス ファミリ IPv4 VRF の下で、BGP ピア グループが設定され、SoO 値がそのピア グループに設定され、ネイバーが特定され、このネイバーがこのピア グループのメンバとして設定されます。

（注） BGP ネイバーまたはピア ポリシーのテンプレート ベースの SoO 設定は、インバウンド ルート マップで設定された SoO 値よりも優先されます。

BGP ネイバーに対する SoO 値の設定は、VPN の入り口であるプロバイダー エッジ（PE）ルータで実行されます。SoO が有効になると、プレフィックスの SoO タグが顧客宅内装置（CPE）用に設定された SoO タグと一致しない場合だけ PE ルータがプレフィックスを CPE に転送します。

たとえば、下の図では、SoO タグは、自律システム番号 65000 のルータ CPE1 と CPE2 を含むお客様のサイトに対して 65000:1 に設定されています。CPE1 がプレフィックスを PE1 に送信すると、PE1 は、このプレフィックスに CPE1 および CPE2 の SoO タグである 65000:1 をタグ付けします。PE1 がタグを付けられたプレフィックスを PE2 に送信すると、PE2 は、CPE2 から SoO タグに対する一致処理を実行します。タグ値が 65000:1 であるすべてのプレフィックスは、SoO タグが CPE2 の SoO タグと一致するため、CPE2 には送信されず、ルーティング ループが回避されます。

図 *62 : SoO* に対するネットワーク ダイアグラム例



BGP のネイバーごとの Site of Origin の利点

この機能が導入される前のリリースでは、SoO 拡張コミュニティ属性は、アップデート プロセス中に SoO 値を設定するインバウンド ルート マップを使用して設定されます。BGP のネイバーごとの Site of Origin 機能の導入に伴い、ルータ コンフィギュレーション モード下のサブモードで設定される 2 つの新しいコマンドにより、SoO 値の設定が簡素化されます。

BGP ピア ポリシー テンプレート

ピア ポリシー テンプレートは、特定のアドレス ファミリに属するネイバーに設定される BGP ポリシー コマンドの設定に使用されます。ピア ポリシー テンプレートは、1 回設定され、その後、ピア ポリシー テンプレートを直接適用するか、またはピア ポリシー テンプレートから継承することによって、多くのネイバーに適用されます。ピア ポリシー テンプレートの設定により、自律システム内のすべてのネイバーに適用される BGP ポリシー コマンドの設定が簡略化されます。

ピア ポリシー テンプレートは継承をサポートします。直接適用されたピア ポリシー テンプレートは、最大 7 つのピア ポリシー テンプレートから設定を直接的または間接的に継承できます。したがって、合計 8 つのピア ポリシー テンプレートをネイバーまたはネイバー グループに適用できます。

ピア ポリシー テンプレートの設定により、BGP 設定が簡略化され、柔軟性が向上します。特定のポリシーを 1 回設定すれば、何回も参照できます。ピア ポリシーは最大 8 レベルの継承をサポートするため、非常に具体的で複雑な BGP ポリシーを作成できます。

BGP ピア ポリシーテンプレートの詳細については、「基本BGP ネットワークの設定」モジュールを参照してください。

BGP のネイバーごとの SoO の設定方法

Cisco Express Forwarding の有効化と VRF インスタンスの設定

次の作業を上の図の両方の PE ルータで実行し、Virtual Routing and Forwarding（VRF）インスタンスをVRF割り当てごとの作業とともに使用されるように設定します。この作業では、Cisco Express Forwarding を有効にし、SOO_VRF という名前の VRF インスタンスを作成します。この VRF を機能させるために、ルート識別子が作成され、この VRF はインターフェイスに関連付けられます。ルート識別子が作成されると、SOO_VRF という名前の VRF インスタンスにルーティングテーブルおよびフォワーディングテーブルが作成されます。VRF をインターフェイスと関連付けた後、インターフェイスは、IP アドレスによって設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **route-target** {**export** | **both**} *route-target-ext-community*
7. **route-target** {**import** | **both**} *route-target-ext-community*
8. **exit**
9. **interface** *type number*
10. **ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
11. **ip address** *ip-address mask* [**secondary**]
12. **end**
13. **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 cef** 例： `Device(config)# ip cef`	ルート プロセッサで Cisco Express Forwarding を有効にします。
ステップ 4	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf SOO_VRF`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。

ステップ 5	**rd** *route-distinguisher*
	例：
	`Device(config-vrf)# rd 1:1`
		VRF にルーティング テーブルとフォワーディング テーブルを作成し、VPN にデフォルト RD を指定します。
		• VPN にデフォルト RD を指定するには、*route-distinguisher* 引数を使用します。次の 2 つの形式を使用して RD を指定できます。
		  • 16 ビットの自律システム番号、コロン、および 32 ビットの数字（例：65000:3）。
		  • 32 ビットの IP アドレス、コロン、および 16 ビットの数字（例：192.168.1.2:51）。
		• この例では、RD は自律システム番号とコロンの後に数字 1 を使用しています。

ステップ 6	**route-target** {**export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target export 1:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • VPN 拡張コミュニティを指定するには、*route-target-ext-community* 引数を使用します。 （注） この手順に適用される構文だけが表示されます。この構文の別の使用方法については、手順 7 を参照してください。

	コマンドまたはアクション	目的
ステップ 7	**route-target** {**import** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target import 1:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲットVPN拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。 • ターゲットVPN拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • VPN 拡張コミュニティを指定するには、*route-target-ext-community* 引数を使用します。
ステップ 8	**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 9	**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 10	**ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] 例： `Device(config-if)# ip vrf forwarding SOO_VRF`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • この例では、SOO_VRF という名前の VRF がギガビット イーサネット インターフェイス 1/0/0 と関連付けられます。 （注） このコマンドをインターフェイス上で実行すると、IP アドレスが削除されるため、IP アドレスを再設定する必要があります。
ステップ 11	**ip address** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 192.168.1.2 255.255.255.0`	IP アドレスを設定します。 • この例では、ギガビットイーサネットインターフェイス 1/0/0 が IP アドレス 192.168.1.2 によって設定されます。
ステップ 12	**end** 例：	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 13	**show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*] 例： `Device# show ip vrf`	設定された VRF を表示します。 • このコマンドを使用して、この作業の設定を確認します。

例

show ip vrf コマンドの次の出力は、この作業で設定された SOO_VRF という名前の VRF を表示します。

```
Device# show ip vrf

Name                                     Default RD            Interfaces
SOO_VRF                                  1:1                   GE1/0/0
```

BGP ピア ポリシー テンプレートを使用したネイバーごとの SoO 値の設定

次の作業を上の図のルータ PE1 で実行し、ピア ポリシー テンプレートを使用して、上の図のルータ CPE1 で BGP ネイバーに SoO 値を設定します。この作業では、ピア ポリシー テンプレートが作成され、SoO 値がピア ポリシーに対して設定されます。アドレス ファミリ IPv4 仮想ルーティング/転送（VRF）の下で、ネイバーが特定され、SoO 値を含むピア ポリシーを継承するように設定されます。

BGP ピアが異なる SoO 値を指定する複数のピア ポリシー テンプレートから継承される場合、最後に適用されたテンプレートの SoO 値が優先され、ピアに適用されます。ただし、BGP ネイバーで SoO 値を直接設定すると、SoO 値の、継承されたあらゆるテンプレート設定が上書きされます。

始める前に

この作業は、Cisco Express Forwarding の有効化と VRF インスタンスの設定 （745 ページ）で説明された作業が実行済みであることを前提としています。

（注） BGP ピアは、ピア ポリシー テンプレートまたはピア セッション テンプレートからの継承と、ピア グループ メンバとしての設定を同時に行うことはできません。BGP テンプレートと BGP ピア グループは同時に使用できません。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **soo** *extended-community-value*
6. **exit-peer-policy**
7. **address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*]
8. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
9. **neighbor** *ip-address* **activate**
10. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*
11. **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 50000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Router(config-router)# template peer-policy SOO_POLICY`	ピア ポリシー テンプレートを作成し、ポリシー テンプレート コンフィギュレーション モードを開始します。
ステップ 5	**soo** *extended-community-value* 例： `Router(config-router-ptmp)# soo 65000:1`	SoO 値を BGP ピア ポリシー テンプレートに設定します。 • *extended-community-value* 引数を使用して、VPN 拡張コミュニティ値を指定します。この値は、次のいずれかの形式です。 • 16 ビットの自律システム番号、コロン、および32 ビットの数字（例：45000:3）。

	コマンドまたはアクション	目的
		• 32 ビットの IP アドレス、コロン、および 16 ビットの数字（例：192.168.10.2:51） • この例では、SoO 値は、65000:1 に設定されます。
ステップ 6	**exit-peer-policy** 例： `Router(config-router-pmtp)# exit-peer-policy`	ポリシー テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 7	**address-family ipv4** [**unicast** | **multicast**| **vrf** *vrf-name*] 例： `Router(config-router)# address-family ipv4 vrf SOO_VRF`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 8	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.1.1 remote-as 65000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 9	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーをイネーブルにして、IPv4 VRF アドレス ファミリのプレフィックスをローカル ルータと交換します。
ステップ 10	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例：	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。

	コマンドまたはアクション	目的
	`Router(config-router-af)# neighbor 192.168.1.1 inherit peer-policy SOO_POLICY`	• この例では、このルータは、SOO_POLICY という名前のピア ポリシー テンプレートを 192.168.1.1 ネイバーに送信して継承するように設定されます。別のピア ポリシー テンプレートが間接的に SOO_POLICY から継承される場合、間接的に継承された設定も適用されます。最大 7 つの追加ピア ポリシー テンプレートを SOO_POLICY から間接的に継承できます。
ステップ 11	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP ネイバー コマンドを使用したネイバーごとの SoO 値の設定

次の作業を上の図のルータ PE2 で実行し、**neighbor** コマンドを使用して、上の図のルータ CPE2 で BGP ネイバーに SoO 値を設定します。IPv4 VRF アドレス ファミリで、ネイバーが特定され、SoO 値がこのネイバーに設定されます。

BGP ネイバーで SoO 値を直接設定すると、継承されたあらゆる SoO 値のピア ポリシー テンプレート設定が上書きされます。

始める前に

この作業は、「CEF の確認および VRF インスタンスの設定」の項で説明された作業が、インターフェイスおよび IP アドレスに対して適切な変更を加えて実行されていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **soo** *extended-community-value*
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf SOO_VRF`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーションモードになります。 • IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.2.1 remote-as 65000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.2.1 activate`	このネイバーをイネーブルにして、IPv4 VRF アドレス ファミリのプレフィックスをローカル ルータと交換します。 • この例では、外部 BGP ピア 192.168.2.1 がアクティブ化されます。 （注） ピア グループが手順 5 で設定済みの場合、任意のパラメータを設定するときに BGP ピア グループがアクティブ化されるため、この手順は行わないでください。たとえば、BGP ピア グループは、手順 7 で **neighbor soo** コマンドを使用して SoO 値が設定されるときにアクティブになります。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soo** *extended-community-value* 例： `Device(config-router-af)# neighbor 192.168.2.1 soo 65000:1`	BGP ネイバーまたはピア グループの Site-of-Origin（SoO）値を設定します。 • この例では、ネイバー 192.168.2.1 が SoO 値 65000:1 とともに設定されます。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP ピア グループを使用したネイバーごとの SoO 値の設定

この作業を上の図のルータ PE1 で実行し、**neighbor** コマンドと BGP ピア グループ使用して、上の図のルータ CPE1 で BGP ネイバーに SoO 値を設定します。アドレス ファミリ IPv4 VRF の下に BGP ピア グループが作成され、BGP **neighbor** コマンドを使用して SoO 値が設定され、その後ネイバーが特定され、ピア グループ メンバとして追加されます。BGP ピア グループ メンバは、ピア グループに関連付けられた設定を継承します。この例では、ピア グループには SoO 値が含まれます。

BGP ネイバーで SoO 値を直接設定すると、継承されたあらゆる SoO 値のピア グループ設定が上書きされます。

始める前に

この作業は、「Cisco Express Forwarding の有効化と VRF インスタンスの設定」で説明された作業が実行済みであることを前提としています。

（注） BGP ピアは、ピア ポリシー テンプレートまたはピア セッション テンプレートからの継承と、ピア グループ メンバとしての設定を同時に行うことはできません。BGP テンプレートと BGP ピア グループは同時に使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** {*ip-address* | *peer-group-name*} **soo** *extended-community-value*
7. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
8. **neighbor** *ip-address* **activate**
9. **neighbor** *ip-address* **peer-group** *peer-group-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4** [**unicast**	**multicast**	**vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf SOO_VRF`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、ルータは IPv4 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。

	コマンドまたはアクション	目的
		• IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router-af)# neighbor SOO_group peer-group`	BGP ピア グループを作成します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **soo** *extended-community-value* 例： `Device(config-router-af)# neighbor SOO_group soo 65000:1`	BGP ネイバーまたはピア グループの Site-of-Origin（SoO）値を設定します。 • この例では、BGP ピア グループである SOO_group が SoO 値 65000:1 を使用して設定されます。
ステップ 7	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 65000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 8	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーを有効にして、IPv4 VRF アドレス ファミリのプレフィックスをローカル ルータと交換します。
ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 peer-group SOO_group`	BGP ネイバーの IP アドレスをピア グループに割り当てます。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP のネイバーごとの SoO 設定の設定例

例：BGP ピア ポリシー テンプレートを使用したネイバーごとの SoO 値の設定

次に、ピア ポリシー テンプレートを作成し、SoO 値をピア ポリシーの一部として設定する方法の例を示します。Cisco Express Forwarding を有効にし、SOO_VRF という名前の VRF インスタンスを設定した後、ピア ポリシー テンプレートが作成され、SoO 値がピア ポリシーの一部として設定されます。IPv4 VRF アドレス ファミリの下で、ネイバーが特定され、SoO 値を含むピア ポリシーを継承するように設定されます。

```
ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface GigabitEthernet 1/0/0
 ip vrf forwarding SOO_VRF
 ip address 192.168.1.2 255.255.255.0
 exit
router bgp 50000
 template peer-policy SOO_POLICY
  soo 65000:1
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.1.1 remote-as 65000
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 inherit peer-policy SOO_POLICY
  end
```

例：BGP ネイバー コマンドを使用したネイバーごとの SoO 値の設定

次に、BGP ネイバーに SoO 値を設定する方法の例を示します。Cisco Express Forwarding を有効にし、SOO_VRF という名前の VRF インスタンスを設定した後、IPv4 VRF アドレス ファミリでネイバーが特定され、SoO 値がこのネイバーに設定されます。

```
ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface GigabitEthernet 1/0/0
 ip vrf forwarding SOO_VRF
 ip address 192.168.2.2 255.255.255.0
 exit
router bgp 50000
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.2.1 remote-as 65000
  neighbor 192.168.2.1 activate
```

```
 neighbor 192.168.2.1 soo 65000:1
 end
```

例：BGP ピア グループを使用したネイバーごとの SoO 値の設定

次に、BGP ピア グループに SoO 値を設定する方法の例を示します。Cisco Express Forwarding を有効にし、SOO_VRF という名前の VRF インスタンスを設定した後、IPv4 VRF アドレス ファミリで BGP ピア グループが設定され、SoO 値がピア グループに設定され、ネイバーが特定され、このネイバーがピア グループのメンバとして設定されます。

```
ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface GigabitEthernet 1/0/0
 ip vrf forwarding SOO_VRF
 ip address 192.168.1.2 255.255.255.0
 exit
router bgp 50000
 address-family ipv4 vrf SOO_VRF
  neighbor SOO_GROUP peer-group
  neighbor SOO_GROUP soo 65000:65
  neighbor 192.168.1.1 remote-as 65000
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 peer-group SOO_GROUP
  end
```

次の作業

- BGP の概要を確認する場合は、「Cisco BGP 概要」モジュールに進んでください。
- 基本的な BGP 機能の作業を実行する場合は、「基本 BGP ネットワークの設定」モジュールに進んでください。
- BGP の拡張機能の作業を実行する場合は、「BGP の拡張機能の設定」モジュールに進んでください。
- BGP ネイバー セッション オプションを設定する場合は、「BGP ネイバー セッション オプションの設定」モジュールに進んでください。
- 内部 BGP 作業を実行する場合は、「内部 BGP 機能の設定」モジュールに進んでください。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
IP スイッチング コマンド	『Cisco IOS IP Switching Command Reference』

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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 のネイバーごとの SoO 設定の機能情報

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

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 *57 : BGP* のネイバーごとの *SoO* 設定の機能情報

機能名	リリース	機能情報
BGP のネイバーごとの SoO 設定	Cisco IOS XE Release 2.1	BGP のネイバー SoO ごとの設定機能を使用すると、Site-of-Origin（SoO）パラメータの設定が簡略化されます。ネイバーごとの SoO 設定により、ルータ コンフィギュレーション モードの下のサブモードで設定可能な 2 つの新しいコマンドが導入され、SoO 値が設定されます。 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。 この機能により、次のコマンドが導入されました。**neighbor soo**、**soo**

第 42 章

BGP ルータ ID の VRF 単位での割り当て

BGP ルータ ID の VRF 単位の割り当て機能により、同じルータ上のボーダー ゲートウェイ プロトコル（BGP）内に VRF-to-VRF ピアリングを持つ機能が追加されます。BGP は、ルータ ID チェックのため、BGP 自身でセッションを拒否するように設計されています。VRF 単位の割り当て機能を使用すると、既存の **bgp router-id** コマンドの新しいキーワードを使用して、VRF 単位で異なるルータ ID を使用できます。ルータ ID は、VRF 単位での手動設定、または、アドレス ファミリ コンフィギュレーション モードでのグローバルな自動割り当てや VRF 単位の自動割り当てが可能です。

- 機能情報の確認 （761 ページ）
- BGP ルータ ID の VRF 単位での割り当ての前提条件 （762 ページ）
- BGP ルータ ID の VRF 単位での割り当てに関する情報 （762 ページ）
- BGP ルータ ID の VRF 単位での割り当ての設定方法 （763 ページ）
- BGP ルータ ID の VRF 単位での割り当ての設定例 （780 ページ）
- その他の参考資料 （787 ページ）
- BGP ルータ ID の VRF 単位での割り当てに関する機能情報 （788 ページ）

機能情報の確認

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

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

BGP ルータ ID の VRF 単位での割り当ての前提条件

この機能を設定する前に、ネットワーク内で Cisco Express Forwarding または distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）が有効になっている必要があり、また、BGP ピアリングがネットワーク内で実行されていることが前提になっています。

BGP ルータ ID の VRF 単位での割り当てに関する情報

BGP ルータ ID

BGP ルータ ID は、ルータの最大 IP アドレスに設定される 4 バイト フィールドです。ループバック インターフェイス アドレスは物理インターフェイスよりも安定しているため、ループバック インターフェイスのアドレスが物理インターフェイスよりも前に考慮されます。BGP ルータ ID は、最小ルータ ID を持つ BGP ルータにプリファレンスが設定されている宛先へのベスト パスを決定するために、BGP アルゴリズムで使用されます。**bgp router-id** コマンドで BGP ルータ ID を手動で設定して、ベスト パスのアルゴリズムに影響を与えることが可能です。

VRF 単位でのルータ ID の割り当て

Cisco IOS XE Release 2.1 以降のリリースでは、各バーチャルプライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに対する個別のルータ ID の設定に対するサポートが追加されました。BGP ルータ ID の VRF 単位の割り当て機能により、同じルータ上のボーダー ゲートウェイ プロトコル（BGP）内に VRF-to-VRF ピアリングを持つ機能が追加されます。BGP は、ルータ ID チェックのため、BGP 自身でセッションを拒否するように設計されています。VRF 単位の割り当て機能を使用すると、既存の **bgp router-id** コマンドの新しいキーワードを使用して、VRF 単位で異なるルータ ID を使用できます。ルータ ID は、VRF 単位での手動設定、または、アドレス ファミリ コンフィギュレーション モードでのグローバルな自動割り当てや VRF 単位の自動割り当てが可能です。

ルート識別子

ルート識別子（RD）はルーティング テーブルとフォワーディング テーブルを作成し、VPN のデフォルトのルート識別子を指定します。IPv4 プレフィックスをグローバルに固有の VPN-IPv4 プレフィックスに変更するために、RD が IPv4 プレフィックスの先頭に追加されます。RD は、自律システム番号と任意番号、または IP アドレスと任意番号のいずれかで構成できます。

RD は、次のいずれかの形式で入力できます。

- 16 ビット自律システム番号、コロン、32 ビット番号を入力します。次に例を示します。

45000:3

- 32 ビット IP アドレス、コロン、16 ビット番号を入力します。次に例を示します。

192.168.10.15:1

BGP ルータ ID の VRF 単位での割り当ての設定方法

VRF インスタンスの設定

VRF インスタンスを VRF 割り当て作業で使用されるように設定するには、この作業を実行します。この作業では、vrf_trans という名前の VRF インスタンスが作成されます。VRF を機能させるために、ルート識別子（RD）が作成されます。ルート識別子が作成されると、vrf_trans という名前の VRF インスタンスにルーティング テーブルとフォワーディング テーブルが作成されます。

始める前に

この作業では、Cisco Express Forwarding または分散型 Cisco Express Forwarding が有効になっていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **both**} *route-target-ext-community*
6. **route-target** {**export** | **both**} *route-target-ext-community*
7. **exit**
8. 定義する VRF 単位で、ステップ 3 ～ステップ 7 を繰り返します。

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf vrf_trans`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 45000:2`	VRF にルーティング テーブルとフォワーディング テーブルを作成し、VPN にデフォルト RD を指定します。 • VPN にデフォルト RD を指定するには、*route-distinguisher* 引数を使用します。RD の指定に使用できる形式は 2 つあります。詳細については、「ルート識別子」の項を参照してください。 • この例では、RD は、コロンの後に番号 2 を持つ自律システム番号を使用します。
ステップ 5	**route-target** {**import** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target import 55000:5`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • VPN 拡張コミュニティを指定するには、*route-target-ext-community* 引数を使用します。
ステップ 6	**route-target** {**export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target export 55000:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • VPN 拡張コミュニティを指定するには、*route-target-ext-community* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Router(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	定義する VRF 単位で、ステップ 3 ～ステップ 7 を繰り返します。	--

VRF インスタンスとインターフェイスの関連付け

VRF 単位での割り当て作業で使用されるインターフェイスに VRF インスタンスを関連付けるには、この作業を実行します。この作業では、vrf_trans という名前の VRF インスタンスがシリアル インターフェイスに関連付けられます。

ip vrf forwarding コマンドにより IP アドレスが削除されるため、VRF インスタンスを関連付けるインターフェイスの IP アドレスをメモしておいてください。ステップ 8 で IP アドレスを再設定できます。

始める前に

- この作業では、Cisco Express Forwarding または分散型 Cisco Express Forwarding が有効になっていることを前提としています。
- この作業は、VRF インスタンスがVRF インスタンスの設定（763 ページ）で設定されていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **exit**
6. **interface** *type number*
7. **ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
8. **ip address** *ip-address mask* [**secondary**]
9. インターフェイスに関連付ける VRF 単位で、ステップ 5 ～ 8 を繰り返します。
10. **end**
11. **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface loopback0`	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。 • この例では、ループバック インターフェイス 0 が設定されます。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 172.16.1.1 255.255.255.255`	IP アドレスを設定します。 • この例では、ループバック インターフェイスが 172.16.1.1 の IP アドレスで設定されます。
ステップ 5	**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、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	**interface** *type number* 例： `Router(config)# interface serial2/0/0`	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。 • この例では、シリアル インターフェイス 2/0/0 が設定されています。
ステップ 7	**ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] 例： `Router(config-if)# ip vrf forwarding vrf_trans`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • この例では、vrf_trans という名前の VRF がシリアル インターフェイス 2/0/0 に関連付けられます。 （注） インターフェイスにこのコマンドを実行すると、IP アドレスが削除されます。IP アドレスを再設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 192.168.4.1 255.255.255.0`	IP アドレスを設定します。 • この例では、シリアル インターフェイス 2/0/0 が 192.168.4.1 の IP アドレスで設定されます。
ステップ 9	インターフェイスに関連付ける VRF 単位で、ステップ 5 ～ 8 を繰り返します。	--
ステップ 10	**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 モードに戻ります。
ステップ 11	**show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] 例： `Router# show ip vrf interfaces`	（任意）定義された VRF および関連付けられたインターフェイスのセットを表示します。 • この例では、このコマンド出力に、作成された VRF および関連付けられたインターフェイスが表示されます。

例

次の出力は、vrf_trans と vrf_users という名前の 2 つの VRF インスタンスが 2 つのシリアル インターフェイスに設定されたことを示しています。

```
Router# show ip vrf interfaces
Interface          IP-Address      VRF                    Protocol
Serial2            192.168.4.1     vrf_trans              up
Serial3            192.168.5.1     vrf_user               up
```

VRF 単位での BGP ルータ ID の手動設定

VRF 単位で BGP ルータ ID を手動で設定するには、この作業を実行します。この作業では、複数のアドレス ファミリ コンフィギュレーションが示され、1 つの VRF インスタンスに対して、IPv4 アドレス ファミリ モードでルータ ID が設定されます。ステップ 22 は、特定のステップを繰り返して、同じルータ上で複数の VRF の設定を許可する方法を示します。

始める前に

この作業は、事前に VRF インスタンスを作成し、そのインスタンスをインターフェイスに関連付けていることを前提とします。詳細については、VRF インスタンスの設定（763 ページ）およびVRF インスタンスとインターフェイスの関連付け（765 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**
5. **bgp log-neighbor-changes**
6. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
9. **neighbor** {*ip-address*| *peer-group-name*} **activate**
10. **neighbor** {*ip-address*| *peer-group-name*} **send-community**{**both**| **standard**| **extended**}
11. **exit-address-family**
12. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
13. **redistribute connected**
14. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
15. **neighbor** *ip-address* **local-as** *autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]
16. **neighbor** {*ip-address*| *peer-group-name*} **ebgp-multihop**[*ttl*]
17. **neighbor** {*ip-address*| *peer-group-name*} **activate**
18. **neighbor** *ip-address* **allowas-in** [*number*]
19. **no auto-summary**
20. **no synchronization**
21. **bgp router-id** {*ip-address*| **auto-assign**}
22. 別の VRF インスタンスを設定するには、ステップ 11 ～ 21 を繰り返します。
23. **end**
24. **show ip bgp vpnv4** {**all**| **rd** *route-distinguisher*| **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 5	**bgp log-neighbor-changes** 例： `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングを有効にします。
ステップ 6	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、ネイバーは内部ネイバーになります。
ステップ 7	**neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number* 例： `Router(config-router)# neighbor 192.168.1.1 update-source loopback0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • この例では、指定されたネイバーの BGP TCP 接続が、最良のローカル アドレスではなく、ループバック インターフェイスの IP アドレスで発信されます。

	コマンドまたはアクション	目的
ステップ 8	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、VPNv4 アドレス ファミリ セッションを作成します。
ステップ 9	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 172.16.1.1 activate`	VPNv4アドレスファミリの下のネイバーをアクティブにします。 • この例では、ネイバー172.16.1.1がアクティブ化されます。
ステップ 10	**neighbor** {*ip-address*| *peer-group-name*} **send-community**{**both**| **standard**| **extended**} 例： `Router(config-router-af)# neighbor 172.16.1.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • この例では、拡張コミュニティ属性が172.16.1.1のネイバーに送信されます。
ステップ 11	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 12	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} 例： `Router(config-router)# address-family ipv4 vrf vrf_trans`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、vrf_trans という名前の VRF インスタンスが後続の IPv4 アドレス ファミリ コンフィギュレーション コマンドに関連付けられるように指定します。
ステップ 13	**redistribute connected** 例： `Router(config-router-af)# redistribute connected`	あるルーティング ドメインから別のルーティング ドメインに再配布します。 • この例では、インターフェイスで IP が有効化されると自動的に確立されるルートを表すために、**connected** キーワードが使用されます。 • この手順に適用される構文だけが表示されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 14	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.1.1 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、192.168.1.1 のネイバーは外部ネイバーです。
ステップ 15	**neighbor** *ip-address* **local-as** *autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]] 例： `Router(config-router-af)# neighbor 192.168.1.1 local-as 50000 no-prepend`	eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズします。 • ローカル BGP ルーティング プロセスからの自律システム番号は、デフォルトで、すべての外部ルートに追加されます。 • eBGP ネイバーから受信されたルートにローカル自律システム番号を付加しない場合は、**no-prepend** キーワードを使用します。 • この例では、192.168.1.1 のネイバーからのルートにローカル自律システム番号が含まれていません。
ステップ 16	**neighbor** {*ip-address*| *peer-group-name*} **ebgp-multihop**[*ttl*] 例： `Router(config-router-af)# neighbor 192.168.1.1 ebgp-multihop 2`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。 • この例では、直接接続されていないネットワーク上に存在するネイバー 192.168.1.1 との接続ができるように BGP を設定します。
ステップ 17	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。 • この例では、ネイバー 192.168.1.1 がアクティブにされます。

	コマンドまたはアクション	目的
ステップ 18	**neighbor** *ip-address* **allowas-in** [*number*] 例： `Router(config-router-af)# neighbor 192.168.1.1 allowas-in 1`	複製の自律システム番号が含まれるプレフィックスをすべて再アドバタイズできるように、プロバイダー エッジ（PE）ルータを設定します。 • この例では、自律システム番号が 45000 の PE ルータが VRF vrf-trans からのプレフィックスを許可するように設定されます。IP アドレスが 192.168.1.1 のネイバー PE ルータが、同じ自律システム番号の別の PE ルータに 1 回再アドバタイズされるように設定されます。
ステップ 19	**no auto-summary** 例： `Router(config-router-af)# no auto-summary`	自動サマライズを無効にし、サブプレフィックス ルーティング情報をクラスフル ネットワーク境界間で送信します。
ステップ 20	**no synchronization** 例： `Router(config-router-af)# no synchronization`	Cisco IOS XE ソフトウェアが内部ゲートウェイ プロトコル（IGP）との同期を待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 21	**bgp router-id** {*ip-address*| **auto-assign**} 例： `Router(config-router-af)# bgp router-id 10.99.1.1`	ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。 • この例では、指定された BGP ルータ ID が、IPv4 アドレス ファミリ コンフィギュレーションに関連付けられた VRF インスタンスに割り当てられます。
ステップ 22	別の VRF インスタンスを設定するには、ステップ 11 ～ 21 を繰り返します。	--
ステップ 23	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 24	**show ip bgp vpnv4** {**all**| **rd** *route-distinguisher*| **vrf** *vrf-name*} 例： `Router# show ip bgp vpnv4 all`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • この例では、すべての VPNv4 データベースが表示されます。

	コマンドまたはアクション	目的
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。

例

次のサンプル出力は、vrf_trans と vrf_user という名前の 2 つの VRF インスタンスが個別のルータ ID で設定されていることを前提としています。ルータ ID が VRF 名の次に表示されます。

```
Router# show ip bgp vpnv4 all
BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

VRF 単位での BGP ルータ ID の自動割り当て

VRF 単位で BGP ルータ ID を自動で設定するには、この作業を実行します。この作業では、ループバック インターフェイスが VRF に関連付けられ、**bgp router-id** コマンドがルータ コンフィギュレーション レベルで設定されて、BGP ルータ ID がすべての VRF インスタンスに自動的に割り当てられます。ステップ 9 は、特定のステップを繰り返して、インターフェイスに関連付けられる各 VRF を設定する方法を示します。ステップ 30 は、同じルータ上で複数の VRF を設定する方法を示します。

始める前に

この作業は、事前に VRF インスタンスを作成していることを前提とします。詳細については、VRF インスタンスの設定 （763 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **exit**
6. **interface** *type number*

7. **ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
8. **ip address** *ip-address mask* [**secondary**]
9. インターフェイスに関連付ける VRF 単位で、ステップ 5 ～ 8 を繰り返します。
10. **exit**
11. **router bgp** *autonomous-system-number*
12. **bgp router-id** {*ip-address*| **vrf auto-assign**}
13. **no bgp default ipv4-unicast**
14. **bgp log-neighbor-changes**
15. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
16. **neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number*
17. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
18. **neighbor** {*ip-address*| *peer-group-name*} **activate**
19. **neighbor** {*ip-address*| *peer-group-name*} **send-community**{**both**| **standard**| **extended**}
20. **exit-address-family**
21. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
22. **redistribute connected**
23. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
24. **neighbor** *ip-address* **local-as** *autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]
25. **neighbor** {*ip-address*| *peer-group-name*} **ebgp-multihop**[*ttl*]
26. **neighbor** {*ip-address*| *peer-group-name*} **activate**
27. **neighbor** *ip-address* **allowas-in** [*number*]
28. **no auto-summary**
29. **no synchronization**
30. 別の VRF インスタンスを設定するには、ステップ 20 ～ 29 を繰り返します。
31. **end**
32. **show ip bgp vpnv4** {**all**| **rd** *route-distinguisher*| **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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** *type number* 例： `Router(config)# interface loopback0`	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。 • この例では、ループバック インターフェイス 0 が設定されます。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 172.16.1.1 255.255.255.255`	IP アドレスを設定します。 • この例では、ループバック インターフェイスが 172.16.1.1 の IP アドレスで設定されます。
ステップ 5	**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、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	**interface** *type number* 例： `Router(config)# interface loopback1`	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。 • この例では、ループバック インターフェイス 1 が設定されます。
ステップ 7	**ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] 例： `Router(config-if)# ip vrf forwarding vrf_trans`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • この例では、vrf_trans という名前の VRF がループバック インターフェイス 1 に関連付けられます。 （注） インターフェイスにこのコマンドを実行すると、IP アドレスが削除されます。IP アドレスを再設定する必要があります。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.99.1.1 255.255.255.255`	IP アドレスを設定します。 • この例では、ループバック インターフェイス 1 が 10.99.1.1 の IP アドレスで設定されます。
ステップ 9	インターフェイスに関連付ける VRF 単位で、ステップ 5 ～ 8 を繰り返します。	--
ステップ 10	**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、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 11	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**bgp router-id** {*ip-address*| **vrf auto-assign**} 例： `Router(config-router)# bgp router-id vrf auto-assign`	ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。 • この例では、BGP ルータ ID が VRF インスタンス単位で自動的に割り当てられます。
ステップ 13	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 14	**bgp log-neighbor-changes** 例： `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングを有効にします。
ステップ 15	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、ネイバーは内部ネイバーになります。

	コマンドまたはアクション	目的
ステップ 16	**neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number* 例： `Router(config-router)# neighbor 192.168.1.1 update-source loopback0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • この例では、指定されたネイバーの BGP TCP 接続が、最良のローカル アドレスではなく、ループバック インターフェイスの IP アドレスで発信されます。
ステップ 17	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、VPNv4 アドレス ファミリ セッションを作成します。
ステップ 18	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 172.16.1.1 activate`	VPNv4 アドレス ファミリの下のネイバーをアクティブにします。 • この例では、ネイバー 172.16.1.1 がアクティブ化されます。
ステップ 19	**neighbor** {*ip-address*| *peer-group-name*} **send-community**{**both**| **standard**| **extended**} 例： `Router(config-router-af)# neighbor 172.16.1.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • この例では、拡張コミュニティ属性が 172.16.1.1 のネイバーに送信されます。
ステップ 20	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 21	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} 例： `Router(config-router)# address-family ipv4 vrf vrf_trans`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、vrf_trans という名前の VRF インスタンスが後続の IPv4 アドレス ファミリ コンフィギュレーション モードのコマンドに関連付けられるように指定します。
ステップ 22	**redistribute connected** 例：	あるルーティング ドメインから別のルーティング ドメインに再配布します。

	コマンドまたはアクション	目的
	`Router(config-router-af)# redistribute connected`	• この例では、インターフェイスで IP が有効化されると自動的に確立されるルートを表すために、**connected** キーワードが使用されます。 • この手順に適用される構文だけが表示されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 23	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.1.1 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、192.168.1.1 のネイバーは外部ネイバーです。
ステップ 24	**neighbor** *ip-address* **local-as** *autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]] 例： `Router(config-router-af)# neighbor 192.168.1.1 local-as 50000 no-prepend`	eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズします。 • ローカル BGP ルーティング プロセスからの自律システム番号は、デフォルトで、すべての外部ルートに追加されます。 • eBGP ネイバーから受信されたルートにローカル自律システム番号を付加しない場合は、**no-prepend** キーワードを使用します。 • この例では、192.168.1.1 のネイバーからのルートにローカル自律システム番号が含まれていません。
ステップ 25	**neighbor** {*ip-address*| *peer-group-name*} **ebgp-multihop**[*ttl*] 例：	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

	コマンドまたはアクション	目的
	`Router(config-router-af)# neighbor 192.168.1.1 ebgp-multihop 2`	• この例では、直接接続されていないネットワーク上に存在するネイバー 192.168.1.1 との接続ができるように BGP を設定します。
ステップ 26	**neighbor** {*ip-address*| *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。 • この例では、ネイバー 192.168.1.1 がアクティブにされます。
ステップ 27	**neighbor** *ip-address* **allowas-in** [*number*] 例： `Router(config-router-af)# neighbor 192.168.1.1 allowas-in 1`	複製の自律システム番号が含まれるプレフィックスをすべて再アドバタイズできるように、プロバイダー エッジ（PE）ルータを設定します。 • この例では、自律システム番号が 45000 の PE ルータが VRF vrf-trans からのプレフィックスを許可するように設定されます。IP アドレスが 192.168.1.1 のネイバー PE ルータが、同じ自律システム番号の別の PE ルータに 1 回再アドバタイズされるように設定されます。
ステップ 28	**no auto-summary** 例： `Router(config-router-af)# no auto-summary`	自動サマライズを無効にし、サブプレフィックス ルーティング情報をクラスフル ネットワーク境界間で送信します。
ステップ 29	**no synchronization** 例： `Router(config-router-af)# no synchronization`	Cisco IOS XE ソフトウェアが内部ゲートウェイ プロトコル（IGP）との同期を待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 30	別の VRF インスタンスを設定するには、ステップ 20 ～ 29 を繰り返します。	--
ステップ 31	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 32	**show ip bgp vpnv4** {**all**| **rd** *route-distinguisher*| **vrf** *vrf-name*} 例： `Router# show ip bgp vpnv4 all`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • この例では、すべての VPNv4 データベースが表示されます。

	コマンドまたはアクション	目的
		（注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。

例

次のサンプル出力は、vrf_trans と vrf_user という名前の 2 つの VRF インスタンスが個別のルータ ID で設定されていることを前提としています。ルータ ID が VRF 名の次に表示されます。

```
Router# show ip bgp vpnv4 all
BGP table version is 43, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 172.22.0.0       0.0.0.0                  0         32768 ?
r> 172.23.0.0       172.23.1.1               0             0 3 1 ?
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
*> 10.52.1.0/24     172.23.1.1                            0 3 1 ?
*> 10.52.2.1/32     172.23.1.1                            0 3 1 3 i
*> 10.52.3.1/32     172.23.1.1                            0 3 1 3 i
*> 10.99.1.1/32     172.23.1.1               0             0 3 1 ?
*> 10.99.1.2/32     0.0.0.0                  0         32768 ?
Route Distinguisher: 10:1
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
r> 172.22.0.0       172.22.1.1               0             0 2 1 ?
*> 172.23.0.0       0.0.0.0                  0         32768 ?
*> 10.21.1.1/32     172.22.1.1                            0 2 1 2 i
*>i10.52.1.0/24     192.168.3.1              0    100      0 ?
*>i10.52.2.1/32     192.168.3.1              0    100      0 3 i
*>i10.52.3.1/32     192.168.3.1              0    100      0 3 i
*> 10.99.1.1/32     0.0.0.0                  0         32768 ?
*> 10.99.1.2/32     172.22.1.1               0             0 2 1 ?
```

BGP ルータ ID の VRF 単位での割り当ての設定例

VRF 単位での BGP ルータ ID の手動設定例

次の例は、vrf_trans と vrf_user の 2 つの VRF を、同じルータ上で相互間のセッションで設定する方法を示します。VRF 単位での BGP ルータ ID は、個別の IPv4 アドレス ファミリの下で手動で設定されます。**show ip bgp vpnv4** コマンドを使用すると、ルータ ID が VRF 単位に設定さ

れていることを確認できます。このコンフィギュレーションは、グローバル コンフィギュレーション モードで開始されます。

```
ip vrf vrf_trans
 rd 45000:1
 route-target export 50000:50
 route-target import 40000:1
!
ip vrf vrf_user
 rd 65500:1
 route-target export 65500:1
 route-target import 65500:1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 45000
 neighbor 192.168.3.1 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.3.1 activate
  neighbor 192.168.3.1 send-community extended
  exit-address-family
 !
 address-family ipv4 vrf vrf_user
  redistribute connected
  neighbor 172.22.1.1 remote-as 40000
  neighbor 172.22.1.1 local-as 50000 no-prepend
  neighbor 172.22.1.1 ebgp-multihop 2
  neighbor 172.22.1.1 activate
  neighbor 172.22.1.1 allowas-in 1
  no auto-summary
  no synchronization
  bgp router-id 10.99.1.1
  exit-address-family
 !
 address-family ipv4 vrf vrf_trans
  redistribute connected
  neighbor 172.23.1.1 remote-as 50000
  neighbor 172.23.1.1 local-as 40000 no-prepend
  neighbor 172.23.1.1 ebgp-multihop 2
  neighbor 172.23.1.1 activate
  neighbor 172.23.1.1 allowas-in 1
  no auto-summary
  no synchronization
  bgp router-id 10.99.1.2
  exit-address-family
```

コンフィギュレーションの後、**show ip bgp vpnv4 all** コマンドの出力には、VRF 名の次に表示されるルータ ID が表示されます。

```
Router# show ip bgp vpnv4 all
BGP table version is 43, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 172.22.0.0       0.0.0.0                  0         32768 ?
```

```
r> 172.23.0.0       172.23.1.1               0             0 3 1 ?
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
*> 10.52.1.0/24     172.23.1.1                            0 3 1 ?
*> 10.52.2.1/32     172.23.1.1                            0 3 1 3 i
*> 10.52.3.1/32     172.23.1.1                            0 3 1 3 i
*> 10.99.1.1/32     172.23.1.1               0            0 3 1 ?
*> 10.99.2.2/32     0.0.0.0                  0        32768 ?
Route Distinguisher: 50000:1
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
Route Distinguisher: 65500:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
r> 172.22.0.0       172.22.1.1               0             0 2 1 ?
*> 172.23.0.0       0.0.0.0                  0        32768 ?
*> 10.21.1.1/32     172.22.1.1                            0 2 1 2 i
*>i10.52.1.0/24     192.168.3.1              0    100      0 ?
*>i10.52.2.1/32     192.168.3.1              0    100      0 3 i
*>i10.52.3.1/32     192.168.3.1              0    100      0 3 i
*> 10.99.1.1/32     0.0.0.0                  0        32768 ?
*> 10.99.2.2/32     172.22.1.1               0             0 2 1 ?
```

指定された VRF の **show ip bgp vpnv4 vrf** コマンドの出力には、出力ヘッダーにルータ ID が表示されます。

```
Router# show ip bgp vpnv4 vrf vrf_user
BGP table version is 43, local router ID is 10.99.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65500:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
r> 172.22.0.0       172.22.1.1               0             0 2 1 ?
*> 172.23.0.0       0.0.0.0                  0        32768 ?
*> 10.21.1.1/32     172.22.1.1                            0 2 1 2 i
*>i10.52.1.0/24     192.168.3.1              0    100      0 ?
*>i10.52.2.1/32     192.168.3.1              0    100      0 3 i
*>i10.52.3.1/32     192.168.3.1              0    100      0 3 i
*> 10.99.1.1/32     0.0.0.0                  0        32768 ?
*> 10.99.2.2/32     172.22.1.1               0             0 2 1 ?
```

指定された VRF の **show ip bgp vpnv4 vrf summary** コマンドの出力には、出力の最初の行にルータ ID が表示されます。

```
Router# show ip bgp vpnv4 vrf vrf_user summary
BGP router identifier 10.99.1.1, local AS number 45000
BGP table version is 43, main routing table version 43
8 network entries using 1128 bytes of memory
8 path entries using 544 bytes of memory
16/10 BGP path/bestpath attribute entries using 1856 bytes of memory
6 BGP AS-PATH entries using 144 bytes of memory
3 BGP extended community entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3744 total bytes of memory
BGP activity 17/0 prefixes, 17/0 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.22.1.1      4     2      20      21       43    0    0 00:12:33        3
```

パスが VRF で送信されると、指定された VRF とネットワーク アドレスの **show ip bgp vpnv4 vrf** コマンドの出力に、正しいルータ ID が表示されます。

```
Router# show ip bgp vpnv4 vrf vrf_user 172.23.0.0
BGP routing table entry for 65500:1:172.23.0.0/8, version 22
```

```
Paths: (1 available, best #1, table vrf_user)
  Advertised to update-groups:
     2          3
  Local
    0.0.0.0 from 0.0.0.0 (10.99.1.1)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:65500:1
```

VRF 単位での BGP ルータ ID の自動割り当て例

次に、BGP が個別のルータ ID を各 VRF インスタンスに自動的に割り当てるように設定する 3 つの異なる設定例を示します。

ループバック インターフェイス IP アドレスを使用してグローバルに自動割り当てされるルータ ID の例

次の例は、vrf_trans と vrf_user の 2 つの VRF を、同じルータ上で相互間のセッションで設定する方法を示します。ルータ コンフィギュレーション モードでは、BGP が、各 VRF に BGP ルータ ID を自動的に割り当てるようにグローバルに設定されます。ループバック インターフェイスは、ルータ ID の IP アドレスを送信するために個別の VRF に関連付けられます。**show ip bgp vpnv4** コマンドを使用すると、ルータ ID が VRF 単位に設定されていることを確認できます。

```
ip vrf vrf_trans
 rd 45000:1
 route-target export 50000:50
 route-target import 40000:1
!
ip vrf vrf_user
 rd 65500:1
 route-target export 65500:1
 route-target import 65500:1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface Loopback1
 ip vrf forwarding vrf_user
 ip address 10.99.1.1 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vrf_trans
 ip address 10.99.2.2 255.255.255.255
!
router bgp 45000
 bgp router-id vrf auto-assign
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 45000
 neighbor 192.168.3.1 update-source Loopback0
 !
address-family vpnv4
  neighbor 192.168.3.1 activate
  neighbor 192.168.3.1 send-community extended
  exit-address-family
 !
 address-family ipv4 vrf vrf_user
  redistribute connected
```

```
 neighbor 172.22.1.1 remote-as 40000
 neighbor 172.22.1.1 local-as 50000 no-prepend
 neighbor 172.22.1.1 ebgp-multihop 2
 neighbor 172.22.1.1 activate
 neighbor 172.22.1.1 allowas-in 1
 no auto-summary
 no synchronization
 exit-address-family
!
address-family ipv4 vrf vrf_trans
 redistribute connected
 neighbor 172.23.1.1 remote-as 50000
 neighbor 172.23.1.1 local-as 2 no-prepend
 neighbor 172.23.1.1 ebgp-multihop 2
 neighbor 172.23.1.1 activate
 neighbor 172.23.1.1 allowas-in 1
 no auto-summary
 no synchronization
 exit-address-family
```

コンフィギュレーションの後、**show ip bgp vpnv4 all** コマンドの出力には、VRF 名の次に表示されるルータ ID が表示されます。この例で使用されているルータ ID が、ループバック インターフェイス 1 およびループバック インターフェイス 2 で設定された IP アドレスから送信されていることに注意してください。ルータ ID は、VRF 単位での BGP ルータ ID の手動設定例（780 ページ）と同じです。

```
Router# show ip bgp vpnv4 all
BGP table version is 43, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:1 (default for vrf vrf_trans) VRF Router ID 10.99.2.2
*> 172.22.0.0       0.0.0.0                  0         32768 ?
r> 172.23.0.0       172.23.1.1               0             0 3 1 ?
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
*> 10.52.1.0/24     172.23.1.1                             0 3 1 ?
*> 10.52.2.1/32     172.23.1.1                             0 3 1 3 i
*> 10.52.3.1/32     172.23.1.1                             0 3 1 3 i
*> 10.99.1.1/32     172.23.1.1               0             0 3 1 ?
*> 10.99.1.2/32     0.0.0.0                  0         32768 ?
Route Distinguisher: 50000:1
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
Route Distinguisher: 65500:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
r> 172.22.0.0       172.22.1.1               0             0 2 1 ?
*> 172.23.0.0       0.0.0.0                  0         32768 ?
*> 10.21.1.1/32     172.22.1.1                             0 2 1 2 i
*>i10.52.1.0/24     192.168.3.1              0    100      0 ?
*>i10.52.2.1/32     192.168.3.1              0    100      0 3 i
*>i10.52.3.1/32     192.168.3.1              0    100      0 3 i
*> 10.99.1.1/32     0.0.0.0                  0         32768 ?
*> 10.99.1.2/32     172.22.1.1               0             0 2 1 ?
```

デフォルト ルータ ID がない場合にグローバルに自動割り当てされるルータ ID の例

次に、ルータを設定して、デフォルトのルータ ID が割り当てられない場合に自動的に BGP ルータ ID が割り当てられる VRF を関連付ける例を示します。

```
ip vrf vpn1
 rd 45000:1
```

```
 route-target export 45000:1
 route-target import 45000:1
!
interface Loopback0
 ip vrf forwarding vpn1
 ip address 10.1.1.1 255.255.255.255
!
router bgp 45000
 bgp router-id vrf auto-assign
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf vpn1
  neighbor 172.22.1.2 remote-as 40000
  neighbor 172.22.1.2 activate
  no auto-summary
  no synchronization
  exit-address-family
```

別のルータが 2 つのルータ間のセッションを確立するように設定されていることを前提として、**show ip interface brief** コマンドの出力には、設定済みの VRF インターフェイスだけが表示されます。

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Serial2/0/0            unassigned      YES NVRAM  administratively down down
Serial3/0/0            unassigned      YES NVRAM  administratively down down
Loopback0              10.1.1.1        YES NVRAM  up                    up
```

show ip vrf コマンドを使用すると、ルータ ID が VRF に対して割り当てられていることを確認できます。

```
Router# show ip vrf
Name                              Default RD          Interfaces
  vpn1                              45000:1           Loopback0
VRF session is established:
```

VRF 単位で自動割り当てされるルータ ID の例

次の例は、vrf_trans と vrf_user の 2 つの VRF を、同じルータ上で相互間のセッションで設定する方法を示します。個別の VRF に関連付けられた IPv4 アドレス ファミリの下では、BGP が自動的に BGP ルータ ID を割り当てるように設定されます。ループバック インターフェイスは、ルータ ID の IP アドレスを送信するために個別の VRF に関連付けられます。**show ip bgp vpnv4** コマンドを使用すると、ルータ ID が VRF 単位に設定されていることを確認できます。

```
ip vrf vrf_trans
 rd 45000:1
 route-target export 50000:50
 route-target import 40000:1
!
ip vrf vrf_user
 rd 65500:1
 route-target export 65500:1
 route-target import 65500:1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
```

```
interface Loopback1
 ip vrf forwarding vrf_user
 ip address 10.99.1.1 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vrf_trans
 ip address 10.99.2.2 255.255.255.255
!
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 45000
 neighbor 192.168.3.1 update-source Loopback0
 !
address-family vpnv4
  neighbor 192.168.3.1 activate
  neighbor 192.168.3.1 send-community extended
  exit-address-family
!
 address-family ipv4 vrf vrf_user
  redistribute connected
  neighbor 172.22.1.1 remote-as 40000
  neighbor 172.22.1.1 local-as 50000 no-prepend
  neighbor 172.22.1.1 ebgp-multihop 2
  neighbor 172.22.1.1 activate
  neighbor 172.22.1.1 allowas-in 1
  no auto-summary
  no synchronization
  bgp router-id auto-assign
  exit-address-family
 !
 address-family ipv4 vrf vrf_trans
  redistribute connected
  neighbor 172.23.1.1 remote-as 50000
  neighbor 172.23.1.1 local-as 40000 no-prepend
  neighbor 172.23.1.1 ebgp-multihop 2
  neighbor 172.23.1.1 activate
  neighbor 172.23.1.1 allowas-in 1
  no auto-summary
  no synchronization
  bgp router-id auto-assign
  exit-address-family
```

コンフィギュレーションの後、**show ip bgp vpnv4 all** コマンドの出力には、VRF 名の次に表示されるルータ ID が表示されます。この例で使用されているルータ ID が、ループバック インターフェイス 1 およびループバック インターフェイス 2 で設定された IP アドレスから送信されていることに注意してください。

```
Router# show ip bgp vpnv4 all
BGP table version is 43, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:1 (default for vrf vrf_trans) VRF Router ID 10.99.2.2
*> 172.22.0.0       0.0.0.0                  0         32768 ?
r> 172.23.0.0       172.23.1.1               0             0 3 1 ?
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
*> 10.52.1.0/24     172.23.1.1                             0 3 1 ?
*> 10.52.2.1/32     172.23.1.1                             0 3 1 3 i
*> 10.52.3.1/32     172.23.1.1                             0 3 1 3 i
*> 10.99.1.1/32     172.23.1.1               0             0 3 1 ?
```

```
*> 10.99.1.2/32     0.0.0.0                  0         32768 ?
Route Distinguisher: 50000:1
*>i10.21.1.1/32     192.168.3.1              0    100      0 2 i
Route Distinguisher: 65500:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
r> 172.22.0.0       172.22.1.1               0             0 2 1 ?
*> 172.23.0.0       0.0.0.0                  0         32768 ?
*> 10.21.1.1/32     172.22.1.1                             0 2 1 2 i
*>i10.52.1.0/24     192.168.3.1              0    100      0 ?
*>i10.52.2.1/32     192.168.3.1              0    100      0 3 i
*>i10.52.3.1/32     192.168.3.1              0    100      0 3 i
*> 10.99.1.1/32     0.0.0.0                  0         32768 ?
*> 10.99.1.2/32     172.22.1.1               0             0 2 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
BGP コマンド：コマンド構文の詳細、デフォルト、コマンド モード、コマンド履歴、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
MPLS コマンド：コマンド構文の詳細、デフォルト、コマンド モード、コマンド履歴、使用上の注意事項、および例	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格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	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
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

BGP ルータ ID の VRF 単位での割り当てに関する機能情報

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 *58 : BGP* ルータ *ID* の *VRF* 単位での割り当てに関する機能情報

機能名	リリース	機能情報
BGP ルータ ID の VRF 単位での割り当て	Cisco IOS XE Release 2.1	BGP ルータ ID の VRF 単位の割り当て機能により、同じルータ上のボーダーゲートウェイ プロトコル（BGP）内に VRF-to-VRF ピアリングを持つ機能が追加されます。BGP は、ルータ ID チェックのため、BGP 自身でセッションを拒否するように設計されています。VRF 単位の割り当て機能を使用すると、既存の **bgp router-id** コマンドの新しいキーワードを使用して、VRF 単位で異なるルータ ID を使用できます。ルータ ID は、VRF 単位での手動設定、または、アドレス ファミリ コンフィギュレーション モードでのグローバルな自動割り当てや VRF 単位の自動割り当てが可能です。 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。 この機能により、次のコマンドが導入または変更されました。**bgp router-id**、**show ip bgp vpnv4**

第 43 章

BGP ネクスト ホップ非変更

外部 BGP（eBGP）セッションでは、デフォルトで、ルータがルートの送信時に BGP ルートのネクスト ホップ属性を（自身のアドレスに）変更します。BGP ネクスト ホップ非変更機能では、ネクスト ホップ属性を変更せずに BGP によって eBGP マルチホップ ピアにアップデートを送信できます。

- 機能情報の確認 （791 ページ）
- ネクスト ホップ非変更に関する情報 （792 ページ）
- BGP ネクスト ホップ非変更の設定方法 （793 ページ）
- BGP ネクスト ホップ非変更の設定例 （795 ページ）
- その他の参考資料 （796 ページ）
- BGP ネクスト ホップ非変更機能の情報 （797 ページ）

機能情報の確認

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

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

ネクスト ホップ非変更に関する情報

BGP ネクスト ホップ非変更

外部 BGP（eBGP）セッションでは、デフォルトで、ルータがルートの送信時に BGP ルートのネクスト ホップ属性を（自身のアドレスに）変更します。BGP ネクスト ホップ非変更機能が設定されている場合、BGP はネクスト ホップ属性を変更せずに eBGP マルチホップ ピアにルートを送信します。ネクスト ホップ属性は変更されません。

（注） ルータがルートを送信するとき、BGP ルートのネクスト ホップ属性を変更するルータのデフォルト動作の例外があります。ネクスト ホップが eBGP ピアのピアリング アドレスと同じサブネットにある場合、ネクスト ホップは変更されません。これは、サード パーティのネクスト ホップと呼ばれます。

BGP ネクスト ホップ非変更機能により、ネットワークの設計および移行を柔軟に実効できます。これは、マルチホップとして設定された eBGP ピア間だけで使用できます。2 つの自律システム間のさまざまなシナリオで使用できます。たとえば、同じ IGP を共有する複数の自律システムが接続される場合、または少なくともルータに互いのネクスト ホップに到達するための別の方法がある（このため、ネクスト ホップを変更しないままにできる）場合などが挙げられます。

この機能の一般的な用途は、RR 間で VPNv4 のマルチホップ MP-eBGP を持つマルチプロトコル ラベル スイッチング（MPLS）Inter-AS を設定することです。

この機能のもう 1 つの一般的な用途は、RFC4364、Section 10 で定義されている VPNv4 Inter-AS オプション C の設定です。この設定では、VPNv4 ルートは、自律システム間で（異なる自律システムの RR 間で）渡されます。RR は複数ホップ離れており、**neighbor next-hop unchanged** が設定されています。異なる自律システムの PE によって、その PE 間に LSP が確立されます（一般的な IGP 経由によって、または ASBR 間のラベル付きルート（1 ホップ離れた異なる自律システムからのルート）経由で PE に接続されたネクスト ホップのアドバタイズによって）。PE は、LSP 経由で別の AS 内の PE のネクスト ホップに到達でき、したがって VRF RIB に VPNv4 ルートをインストールできます。

制約事項

BGP ネクスト ホップ非変更機能は、マルチホップ eBGP ピア間だけで設定できます。直接接続されたネイバーにこの機能を設定しようとすると、次のエラー メッセージが表示されます。

```
%BGP: Can propagate the nexthop only to multi-hop EBGP neighbor
```

BGP ネクスト ホップ非変更の設定方法

eBGP ピアの BGP ネクスト ホップ非変更の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**ipv4** | **ipv6** | **l2vpn** | **nsap** | **rtfilter** | **vpnv4** | **vpnv6**}
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address* **activate**
7. **neighbor** *ip-address* **ebgp-multihop** *ttl*
8. **neighbor** *ip-address* **next-hop-unchanged**
9. **end**
10. **show ip bgp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 65535`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family** {**ipv4** | **ipv6** | **l2vpn** | **nsap** | **rtfilter** | **vpnv4** | **vpnv6**} 例： `Router(config-router-af)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 5	**neighbor** *ip-address* **remote-as** *as-number* 例：	エントリを BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的
	`Router(config-router-af)# neighbor 10.0.0.100 remote-as 65600`	
ステップ 6	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 10.0.0.100 activate`	ピアとの情報交換をイネーブルにします。
ステップ 7	**neighbor** *ip-address* **ebgp-multihop** *ttl* 例： `Router(config-router-af)# neighbor 10.0.0.100 ebgp-multihop 255`	ローカル ルータを設定して、直接接続されていないネットワークに存在する外部ピアとの接続を受け入れて開始するようにします。
ステップ 8	**neighbor** *ip-address* **next-hop-unchanged** 例： `Router(config-router-af)# neighbor 10.0.0.100 next-hop-unchanged`	ネクストホップ属性を変更せずに指定された eBGP ピアに BGP アップデートを送信するようにルータを設定します。
ステップ 9	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp** 例： `Router# show ip bgp`	（任意）BGP ルーティング テーブルのエントリを表示します。 • 出力には、選択されたアドレスについて **neighbor next-hop-unchanged** コマンドが設定されているかどうかが示されます。

ルートマップを使用した BGP ネクスト ホップ非変更の設定

eBGP ネイバーに対する発信ルートマップの設定

ルートマップを定義し、ネイバーに対する発信ポリシーを適用するには、**set ip next-hop unchanged** コマンドを使用します。

次の設定では、プレフィックス 1.1.1.1 のネクストホップは eBGP ネイバー 15.1.1.2 への送信時に変更されません。

```
enable
config terminal
router bgp 2
 bgp log-neighbor-changes
 neighbor 15.1.1.2 remote-as 3
```

```
 neighbor 15.1.1.2 ebgp-multihop 10
 !
 address-family ipv4
  neighbor 15.1.1.2 activate
  neighbor 15.1.1.2 route-map A out
  exit address-family
!
route-map A permit 10
 match ip address 1
 set ip next-hop unchanged
!
access-list 1 permit 1.1.1.1
end
```

eBGP ネイバーへの送信時における iBGP および eBGP パス プレフィックスのネクストホップ非変更の設定

eBGP ネイバーへの送信時に iBGP および eBGP パス プレフィックスのネクストホップを変更しないよう設定するには、**next-hop-unchanged allpaths** コマンドを使用します。

（注） Cisco IOS XE Denali 16.3 リリースから、**next-hop-unchanged allpaths** コマンドは、VPNv4 および VPNv6 アドレス ファミリに加えて、IPv4 および IPv6 アドレス ファミリをサポートするようになりました。

次の設定では、iBGP パス プレフィックスでも eBGP パス プレフィックスでも、ネクストホップは eBGP ネイバー 15.1.1.2 への送信時に変更されません。

```
enable
config terminal
router bgp 2
 bgp log-neighbor-changes
 neighbor 15.1.1.2 remote-as 3
 neighbor 15.1.1.2 ebgp-multihop 10
!
address-family ipv4
 neighbor 15.1.1.2 activate
 neighbor 15.1.1.2 next-hop-unchanged allpaths
 exit address-family
!
end
```

BGP ネクスト ホップ非変更の設定例

例：eBGP ピアの BGP ネクスト ホップ非変更

次に、リモート AS にマルチホップ eBGP ピア 10.0.0.100 を設定する例を示します。ローカル ルータがそのピアにアップデートを送信する場合、ネクスト ホップ属性を変更せずにアップデートを送信します。

```
router bgp 65535
```

```
address-family ipv4
neighbor 10.0.0.100 remote-as 65600
neighbor 10.0.0.100 activate
neighbor 10.0.0.100 ebgp-multihop 255
neighbor 10.0.0.100 next-hop-unchanged
end
```

（注） IPv4、IPv6、VPNv4、VPNv6、L2VPN など、すべてのアドレス ファミリが **next-hop unchanged** コマンドをサポートしています。ただし、アドレス ファミリ L2VPN BGP VPLS シグナリングについては、正常に機能させるためには **next-hop self** コマンドを使用する必要があります。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
iBGP ピアに対する IP ネクスト ホップを設定するルート リフレクタの BGP アウトバウンド ルート マップ	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「内部 BGP 機能の設定」

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 ネクスト ホップ非変更機能の情報

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 *59 : BGP* ネクスト ホップ非変更機能の情報

機能名	リリース	機能情報
BGP ネクスト ホップ非変更	Cisco IOS XE Release 2.1	BGP ネクスト ホップ非変更機能では、ネクスト ホップ属性を変更せずに BGP によって eBGP マルチホップ ピアにアップデートを送信できます。 この機能により、**neighbor next-hop-unchanged** コマンドが追加されました。
set ip next-hop unchanged/next-hop-unchanged allpaths IPv4/IPv6	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3 リリースでは、set ip next-hop unchanged/next-hop-unchanged allpaths IPv4/IPv6 機能により、BGP ネクスト ホップ非変更のサポートが IPv4 および IPv6 の allpaths に拡張されています。 set ip next-hop unchanged/next-hop-unchanged allpaths IPv4/IPv6 機能により、BGP ネクスト ホップ非変更をサポートする 2 つの新しいノブが追加されています。「set ip next-hop unchanged」ノブが route-map に追加され、「next-hop-unchanged allpaths」が neighbor に追加されました。 この機能により、 **set ip next-hop unchanged** コマンドが変更されました。

第 44 章

L2VPN アドレス ファミリに対する BGP サポート

レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）アドレス ファミリに対する BGP サポートでは、L2VPN エンドポイント プロビジョニング情報を配布する BGP をベースとした自動検出メカニズムが導入されています。BGP では、エンドポイント プロビジョニング情報を保存する際に個別の L2VPN ルーティング情報ベース（RIB）が使用されます。これは、レイヤ 2 Virtual Forwarding Instance（VFI）が設定されたときに毎回アップデートされます。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、エンドポイント情報を使用して Pseudowire メッシュがセットアップされます。

- 機能情報の確認 （799 ページ）
- L2VPN アドレス ファミリに対する BGP サポートの前提条件 （800 ページ）
- L2VPN アドレス ファミリに対する BGP サポートの制約事項 （800 ページ）
- L2VPN アドレス ファミリに対する BGP サポートに関する情報 （800 ページ）
- L2VPN アドレス ファミリに対する BGP サポートの設定方法 （802 ページ）
- L2VPN アドレス ファミリに対する BGP サポートの設定例 （809 ページ）
- 次の作業 （812 ページ）
- その他の参考資料 （812 ページ）
- L2VPN アドレス ファミリに対する BGP サポートに関する機能情報 （813 ページ）

機能情報の確認

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

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

L2VPN アドレス ファミリに対する BGP サポートの前提条件

L2VPN アドレス ファミリに対する BGP サポート機能では、バーチャル プライベート ネットワーク（VPN）、バーチャル プライベート LAN サービス（VPLS）、およびマルチプロトコル レイヤ スイッチング（MPLS）テクノロジーに関してあらかじめ知識があることを前提としています。

L2VPN アドレス ファミリに対する BGP サポートの制約事項

- L2VPN アドレス ファミリ コンフィギュレーションで使用された場合、BGP 内で使用されるルートマップでは、プレフィックス処理、タグ処理、および自動タグ処理に関連するすべてのコマンドは無視されます。その他すべてのルート マップ コマンドはサポートされています。
- L2VPN アドレス ファミリでは、BGP マルチパスおよびコンフェデレーションはサポートされていません。

L2VPN アドレス ファミリに対する BGP サポートに関する情報

L2VPN アドレス ファミリ

Cisco IOS XE Release 2.6 以降のリリースでは、L2VPN アドレス ファミリのサポートが導入されています。L2VPN は、IP セキュリティ（IPsec）または総称ルーティング カプセル化（GRE）などの暗号化テクノロジーを使用して、セキュアでないネットワーク内で運用されるセキュアなネットワークと定義されています。L2VPN アドレス ファミリは BGP ルーティング コンフィギュレーション モードで設定され、L2VPN アドレス ファミリ内では VPLS Subsequent Address Family Identifier（SAFI）がサポートされています。

L2VPN アドレス ファミリに対する BGP サポートでは、L2VPN エンドポイント プロビジョニング情報を配布する BGP をベースとしたオートディスカバリ メカニズムが導入されています。BGP では、エンドポイント プロビジョニング情報を保存する際に個別の L2VPN ルーティング

情報ベース（RIB）が使用されます。これは、レイヤ2 VFIが設定されたときに毎回アップデートされます。プレフィックスおよびパス情報はL2VPNデータベースに保存され、ベスト パスがBGPにより決定されるようになります。BGPにより、アップデート メッセージですべてのBGPネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPNベースのサービスをサポートするために、エンドポイント情報を使用してPseudowireメッシュがセットアップされます。

BGPオートディスカバリ メカニズムにより、Cisco IOS Virtual Private LAN Service（VPLS）機能に必要不可欠なL2VPNサービスのセットアップが簡易化されます。VPLSは、高速イーサネットを使用した堅牢でスケーラブルなIP MPLSネットワークによる大規模なLANとして、地理的に分散した拠点間を接続することで柔軟なサービスの展開を実現します。VPLSの詳細については、「VPLS Autodiscovery: BGP Based」機能を参照してください。

L2VPNアドレス ファミリでは、次のBGPコマンドがサポートされています。

- **bgp nexthop**
- **bgp scan-time**
- **neighbor activate**
- **neighbor advertisement-interval**
- **neighbor allowas-in**
- **neighbor capability**
- **neighbor inherit**
- **neighbor maximum-prefix**
- **neighbor next-hop-self**
- **neighbor next-hop-unchanged**
- **neighbor peer-group**
- **neighbor remove-private-as**
- **neighbor route-map**
- **neighbor route-reflector-client**
- **neighbor send-community**
- **neighbor soft-reconfiguration**
- **neighbor soo**
- **neighbor weight**

（注） L2VPNを使用したルート リフレクタでは、**neighbor next-hop-self** コマンドおよび **neighbor next-hop-unchanged** コマンドはサポートされていません。

L2VPN アドレス ファミリ コンフィギュレーションで使用された場合、BGP 内で使用されるルートマップでは、プレフィックス処理、タグ処理、および自動タグ処理に関連するすべてのコマンドは無視されます。その他すべてのルート マップ コマンドはサポートされています。

L2VPN アドレス ファミリでは、BGP マルチパスおよびコンフェデレーションはサポートされていません。

VPLS ID

VPLS ID は、VPLS ドメインを示す BGP 拡張コミュニティ値です。デフォルトの VPLS ID は BGP 自律システム番号および設定済みの VPN ID を使用して生成されるため、この ID の手動設定は任意です。VPLS ID は、自律システム番号と任意番号、または IP アドレスと任意番号のいずれかで構成できます。

VPLS ID は、次のいずれかの形式で入力できます。

- 16 ビット自律システム番号、コロン、32 ビット番号を入力します。次に例を示します。

45000:3

- 32 ビット IP アドレス、コロン、16 ビット番号を入力します。次に例を示します。

192.168.10.15:1

L2VPN アドレス ファミリに対する BGP サポートの設定方法

BGP および L2VPN アドレス ファミリを使用した VPLS オートディスカバリの設定

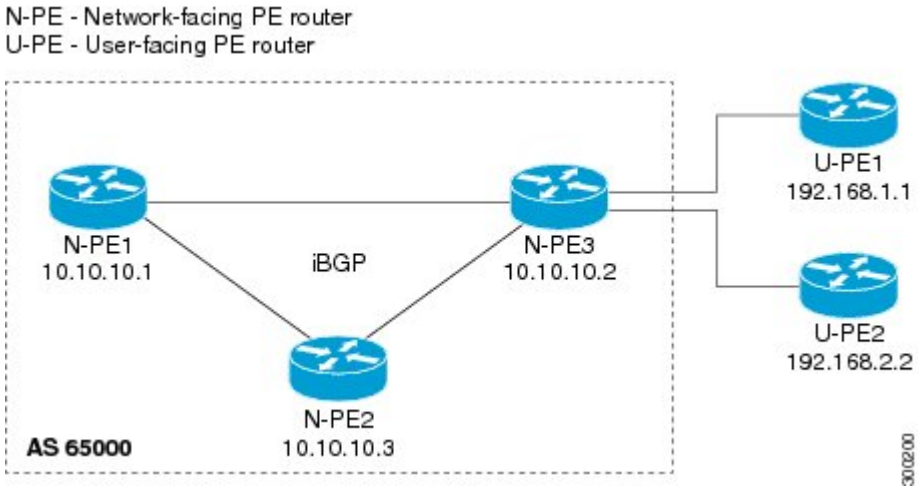
特定の VPLS のメンバーである各プロバイダー エッジ（PE）ルータの VPLS オートディスカバリを実装するには、次の作業を実行します。Cisco IOS XE Release 2.6 では、エンドポイントプロビジョニング情報が含まれている個別の L2VPN RIB で BGP L2VPN アドレス ファミリが導入されました。BGP は、レイヤ 2 仮想転送インスタンス（VFI）が設定されたときに毎回アップデートされる L2VPN データベースからのエンドポイント プロビジョニング情報を学習します。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、エンドポイント情報を使用して Pseudowire メッシュがセットアップされます。

BGP ベースの VPLS オートディスカバリにより、VPLS ネイバーを手動でプロビジョニングする必要がなくなります。PE ルータが自身を特定の VPLS のメンバーとして設定すると、同じ VPLS内のリモートルータへの接続を設定するために必要な情報が、ディスカバリ プロセスによって配布されます。ディスカバリ プロセスが完了したとき、VPLS の各メンバーは、VPLS

に必要な疑似回線のフルメッシュを形成するようVPLS疑似回線を設定するために必要な情報を入手済みです。

この作業は下の図のルータ N-PE3 で設定し、ルータ N-PE1 と N-PE2 に対して、別の IP アドレスを指定するなどの必要な変更を加えて繰り返す必要があります。これらのルータの詳細な設定については、下の図を参照してください。

図 *63 : L2VPN* アドレス ファミリを使用した *BGP* オートディスカバリのネットワーク図



この作業では、レイヤ 2 ルータ ID、VPN ID、VPLS ID を使用して上の図の PE ルータ N-PE3 を設定し、同じ VPLS ドメイン内にある他の PE ルータが自動的に検出されるように設定します。BGP セッションが作成され、L2VPN アドレス ファミリで BGP ネイバーがアクティブになります。最後に、2 つのオプション **show** コマンドを入力して、この作業の手順を検証します。

始める前に

この作業は、MPLS が VPLS オプションを使用して設定されていることを前提にしています。詳細については、「VPLS Autodiscovery: BGP Based」機能を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **l2 router-id** *ip-address*
4. **l2 vfi** *vfi-name* **autodiscovery**
5. **vpn id** *vpn-id*
6. **vpls-id** *vpls-id*
7. **exit**
8. 手順 4 ～ 6 を繰り返して、他の L2 VFI および関連する VPN および VPLS ID を設定します。
9. **router bgp** *autonomous-system-number*
10. **no bgp default ipv4-unicast**
11. **bgp log-neighbor-changes**

12. **bgp update-delay** *seconds*
13. **neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number*
14. **neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number*
15. 他の BGP ネイバーを設定する場合は、手順 13 と 14 を繰り返します。
16. **address-family l2vpn** [**vpls**]
17. **neighbor** *ip-address* **activate**
18. **neighbor** {*ip-address*| *peer-group-name*} **send-community**[**both**| **standard**| **extended**]
19. 手順17と18を繰り返して、L2VPNアドレス ファミリ内の他のBGPネイバーをアクティブにします。
20. **end**
21. **show vfi**
22. **show ip bgp l2vpn vpls** {**all** | **rd** *vpn-rd*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**l2 router-id** *ip-address* 例： `Router(config)# l2 router-id 10.1.1.3`	VPLS オートディスカバリ疑似回線で使用する PE ルータのルータ ID を（IP アドレス形式で）指定します。 • この例では、L2 ルータ ID が 10.1.1.3 として定義されています。
ステップ 4	**l2 vfi** *vfi-name* **autodiscovery** 例： `Router(config)# l2 vfi customerA autodiscovery`	L2 VFI を作成し、VPLS PE ルータが同じ VPLS ドメイン内の他の PE ルータを自動的に検出されるように設定し、L2 VFI オートディスカバリ コンフィギュレーション モードを開始します。 • この例では、customerA という名前の L2 VFI が作成されます。
ステップ 5	**vpn id** *vpn-id* 例： `Router(config-vfi)# vpn id 100`	VPN ID を指定します。 • 同じ VPN に属する PE ルータには同じ VPN ID を使用します。サービス プロバイダー ネットワークの VPN ごとに、VPN ID が一意になるようにします。

	コマンドまたはアクション	目的
		• *vpn-id* 引数を使用して、1 ～ 4294967295 の範囲で数値を指定します。 • この例では、VPN ID 100 が指定されています。
ステップ 6	**vpls-id** *vpls-id* 例： `Router(config-vfi)# vpls-id 65000:100`	（任意）VPLS ID を指定します。 • VPLS ID は、VPLS ドメインを識別するために使用される識別子です。デフォルトの VPLS ID は BGP 自律システム番号および VFI 用に設定済みの VPN ID を使用して自動生成されるため、このコマンドは任意です。各 VFI に 1 つの VPLS ID を設定できます。同じルータ上の複数の VFI で同じ VPLS ID を設定することはできません。 • この例では、VPLS ID 65000:100 が指定されています。
ステップ 7	**exit** 例： `Router(config-vfi)# exit`	L2 VFI オートディスカバリ 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	手順 4 ～ 6 を繰り返して、他の L2 VFI および関連する VPN および VPLS ID を設定します。	--
ステップ 9	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 10	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリを無効にします。 （注） IPv4 ユニキャスト アドレス ファミリのルーティング情報は、**neighbor remote-as** ルータ コンフィギュレーション コマンドで設定された各 BGP ルーティング セッションに対して、デフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に、**no bgp default ipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。

	コマンドまたはアクション	目的
ステップ 11	**bgp log-neighbor-changes** 例： `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバーリセットのロギングを有効にします。
ステップ 12	**bgp update-delay** *seconds* 例： `Router(config-router)# bgp update-delay 1`	BGP 対応ネットワーキング デバイスが最初の更新を送信するまでの初期遅延の最大時間を設定します。 • *seconds* 引数を使用して、遅延時間を設定します。
ステップ 13	**neighbor** {*ip-address*| *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.10.10.1 remote-as 65000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、10.10.10.1 のネイバーは内部 BGP ネイバーです。
ステップ 14	**neighbor** {*ip-address*| *peer-group-name*} **update-source** *interface-type interface-number* 例： `Router(config-router)# neighbor 10.10.10.1 update-source loopback 1`	（任意）ルーティング テーブル アップデートを受信するための特定のソース、またはインターフェイスを選択するようにルータを設定します。 • この例では、ループバック インターフェイスを使用します。このコンフィギュレーションの利点は、ループバック インターフェイスはフラッピング インターフェイスの効果の影響を受けにくいところにあります。
ステップ 15	他の BGP ネイバーを設定する場合は、手順 13 と 14 を繰り返します。	--
ステップ 16	**address-family l2vpn** [**vpls**] 例：	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-router)# address-family l2vpn vpls`	• オプションの **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布されるように指定します。 • この例では、L2VPN VPLS アドレス ファミリ セッションが作成されます。
ステップ 17	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 10.10.10.1 activate`	このネイバーをイネーブルにして、L2VPN VPLS アドレス ファミリの情報をローカル ルータと交換します。 （注） BGP ピア グループをネイバーとして設定した場合は、このステップを使用しません。BGP パラメータが設定されると、BGP ピア グループがアクティブになります。たとえば、次の手順の **neighbor send-community** コマンドでは、ピア グループが自動的にアクティブになります。
ステップ 18	**neighbor** {*ip-address*| *peer-group-name*} **send-community**[**both**| **standard**| **extended**] 例： `Router(config-router-af)# neighbor 10.10.10.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。
ステップ 19	手順 17 と 18 を繰り返して、L2VPN アドレス ファミリ内の他の BGP ネイバーをアクティブにします。	--
ステップ 20	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 21	**show vfi** 例： `Router# show vfi`	（任意）設定した VFI インスタンスに関する情報を表示します。
ステップ 22	**show ip bgp l2vpn vpls** {**all** | **rd** *vpn-rd*} 例： `Router# show ip bgp l2vpn vpls all`	（任意）L2 VPN VPLS アドレス ファミリに関する情報を表示します。

例

次に、CustomerA と CustomerB という 2 つの VFI と、それらに関連付けられた VPN および VPLS ID を表示する **show vfi** コマンドの出力例を示します。

```
Router# show vfi
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: customerA, state: down, type: multipoint
  VPN ID: 100, VPLS-ID: 65000:100
  RD: 65000:100, RT: 65000:100
  Local attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        Discovered Router ID    S
  10.10.10.1         100        10.10.10.99             Y
VFI name: customerB, state: down, type: multipoint
  VPN ID: 200, VPLS-ID: 65000:200
  RD: 65000:200, RT: 65000:200
  Local attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        Discovered Router ID    S
  10.10.10.3         200                10.10.10.98    Y
```

次に、VPN ルート識別子によって識別された 2 つの VFI を表示する **show ip bgp l2vpn vpls all** コマンドの出力例を示します。

```
Router# show ip bgp l2vpn vpls all
BGP table version is 5, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:100
*> 65000:100:10.10.10.1/96
                    0.0.0.0                              32768 ?
*>i65000:100:192.168.1.1/96
                    10.10.10.2               0    100      0 ?
Route Distinguisher: 65000:200
*> 65000:200:10.10.10.3/96
                    0.0.0.0                              32768 ?
*>i65000:200:192.168.2.2/96
                    10.10.10.2               0    100      0 ?
```

次の作業

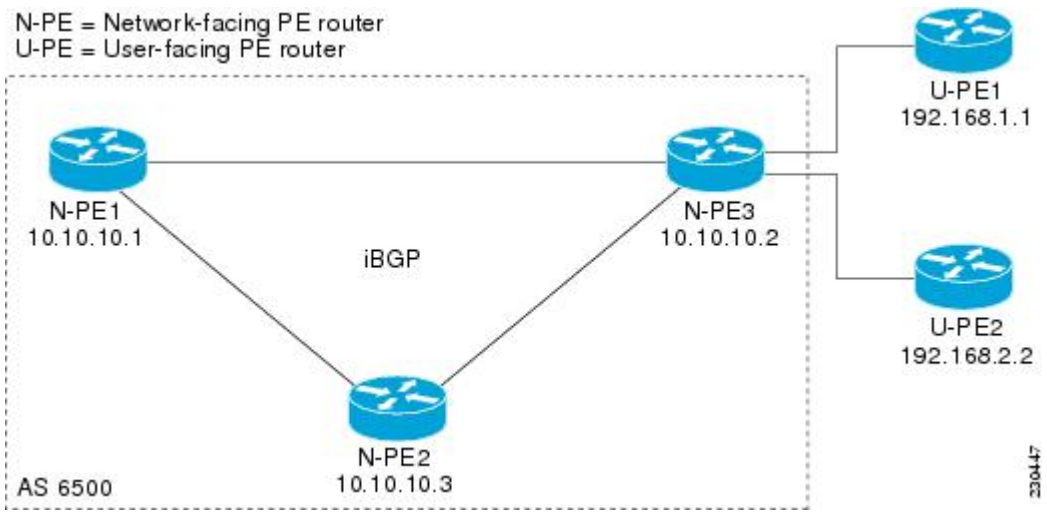
その他の VPLS 機能を設定するには、『*MPLS Layer 2 VPNs Configuration Guide*』の「VPLS Autodiscovery: BGP Based」モジュールを参照してください。

L2VPN アドレス ファミリに対する BGP サポートの設定例

例：BGP および L2VPN アドレス ファミリを使用した VPLS 自動検出の設定

この設定例では、下の図に示す自律システム 65000 のすべてのルータが L2VPN アドレス ファミリの BPG サポートを提供するように設定されています。VPLS オートディスカバリはイネーブルで、L2 VFI および VPN ID が設定されています。VPLS エンドポイント プロビジョニング情報が個別の L2VPN RIB に保存され、BGP 更新メッセージで他の BGP ピアに配布されるように、BGP ネイバーが L2VPN アドレス ファミリで設定およびアクティブ化されます。BGP ピアでエンドポイント情報が受信されると、L2VPN ベースのサービスをサポートするために Pseudowire メッシュが設定されます。

図 *64 : BGP* および *L2VPN* アドレス ファミリを使用した *VPLS* オートディスカバリのネットワーク図



ルータ N-PE1

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 1000 2000
mpls label protocol ldp
l2 router-id 10.1.1.1
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
```

```
 ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0/1
 description Backbone interface
 ip address 10.0.0.1 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 update-source Loopback 1
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 update-source Loopback 1
!
 address-family l2vpn vpls
 neighbor 10.10.10.2 activate
 neighbor 10.10.10.2 send-community extended
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-community extended
 exit-address-family
!
ip classless
```

ルータ N-PE2

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 2000 3000
mpls label protocol ldp
l2 router-id 10.1.1.2
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.2 255.255.255.255
!
interface GigabitEthernet0/0/1
 description Backbone interface
 ip address 10.0.0.2 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
```

```
 neighbor 10.10.10.1 remote-as 65000
 neighbor 10.10.10.1 update-source Loopback1
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 update-source Loopback1
!
 address-family l2vpn vpls
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-community extended
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-community extended
 exit-address-family
!
ip classless
```

ルータ N-PE3

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 2000 3000
mpls label protocol ldp
l2 router-id 10.1.1.3
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.3 255.255.255.255
!
interface GigabitEthernet0/0/1
 description Backbone interface
 ip address 10.0.0.3 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.10.10.1 remote-as 65000
 neighbor 10.10.10.1 update-source Loopback1
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 update-source Loopback1
!
 address-family l2vpn vpls
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-community extended
 neighbor 10.10.10.2 activate
 neighbor 10.10.10.2 send-community extended
 exit-address-family
!
ip classless
```

次の作業

VPLS 自動検出の設定の詳細については、『*MPLS Layer 2 VPNs Configuration Guide*』の「VPLS Autodiscovery: BGP Based」モジュールを参照してください。

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

MIB

MIB	MIB のリンク
—	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

L2VPN アドレス ファミリに対する BGP サポー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。

表 *60 : L2VPN* アドレス ファミリに対する *BGP* サポートに関する機能情報

機能名	リリース	機能情報
L2VPN アドレス ファミリに対する BGP サポート	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.3SG	L2VPN アドレス ファミリに対する BGP サポートでは、L2VPN エンドポイント プロビジョニング情報を配布する BGP をベースとしたオートディスカバリ メカニズムが導入されています。BGP では、エンドポイント プロビジョニング情報を保存する際に個別の L2VPN ルーティング情報ベース（RIB）が使用されます。これは、レイヤ 2 VFI が設定されたときに毎回アップデートされます。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、エンドポイント情報を使用して Pseudowire メッシュがセットアップされます。 この機能により、次のコマンドが導入または変更されました。**address-family l2vpn**、**clear ip bgp l2vpn**、**show ip bgp l2vpn**

第 45 章

BGP イベントベース VPN インポート

BGPイベントベースVPNインポート機能は、既存のボーダーゲートウェイプロトコル（BGP）パスのインポートプロセスに変更を加えるものです。拡張BGPパスインポートはイベントの発生時に実行されます。BGPパスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。ソフトウェアがアップデート処理前に定期的なスキャナ時間まで待つことに起因するルートの伝播の遅延もなくなるため、コンバージェンス時間が大幅に短縮されます。新しい処理の実装用に、新たなコマンドラインインターフェイス（CLI）が導入されています。

- 機能情報の確認 （815 ページ）
- BGP イベントベース VPN インポートの前提条件 （816 ページ）
- BGP イベントベース VPN インポートの概要 （816 ページ）
- BGP イベントベース VPN インポートの設定方法 （817 ページ）
- BGP イベントベース VPN インポートの設定例 （824 ページ）
- その他の参考資料 （824 ページ）
- BGP イベントベース VPN インポートの機能情報 （826 ページ）

機能情報の確認

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

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

BGP イベントベース VPN インポートの前提条件

関係するルータすべてで、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングが有効になっている必要があります。

BGP イベントベース VPN インポートの概要

BGP イベントベース VPN インポート

BGP イベントベース VPN インポート機能は、既存の BGP パスのインポート プロセスに変更を加えるものです。BGP バーチャル プライベート ネットワーク（VPN）インポートは、BGP パスが BGP VPN テーブルから BGP VPN ルーティング/転送（VRF）トポロジへインポートされる場合に、インポート機能を提供するものです。既存のパス インポート プロセスでは、パスにアップデートが発生すると、次のスキャン時間の間にインポートアップデート処理が行われ、スキャンの間隔は 5 ～ 15 秒の間で設定されています。スキャン時間のために、ルートの伝播に遅延が発生します。拡張BGPパスインポートはイベントの発生時に実行されます。BGP パスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。

BGPイベントベースVPNインポート機能を使用すると、プロバイダーエッジ（PE）ルータはVPNパスをカスタマーエッジ（CE）ルータへとスキャン時間の遅延なしに伝播できるため、コンバージェンス時間は大幅に短縮されます。インポートされたルート ターゲットを VRF に追加するといった設定変更は即時処理されず、これまでどおり 60 秒ごとの定期的なスキャナ通過の間に処理されます。

インポート パス選択ポリシー

イベントベース VPN インポートには、3 種類のパス選択ポリシーが準備されています。

- すべて：インポートする VRF インスタンスに関連付けられたルート ターゲット（RT）のいずれかに一致するエクスポート側ネットから、使用できるパスすべてをインポートします。
- ベスト パス：VRF インスタンスの RT に一致する、最適使用可能パスをインポートします。エクスポート側ネット内のベストパスがVRFインスタンスのRTに一致しない場合、VRF インスタンスの RT に一致する、最適使用可能パスがインポートされます。
- マルチパス：VRFインスタンスのRTに一致する、ベストパスおよびマルチパスとマークされたすべてのパスをインポートします。一致するベストパスやマルチパスがない場合、最適使用可能パスが選択されます。

マルチパスおよびベスト パス オプションは、設定されたオプションでのみ選択されるよう、オプションのキーワードを使用して制限することができます。**import path selection** コマンドで **strict** キーワードを設定すると、最適使用可能パス選択のフォールバック安全性オプション

がソフトウェアにより無効になります。エクスポート側ネットにVRFインスタンスのRTに一致する設定されたオプション（ベストパスまたはマルチパス）に適したパスがない場合、どのパスもインポートされません。この動作は、BGP イベントベース VPN インポート機能導入前の動作と一致しています。

制限が設定されない場合、最適使用可能パスとしてインポートされるパスはタグ付きになります。**show** コマンド出力では、これらのパスが「imported safety path」という言い方で識別されます。

VRFインスタンスへインポートされると見なされるエクスポート側ネットの既存のパスは、別のピア ルータから受信したものであるために VPN インポートのルールが適用されていない場合があります。ルート識別子（RD）情報はルータに対してローカルなため、これらのパスには同一の RD 情報が含まれていることがあります。しかし、これらのパスの一部は、インポートする VRF インスタンスの RT と一致しないため、**show** コマンドの出力では「not-in-vrf」とマークされます。VRF にないパスは VRF にあるパスよりも優先度が低く見えるため、「not-in-vrf」とマークされたどのパスも、ベスト パスと見なされることはありません。

インポート パスの制限

メモリ利用を制御するため、エクスポート側ネットからインポートされるパスの最大数の制限をインポート側ネットごとに指定できます。インポートされるパスが1つ以上のエクスポート側ネットから選択される場合、最も優先的に選択されるのはベストパス、次に優先的に選択されるのがマルチパスとなり、非マルチパスの優先度が最も低くなります。

BGP イベントベース VPN インポートの設定方法

マルチプロトコル VRF の設定

マルチプロトコル VRF を使用して、ルート ターゲット ポリシー（インポートおよびエクスポート）を IPv4 と IPv6 との間で共有したり、IPv4 VPN と IPv6 VPN に別々のルート ターゲットポリシーを設定したりすることができます。使用するよう設定するには、この作業を実行します。この作業では、IPv4 アドレス ファミリだけを設定しますが、新しい VRF 設定すべてにマルチプロトコル VRF を使用することを推奨します。

（注） この作業は、BGP イベントベース VPN インポート機能特有のものではありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*

6. **address-family ipv4** [**unicast**]
7. **exit-address-family**
8. **exit**
9. **interface** *type number*
10. **vrf forwarding** *vrf-name*
11. **ip address** *ip-address mask*
12. **no shutdown**
13. **exit**
14. 他の VRF インスタンスをインターフェイスにバインドするには、手順 3 ～ 13 を繰り返します。
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf definition** *vrf-name* 例： `Router(config)# vrf definition vrf-A`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • VRF に割り当てる名前を指定するには、*vrf-name* 引数を使用します。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 45000:1`	ルーティング テーブル、およびフォワーディング テーブルを作成し、VPN 用のデフォルト ルート識別子を指定します。 • 一意の VPN IPv4 プレフィックスを作成するために、IPv4 プレフィックスに 8 バイト値を追加するには、*route-distinguisher* 引数を使用します。
ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target both 45000:100`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • ターゲット VPN 拡張コミュニティからルーティング情報をインポートするには、**import** キーワードを使用します。

	コマンドまたはアクション	目的
		• ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするには、**export** キーワードを使用します。 • ターゲットVPN拡張コミュニティからルーティング情報をインポートするとともに、ルーティング情報を拡張コミュニティにエクスポートするには、**both** キーワードを使用します。 • ルートターゲット拡張コミュニティ属性をVRFのインポート、エクスポート、または両方（インポートとエクスポート）のルート ターゲット拡張コミュニティ リストに追加するには、*route-target-ext-community* 引数を使用します。
ステップ 6	**address-family ipv4** [**unicast**] 例： `Router(config-vrf)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、VRF アドレス ファミリ コンフィギュレーション モードを開始します。 • ここでは、この前のステップで定義されたVRFにアドレス ファミリを指定するために、このステップが必要になります。
ステップ 7	**exit-address-family** 例： `Router(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRFコンフィギュレーションモードに戻ります。
ステップ 8	**exit** 例： `Router(config-vrf)# exit`	VRF 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 モードを開始します。
ステップ 9	**interface** *type number* 例： `Router(config)# interface FastEthernet 1/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**vrf forwarding** *vrf-name* 例： `Router(config-if)# vrf forwarding vrf-A`	VRFインスタンスを手順9で設定したインターフェイスと関連付けます。 • インターフェイスが VRF にバインドされている場合、それ以前に設定されていた IP アドレスは削除され、インターフェイスはディセーブルにされます。

	コマンドまたはアクション	目的
ステップ 11	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.4.8.149 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 12	**no shutdown** 例： `Router(config-if)# no shutdown`	ディセーブルにされたインターフェイスを再起動します。
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、グローバルコンフィギュレーションモードに入ります。
ステップ 14	他の VRF インスタンスをインターフェイスにバインドするには、手順 3 ～ 13 を繰り返します。	--
ステップ 15	**end** 例： `Router(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。

BGP パスへのイベントベース VPN インポート処理の設定

次の作業を行って、BGP パスを VRF テーブルへインポートするためイベントベース処理設定で BGP パスを変更する場合のコンバージェンス時間を短くします。2 つの新しい CLI コマンドにより、インポート側ネットごとのインポートパスの上限値の設定と、パス選択ポリシーの設定が可能になっています。

始める前に

この作業は、VRF が VRF アドレス ファミリ構文で使用されるようすでに設定されているものとしています。VRF を設定するには、このモジュールで前述した「マルチプロトコル VRF の設定」の項を参照して下さい。

BGP ネイバーの設定も完了しているものとします。設定例については、このモジュールの「例：BGP パスへのイベントベース VPN インポート処理の設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*

5. **import path selection** {**all** | **bestpath** [**strict**] | **multipath** [**strict**]}
6. **import path limit** *number-of-import-paths*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4 vrf** *vrf-name* 例： `Router(config-router)# address-family ipv4 vrf vrf-A`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**import path selection** {**all**	**bestpath** [**strict**]	**multipath** [**strict**]} 例： `Router(config-router-af)# import path selection all`	VRF テーブルにルートをインポートする BGP パスの選択ポリシーを指定します。 • この例では、VRF インスタンスの RT に一致するすべてのパスがインポートされます。
ステップ 6	**import path limit** *number-of-import-paths* 例： `Router(config-router-af)# import path limit 3`	エクスポート側ネットからインポート可能な BGP パスの最大数をインポート側ネットごとに指定します。
ステップ 7	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP イベントベース VPN インポート処理のモニタリングとトラブルシューティング

必要に応じて BGP イベントベース VPN インポート処理のモニタリングとトラブルシューティングを行うには、この作業の手順を実行します。

この作業で使用する **show** コマンドについて、ここではコマンド構文の一部だけが表示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*network-address* [*mask*]]
3. **show ip route** [**vrf** *vrf-name*] [*ip-address* [*mask*]]
4. **debug ip bgp vpnv4 unicast import** {**events** | **updates** [*access-list*]}

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [network-address [mask]]

この出力例では、**strict** キーワードが **import path selection** コマンドを使用して設定されていないため、安全インポートパス選択ポリシーが有効になっています。あるパスが最適使用可能パスとしてインポートされる場合（インポートの際にベストパスやマルチパスが不適切である場合）、出力にあるように「imported safety path」とマークされます。

例：

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

VRF インスタンスへインポートされると見なされるエクスポート側ネットの既存のパスは、別のピアルータから受信したものであるために VPN インポートのルールが適用されていない場合があります。ルート識別子（RD）情報はルータに対してローカルなため、これらのパスには同一の RD 情報が含まれていること

があります。しかし、これらのパスの一部は、インポートする VRF インスタンスの RT と一致しないため、**show** コマンドの出力では「not-in-vrf」とマークされます。

次の出力例では、パスは別のピア ルータから受信したもので、VPN インポート規則が適用されていません。この 10.0.101.2 というパスは、VPNv4 テーブルに追加され、vrf-A ネットに関連付けられています。元のルータからの RD 情報とはいえ、RD 情報との一致を含んでいるからです。しかし、このパスは vrf-A に RT 一致ではないため、「not-in-vrf」とマークされています。vrf-A のネットでは、このパスはベスト パスとはならないことに注意してください。VRF にないどのパスも、VRF にあるパスより適したパスとは見られないからです。

例：

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
       mpls labels in/out nolabel/16
```

ステップ 3 **show ip route** [**vrf** *vrf-name*] [*ip-address* [*mask*]]

この出力例には、VRF vrf-A のルーティング テーブルについての情報が表示されています。

例：

```
Router# show ip route vrf vrf-A 172.17.0.0

Routing Table: vrf-A
Routing entry for 172.17.0.0/16
  Known via "bgp 1", distance 200, metric 50
  Tag 2, type internal
  Last update from 10.0.101.33 00:00:32 ago
  Routing Descriptor Blocks:
  * 10.0.101.33 (default), from 10.0.101.33, 00:00:32 ago
      Route metric is 50, traffic share count is 1
      AS Hops 1
      Route tag 2
      MPLS label: 16
      MPLS Flags: MPLS Required
```

ステップ 4 **debug ip bgp vpnv4 unicast import** {**events** | **updates** [*access-list*]}

BGP パスの VRF インスタンス テーブルへのインポートに関連したデバッグ情報を表示するには、このコマンドを使用します。実際の出力は、続けて入力されるコマンドによって変化します。

（注） updates キーワード使用時にフィルタ プレフィックスへのアクセス リストを指定しない場合、全プレフィックスに対するアップデートすべてが表示されることになり、ネットワークの速度低下が発生することがあります。

例：

```
Router# debug ip bgp vpnv4 unicast import events

BGP import events debugging is on
```

BGP イベントベース VPN インポートの設定例

例：BGP パスへのイベントベース VPN インポート処理の設定

この例では、VRF（vrf-A）が設定され、ファスト イーサネット インターフェイス 1/1 に VRF 転送が適用されます。アドレス ファミリ モードでは、インポート パス選択が「すべて」に、インポート パス数は「3」に設定されています。IPv4 アドレス ファミリのもとで 2 つの BGP ネイバーが設定され、VPNv4 アドレス ファミリのもとでアクティブにされています。

```
vrf definition vrf-A
 rd 45000:1
 route-target import 45000:100
 address-family ipv4
  exit-address-family
!
interface FastEthernet1/1
 no ip address
 vrf forwarding vrf-A
 ip address 10.4.8.149 255.255.255.0
 no shut
 exit
!
router bgp 45000
 network 172.17.1.0 mask 255.255.255.0
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 address-family ipv4 vrf vrf-A
  import path selection all
  import path limit 3
  exit-address-family
 address-family vpnv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  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』

関連項目	マニュアル タイトル
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準

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

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS 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

RFC

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

テクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 イベントベース VPN インポートの機能情報

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 *61 : BGP* イベントベース *VPN* インポートの機能情報

機能名	リリース	機能情報
BGP イベントベース VPN インポート	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.3SG	BGP イベントベース VPN インポート機能は、既存のボーダーゲートウェイ プロトコル（BGP）パスのインポート プロセスに変更を加えるものです。拡張 BGP パス インポートはイベントの発生時に実行されます。BGP パスが変更されると、インポートされたコピーすべてのアップデートも、処理が可能になるとすぐに実行されます。ソフトウェアがアップデート処理前に定期的なスキャナ時間まで待つことに起因するルートの伝播の遅延もなくなるため、コンバージェンス時間が大幅に短縮されます。新しい処理の実装用に、新たなコマンドライン インターフェイス（CLI）が導入されています。 次のコマンドが導入または変更されました。 • **bgp scan-time** • **import path limit** • **import path selection** • **maximum-path ebgp** • **maximum-path ibgp** • **show ip bgp vpnv4** • **show ip bgp vpnv6**

第 46 章

BGP 最良外部

BGP最良外部機能を使用すると、ネットワークにバックアップ外部ルートを用意でき、プライマリ外部ルートの接続が失われるのを回避できます。BGP最良外部機能は、外部ネイバーから受信したルートのうち最も優先するルートを、バックアップ ルートとしてアドバタイズします。この機能は、アクティブバックアップ トポロジで便利です。アクティブバックアップ トポロジでは、サービス プロバイダーはルーティング ポリシーを使用し、そのルーティング ポリシーにより、境界ルータは、内部ボーダー ゲートウェイ プロトコル（iBGP）セッションを通じて受信するパス（別の境界ルータのパス）を、プレフィックスのベストパスとして選択します。これは、ルータが外部ボーダー ゲートウェイ プロトコル（eBGP）学習パスを保持する場合も同じです。このアクティブバックアップ トポロジでは、自律システムのプレフィックスに対し1つの終了または出力ポイントが定義され、プライマリ リンクまたはeBGP ピアリングが使用不可になった場合のバックアップとして他のポイントが使用されます。ポリシーにより、境界ルータは、eBGP セッションを通じて学習したパスを、自律システムから隠します。これは、そういったプレフィックスのパスをアドバタイズしないためです。この状況に対処するために、一部のデバイスは、ベスト外部パスと呼ばれる1つの外部学習パスをアドバタイズします。

- 機能情報の確認 （827 ページ）
- BGP 最良外部の前提条件 （828 ページ）
- BGP 最良外部の制約事項 （828 ページ）
- BGP 最良外部に関する情報 （829 ページ）
- BGP 最良外部の設定方法 （833 ページ）
- BGP 最良外部の設定例 （842 ページ）
- その他の参考資料 （843 ページ）
- BGP 最良外部の機能情報 （845 ページ）

機能情報の確認

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

リースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

BGP 最良外部の前提条件

- リンク障害を迅速に検出するために、双方向フォワーディング検出（BFD）プロトコルをイネーブルにする必要があります。
- BGP およびマルチプロトコル ラベル スイッチング（MPLS）ネットワークが稼働していて、複数のパス（マルチホーム）によりプロバイダーサイトと接続されているカスタマーサイトで実行されている必要があります。
- バックアップ パスには、ベスト パスのネクスト ホップと異なる固有のネクスト ホップがある必要があります。
- BGP では、動作するパス間のロスレス スイッチオーバーをサポートする必要があります。

BGP 最良外部の制約事項

- BGP マルチパスがインストールされており、BGP テーブル内にマルチパスが存在する場合、BGP 最良外部機能では、バックアップ パスはインストールされません。マルチパスのいずれかが、自動的に他のパスのバックアップとして機能します。
- 次の機能では、BGP 最良外部機能はサポートされていません。
  - MPLS VPN Carrier Supporting Carrier
  - MPLS VPN 相互自律システム、オプション B
  - Virtual Routing and Forwarding（VRF）ラベル単位での MPLS VPN
- BGP 最良外部機能は、マルチキャストまたは L2VPN VRF アドレス ファミリでは設定できません。
- Cisco IOS XE Release 3.4S 以降を実行している場合を除き、BGP 最良外部機能をルート リフレクタで設定することはできません。
- BGP 最良外部機能は NSF/SSO をサポートしていません。ただし、両方のルート プロセッサで BGP 最良外部機能が設定されている場合は、ISSU がサポートされます。
- BGP 最良外部機能は、VPNv4、VPNv6、IPv4 VRF、IPv6 VRF アドレス ファミリでのみ設定できます。

- **bgp advertise-best-external** コマンドを使用して BGP 最良外部機能を設定する場合は、**bgp additional-paths install** コマンドで BGP PIC 機能を有効にする必要はありません。BGP PIC 機能は、BGP 最良外部機能によって自動的に有効化されます。
- BGP 最良外部機能を設定すると、「MPLS VPN--BGP ローカル コンバージェンス」の機能がオーバーライドされます。ただし、設定から **protection local-prefixes** コマンドを削除する必要はありません。

BGP 最良外部に関する情報

BGP 最良外部の概要

サービスプロバイダーはルーティングポリシーを使用し、そのルーティングポリシーにより、境界ルータは、iBGP セッションを通じて受信するパス（別の境界ルータのパス）を、プレフィックスのベストパスとして選択します。これは、ルータが eBGP 学習パスを保持する場合も同じです。この手法は一般にアクティブバックアップ トポロジと呼ばれており、自律システムのプレフィックスに対し 1 つの終了または出力ポイントを定義すること、およびプライマリリンクまたは eBGP ピアリングが使用不可になった場合のバックアップとして他のポイントを使用することを目的としています。

ポリシーには利点もありますが、ポリシーにより、境界ルータは、eBGP セッションを通じて学習したパスを、自律システムから隠します。これは、そういったプレフィックスのパスをアドバタイズしないためです。この状況に対処するために、一部のルータは、ベスト外部パスと呼ばれる 1 つの外部学習パスをアドバタイズします。最良外部の動作により、次のように、BGP 選択プロセスではすべての宛先に対して 2 つのパスが選択されます。

- その宛先への既知ルートの完全セットからベスト パスが選択されます。
- その外部ピアから受信したルートのセットからベスト外部パスが選択されます。

BGP は外部ピアにベスト パスをアドバタイズします。BGP では、iBGP パスをベスト パスとして選択した場合に内部ピアからベストパスを取り消すのではなく、ベスト外部パスを内部ピアにアドバタイズします。

BGP 最良外部機能は、インターネット アクセスと MPLS VPN シナリオのプレフィックス独立コンバージェンス（PIC）エッジの必須コンポーネントであり、代替パスをアクティブバックアップ トポロジのネットワークで利用可能にします。

ベスト外部ルートとは

BGP 最良外部機能では、「ベスト外部ルート」をバックアップ パスとして使用します。これは、draft-marques-idr-best-external に基づく、外部ネイバーから受信したルートのうち最も優先されるルートです。外部ネイバーからの最優先ルートとして以下が有効です。

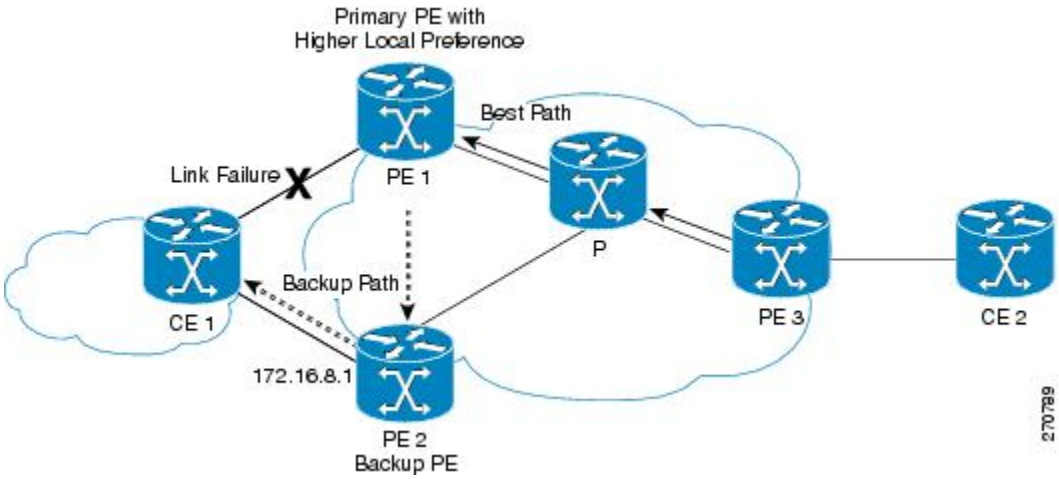
- 内部ボーダー ゲートウェイ プロトコル（iBGP）セッションを相互間で使用する、異なるクラスタ内の 2 つのルータ。
- 外部ボーダー ゲートウェイ プロトコル（eBGP）セッションを相互間で使用する、コンフェデレーションの異なる自律システム内の 2 つのルータ。

ベスト外部ルートは、ルーティング情報ベース（RIB）にインストールされているベストルートとは異なる場合があります。ベスト ルートが内部ルートの場合もあります。ベスト ルートに加えて、ベスト外部ルートをアドバタイズおよび保存できるようにすることで、プライマリ パスに障害が発生した場合でも、使用可能な追加のパスが用意されているため、ネットワークの接続をより迅速に復元できます。

BGP 最良外部機能の仕組み

BGP 最良外部機能は、Internet Engineering Task Force（IETF）の draft-marques-idr-best-external.txt に基づいています。BGP 最良外部機能は、ベスト外部ルートをバックアップ ルートとして内部ピアにアドバタイズします。バックアップ ルートは RIB および Cisco Express Forwarding に保存されます。プライマリ パスに障害が発生した場合でも、BGP PIC 機能により、ベスト外部パスを代わりに使用できるため、接続をより迅速に復元できます。

図 *65 : MPLS VPN*：*MPLS VPN* エッジの最良外部



上の図は、BGP 最良外部機能を使用した MPLS VPN を示しています。このネットワークは、以下のコンポーネントで構成されています。

- プロバイダー エッジ（PE）ルータとカスタマー エッジ（CE）ルータの間に eBGP セッションが存在します。
- PE1 はプライマリ ルータで、ローカル プリファレンス設定がより高くなっています。
- CE2 からのトラフィックでは、PE1 を使用してルータ CE1 に到達します。
- PE1 には、CE1 に到達するためのパスが 2 つあります。
- CE1 は PE1 および PE2 とデュアルホーム接続されています。

• PE1 はプライマリ パスで、PE2 はバックアップ パスです。

上の図では、MPLS クラウドのトラフィックは PE1 を通過して CE1 に到達します。したがって、PE2 は、PE1 をベスト パスとして、PE2 をバックアップ パスとして使用します。

PE1 および PE2 は BGP 最良外部機能を使用して設定されています。BGP は、ベスト パス（PE1-CE1 リンク）とバックアップ パス（PE2）を計算し、両方のパスを RIB および Cisco Express Forwarding にインストールします。ベストパスに加えて、ベスト外部パス（PE2）もピア ルータにアドバタイズされます。

Cisco Express Forwarding は PE1-CE1 リンクでリンク障害を検出すると、ただちにバックアップ パス PE2 に切り替えます。トラフィックは、バックアップ パスを使用して、Cisco Express Forwarding でのローカル高速コンバージェンスによって迅速に再ルーティングされます。これにより、トラフィックの損失は最小限に抑えられ、迅速なコンバージェンスが行われます。

BGP 最良外部を有効にするためのコンフィギュレーション モード

BGP最良外部機能はさまざまなモードで有効にすることができ、各モードはそれぞれ独自の方法で Virtual Routing and Forwarding（VRF）を保護します。

- VPNv4 アドレス ファミリ コンフィギュレーション モードで **bgp advertise-best-external** コマンドを発行すると、すべての IPv4 VRF に適用されます。このモードでコマンドを発行する場合は、特定の VRF に対して発行する必要はありません。
- IPv4 アドレス ファミリ コンフィギュレーション モードで **bgp advertise-best-external** コマンドを発行すると、その VRF にのみ適用されます。

クラスタ間の RR での BGP ベスト外部パス

Cisco IOS XE Release 3.4S から、BGP 最良外部は、クラスタ間の RR での BGP 最良外部に拡張されています。この機能は、非クライアント iBGP ピアに対する最良外部機能を提供して、RR クラスタ間におけるパスの多様性を実現します。この機能は、「クラスタ間ベスト外部パス」とも呼ばれます。

RR でのベスト外部パスとは、RR のクラスタ内のベスト パスを意味します。このパスは、ベスト内部パスと呼ばれる場合もあります。

ある RR（RR1）が非クライアント iBGP パス（つまり、別の RR（たとえば、RR2）から学習したパス）を全体でのベスト パスとして選択する場合、クラスタ間の RR での BGP 最良外部機能を使用すると、RR1 はそのベスト内部パスを非クライアント iBGP ピアにアドバタイズできるようになります。これにより、RR2 は追加のパスを学習して、ダイバース パスを提供できます。

RR での最良外部機能は、非クライアント iBGP ピアのみを対象とします。RR は、全体としてのベストパス（クライアントパスである場合も非クライアント eBGP パスである場合もある）をアドバタイズする必要があるため、ベスト外部パスをクライアントにアドバタイズすることはできません。

RR によって計算されるベスト外部パスは、クラスタのベスト内部パスです。このパスは、この RR での全体としてのベスト パスが非クライアント iBGP パスである場合にのみ非クライアント iBGP ピアにアドバタイズされます。

複数の RR が存在し、それぞれ独自のクラスタに含まれている場合、各 RR では、ネイバー RR ごとに **neighbor advertise best-external** コマンドを設定する必要があります。

RR がフォワーディング プレーンにある場合は、**bgp additional paths install** コマンドが必要です。

クラスタ間の RR でのベスト外部パスに関する CLI の違い

Cisco IOS XE Release 3.4S までは、BGP 最良外部機能は PE でのみ使用可能であり、 **bgp advertise-best-external** コマンドで設定していました。バックアップ パスの計算、インストール、およびアドバタイズは、1 つのコマンドにまとめられていました。

Cisco IOS XE Release 3.4S からは、PE および RR で BGP 最良外部機能を使用できます。**bgp advertise-best-external** コマンドの機能は、それぞれベスト外部パスを計算、インストール、およびアドバタイズする次の 3 つのコマンドに分けられています。

- **bgp additional-path select best-external**
- **bgp additional-path install**
- **neighbor advertise diverse-path best-external**

bgp additional-path select best-external コマンドが設定されていない場合は、ベスト外部パスが計算されてインストールされますが、アドバタイズは行われません。

neighbor advertise diverse-path best-external コマンドは、指定したネイバーにベスト外部パスをアドバタイズできるようにします。

クラスタ間の RR での BGP ベスト外部パスの計算に使用されるルール

非クライアント（別のクラスタの RR）に対する RR でのベスト内部パスの実装は、次のルールに基づいて計算されます。

1. 通常のベストパス選択ルールに従って、RR での全体としてのプライマリ ベストパスを計算します。
2. バックアップ パス設定が有効になっている場合は、2 番目のベストパス（ルール 1 で選択されたプライマリ ベストパスとは異なるパスで、このベストパスとは異なるネクストホップを持つパス）を計算し、バックアップ パスとしてマークします。バックアップ パス選択は、**bgp additional-paths install** または **bgp additional-paths select [best-external] [backup]** コマンドを使用して有効にします。
3. RR での全体としてのベスト パスが非クライアント iBGP パスであり、eBGP パスでない場合は、ルール 1 およびルール 2 による結果を除外した後、他のクラスタから得た他のパスをすべて無視して、残りのパスからベスト外部/内部パスを計算し、残りの eBGP パスおよ

び iBGP パスをすべて含めて通常のベストパス ルールを実行します。新たに得られたベストパスを選択し、ベスト内部パスとしてマークします。

4. このベスト内部パスをアドバタイズします。これは、**neighbor advertise best-external** が非クライアント RR に対して設定されている場合、非クライアント RR に対する eBGP パス（RR/ASBR の CE ピアから受信）または iBGP パス（RR クライアントから受信）になります。

5. 全体としてのベストパスが RR クライアントまたは eBGP ピア（RR/ASBR の場合）から受信されたパスである場合は、iBGP パスまたは eBGP パスが通常のベストパス アルゴリズムに従ってベストパスとして選択されます。全体としてのベストパスは内部クライアントパスであるため、通常のアドバタイズメントルールによって自動的にこのパスが非クライアント iBGP ピア/RR にアドバタイズされます。この動作は、RR クライアントのパスが全体としてのベストパスとして選択される場合、既存の動作と同じになります（RR で最良外部が有効になっていない場合）。

6. RR クライアントに対する RR でベスト外部パスを設定することはできません。**neighbor advertise best-external** コマンドは、非クライアントに対する、または他のクラスタ内の RR とピアリングする RR/ASBR のみで設定できます。

7. RR でマルチパスが有効になっている場合に、全体としてのベストパスが非クライアントからのパスであり、クラスタ内クライアントパスも一部がマルチパスとしてマークされているときに限り、RR で最良外部を有効化すると（RR 非クライアントに対する **neighbor advertise best-external**）、アルゴリズムでは、クラスタ内クライアントのマルチパス（クラスタ内の RR クライアントおよび eBGP ピアから取得されたパス）のうち、より古いマルチパスを選択し、ベスト内部パスとしてマークし、ベスト外部パスとして非クライアントに通知します。これにより、非クライアントに対してこのクラスタからパスの多様性が提供されます。クラスタ内のマルチパスが見つからない場合は、ルール 3 ～ 5 に従ってベスト外部パスが選択されます。

BGP 最良外部の設定方法

BGP 最良外部機能の設定

BGP 最良外部機能を設定するには、次の作業を実行します。この作業では、IPv4 または VPNv4 アドレス ファミリで BGP 最良外部機能を設定する方法を示します。VPNv4 アドレス ファミリ コンフィギュレーション モードでは、すべての IPv4 Virtural Routing Forwarding（VRF）に BGP 最良外部機能が適用されます。特定の VRF に対して設定する必要はありません。IPv4 VRF アドレス ファミリ コンフィギュレーション モードで **bgp advertise-best-external** コマンドを発行した場合は、その VRF にのみ BGP 最良外部機能が適用されます。

始める前に

- BGP 最良外部機能を設定する前に、MPLS VPN を設定し、正常に動作していることを確認します。詳細については、「Configuring MPLS Layer 3 VPNs」の項を参照してください。

- マルチプロトコル VRF を設定して、ルート ターゲット ポリシー（インポートおよびエクスポート）を IPv4 と IPv6 との間で共有したり、IPv4 VPN と IPv6 VPN に別々のルート ターゲット ポリシーを設定したりすることができるようにします。マルチプロトコル VRF の設定については、「MPLS VPN--VRF CLI for IPv4 and IPv6 VPNs」の項を参照してください。
- カスタマー エッジ（CE）ルータが少なくとも 2 つのパスによってネットワークに接続されていることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. 次のいずれかを実行します。
   - **address-family ipv4** [**unicast** | **vrf** *vrf-name*]
   - または
   - **address-family vpnv4** [**unicast**]
   - または
5. **bgp advertise-best-external**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **activate**
8. **neighbor** *ip-address* **fall-over** [**bfd** | **route-map** *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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **address-family ipv4** [**unicast** | **vrf** *vrf-name*]
	• または
	• **address-family vpnv4** [**unicast**]
	• または
	例：
	`Router(config-router)# address-family ipv4 unicast`
	例：
	`Router(config-router)# address-family vpnv4`
		IPv4 または VPNv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
		• **unicast** キーワードは、IPv4 または VPNv4 ユニキャスト アドレス ファミリを指定します。
		• **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

ステップ 5	**bgp advertise-best-external** 例： `Router(config-router-af)# bgp advertise-best-external`	外部バックアップ パスを計算および使用し、RIB および Cisco Express Forwarding にインストールします。
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィックスだけを交換します。その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 192.168.1.1 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。
ステップ 8	**neighbor** *ip-address* **fall-over** [**bfd** | **route-map** *map-name*] 例： `Router(config-router-af)# neighbor 192.168.1.1 fall-over bfd`	高速セッションの非アクティブ化を使用するように BGP ピアリングを設定し、フェールオーバーでの BFD プロトコル サポートを有効にします。 • BGP は、セッションが無効になると、このピアで学習したすべてのルートを削除します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-router-af)# end`	（任意）アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP 最良外部機能の確認

BGP 最良外部機能が正しく設定されていることを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show vrf detail**
3. **show ip bgp ipv4 mdt all** | **rd vrf**} | **multicast** | **tunnel unicast** or **show ip bgp vpn4 all rd** *route-distinguisher* | **vrf** *vrf-name* **rib-failure** *ip-prefix/length* **longer-prefixes**]] *network-address mask* **longer-prefixes**]] **cidr-only community** *community-list* **dampened-paths filter-list**] [**flap-statistics inconsistent-as neighbors paths line**]] **peer-group quote-regexp regexp**] [**summary labels**
4. **show bgp vpnv4 unicast vrf** *vrf-name ip-address*
5. **show ip route vrf** *vrf-name* **repair-paths** *ip-address*
6. **show ip cef vrf** *vrf-name ip-address* **detail**

手順の詳細

ステップ 1 enable

このコマンドを使用して、特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。次に例を示します。

例：

```
Router> enable
Router#
```

ステップ 2 show vrf detail

このコマンドを使用して、BGP 最良外部機能が有効になっていることを確認します。次の **show vrf detail** コマンド出力は、 BGP 最良外部機能が有効になっていることを示しています。

例：

```
Router# show vrf detail
VRF test1 (VRF Id = 1); default RD 400:1; default VPNID <not set>
  Interfaces:
    Se4/0
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:100:1                RT:200:1                RT:300:1
```

```
    RT:400:1
  Import VPN route-target communities
    RT:100:1                RT:200:1                RT:300:1
    RT:400:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

 Prefix protection with additional path enabled
Address family ipv6 not active.
```

ステップ 3 **show ip bgp ipv4 mdt all** | **rd vrf**} | **multicast** | **tunnel unicast** or **show ip bgp vpn4 all rd** *route-distinguisher* | **vrf** *vrf-name* **rib-failure** *ip-prefix/length* **longer-prefixes**]] *network-address mask* **longer-prefixes**]] **cidr-only community** *community-list* **dampened-paths filter-list**] [**flap-statistics inconsistent-as neighbors paths line**]] **peer-group quote-regexp regexp**] [**summary labels**

このコマンドを使用して、ベスト外部ルートがアドバタイズされていることを確認します。コマンド出力で、コード b はバックアップ パスを示し、コード x はベスト外部パスを示します。

例：

```
Router# show ip bgp vpnv4 all
BGP table version is 1104964, local router ID is 10.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, multipath,
b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 11:12 (default for vrf blue)
*>i1.0.0.1/32       10.10.3.3                0     200      0 1 ?
* i                 10.10.3.3                0     200      0 1 ?
*                   10.0.0.1                               0 1 ?
*bx                 10.0.0.1                 0             0 1 ?
*                   10.0.0.1                               0 1 ?
```

ステップ 4 **show bgp vpnv4 unicast vrf** *vrf-name ip-address*

このコマンドを使用して、ベスト外部ルートがアドバタイズされていることを確認します。

例：

```
Router# show bgp vpnv4 unicast vrf vpn1 10.10.10.10
BGP routing table entry for 10:10:10.10.10.10/32, version 10
Paths: (2 available, best #1, table vpn1)
  Advertise-best-external
  Advertised to update-groups:
    1          2
  200
    10.6.6.6 (metric 21) from 10.6.6.6 (10.6.6.6)
    Origin incomplete, metric 0, localpref 200, valid, internal, best
    Extended Community: RT:1:1
    mpls labels in/out 23/23
  200
    10.1.2.1 from 10.1.2.1 (10.1.1.1)
    Origin incomplete, metric 0, localpref 100, valid,
external, backup/repair,     advertise-best-external
    Extended Community: RT:1:1 , recursive-via-connected
    mpls labels in/out 23/nolabel
```

ステップ 5 **show ip route vrf** *vrf-name* **repair-paths** *ip-address*

このコマンドを使用して、修復ルートを表示します。

例：

```
Router# show ip route vrf vpn1 repair-paths

Routing Table: vpn1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B        10.1.1.0/24 [200/0] via 10.6.6.6, 00:38:33
                     [RPR][200/0] via 10.1.2.1, 00:38:33
B        10.1.1.1/32 [200/0] via 10.6.6.6, 00:38:33
                     [RPR][200/0] via 10.1.2.1, 00:38:33
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.2.0/24 is directly connected, Ethernet0/0
L        10.1.2.2/32 is directly connected, Ethernet0/0
B        10.1.6.0/24 [200/0] via 10.6.6.6, 00:38:33
                      [RPR][200/0] via 10.1.2.1, 00:38:33
```

ステップ 6 **show ip cef vrf** *vrf-name ip-address* **detail**

このコマンドを使用して、ベスト外部ルートを表示します。

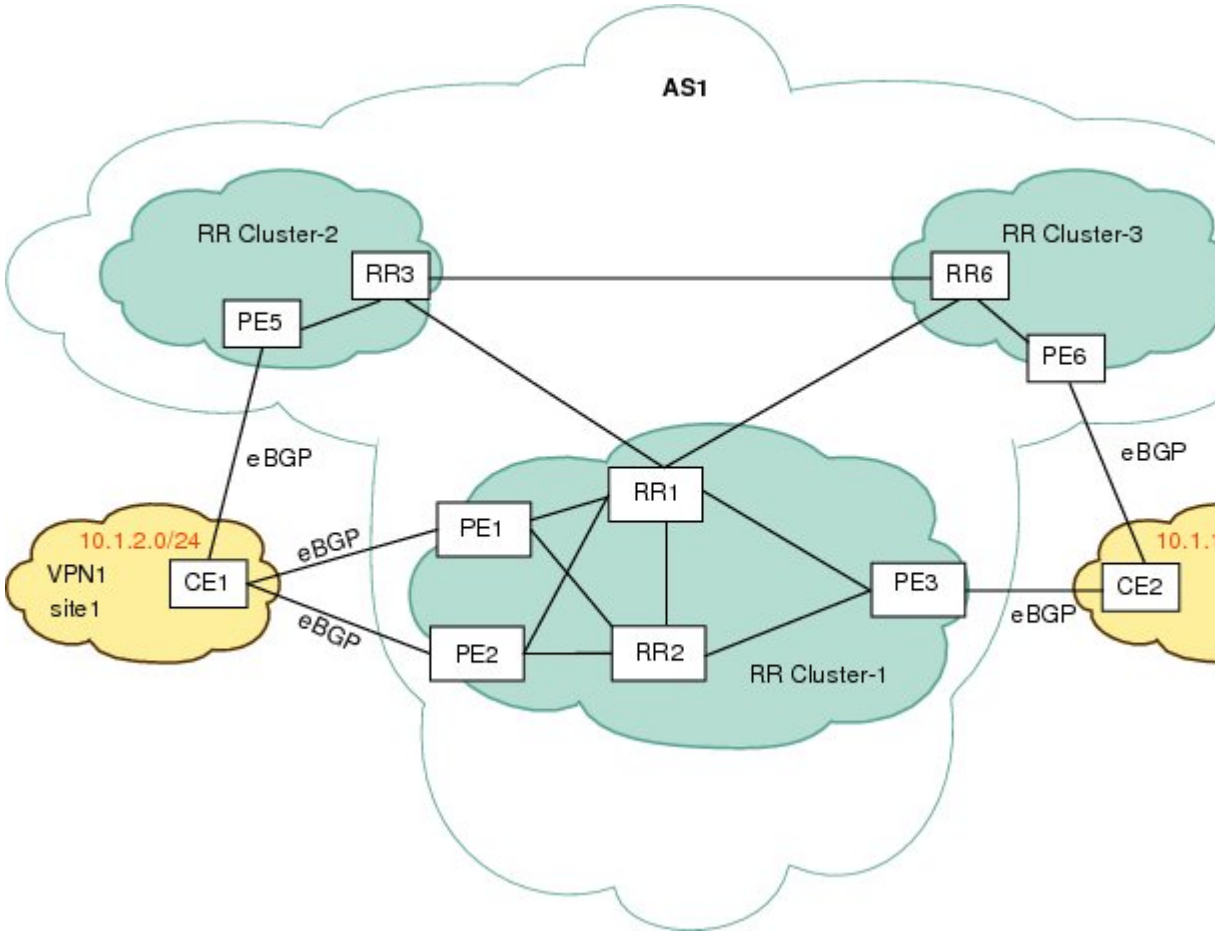
例：

```
Router# show ip cef vrf test 10.71.8.164 detail

10.71.8.164/30, epoch 0, flags rib defined all labels
 recursive via 10.249.0.102 label 35
   nexthop 10.249.246.101 Ethernet0/0 label 25
 recursive via 10.249.0.104 label 28,
repair
   nexthop 10.249.246.101 Ethernet0/0 label 24
```

クラスタ間の RR でのベスト外部パスの設定

クラスタ間の RR でのベスト外部パスを設定するには、次の作業を実行します。この特定作業の手順では、IPv4 アドレス ファミリで、下の図の RR1 を設定します。アドレス ファミリを設定する手順では、サポートされているその他のアドレス ファミリを一覧表示します。

図 *66* : クラスタ間の *RR* での *BGP* ベスト外部パスを設定するシナリオ



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **address-family ipv4 unicast**
7. **neighbor** *ip-address* **activate**
8. **neighbor***ip-address* **activate**
9. **bgp additional-paths select best-external**
10. **bgp additional-paths install**
11. **neighbor** *ip-address* **advertise best-external**
12. **neighbor** *ip-address***advertise best-external**
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 1`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.5.1.1 remote-as 1`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • この手順は RR3 用です。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.5.1.2 remote-as 1`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • この手順は RR6 用です。
ステップ 6	**address-family ipv4 unicast** 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • サポートされているアドレス ファミリは、IPv4 ユニキャスト、VPNv4 ユニキャスト、IPv6 ユニキャスト、VPNv6 ユニキャスト、IPv4+ラベル、IPv6+ラベルです。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Router(config-router-af)# neighbor 10.5.1.1 activate`	BGP ネイバーとの情報交換を有効にします。 • この手順は RR3 用です。
ステップ 8	**neighbor***ip-address* **activate** 例： `Router(config-router-af)# neighbor 10.5.1.2 activate`	BGP ネイバーとの情報交換を有効にします。 • この手順は RR6 用です。

	コマンドまたはアクション	目的
ステップ 9	**bgp additional-paths select best-external** 例： `Router(config-router-af)# bgp additional-paths select best-external`	ベスト外部パス（RR クラスタ外）を計算するようにシステムを設定します。
ステップ 10	**bgp additional-paths install** 例： `Router(config-router-af)# bgp additional-paths install`	BGP で特定のアドレス ファミリのバックアップ パスを計算し、RIB および CEF にインストールできるようにします。 • この手順は、RR が転送に対して有効になっている場合（RR がフォワーディング プレーンにある場合）に必要です。それ以外の場合、この手順は不要です。
ステップ 11	**neighbor** *ip-address* **advertise best-external** 例： `Router(config-router-af)# neighbor 10.5.1.1 advertise best-external`	（任意）アドバタイズでベスト外部パスを受信するようにネイバーを設定します。 • この手順は RR3 用です。
ステップ 12	**neighbor** *ip-address***advertise best-external** 例： `Router(config-router-af)# neighbor 10.5.1.2 advertise best-external`	（任意）アドバタイズでベスト外部パスを受信するようにネイバーを設定します。 • この手順は RR6 用です。
ステップ 13	**end** 例： Router(config-router-af)# end	（任意）アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

上記のシナリオでは、次のパスが、3 つの異なるクラスタ内にある 3 つの RR でベスト パス、バックアップ パス、ベスト内部パスとして選択されます。

RR1：

RR3：

RR6：

プレフィックス 10/8 に到達するため	ネクスト ホップ：
	PE5（ベストパス、ローカル プリファレンス = 200）
	PE3（バックアップ パス、ローカル プリファレンス = 150）

	PE3（ベスト内部パス、ローカル プリファレンス = 150）

プレフィックス 10/8 に到達するため	ネクスト ホップ：
	PE5（ベストパス、ローカル プリファレンス = 200）
	PE6（バックアップ パス、ローカル プリファレンス = 50）
	PE3（RR1 からベスト外部パスとして受信、ローカル プリファレンス = 150）

プレフィックス 10/8 に到達するため	ネクスト ホップ：
	PE5（ベストパス、ローカル プリファレンス = 200）
	PE6（バックアップ パス、ローカル プリファレンス = 50）
	PE3（RR1 からベスト外部パスとして受信、ローカル プリファレンス = 150）

BGP 最良外部の設定例

例：BGP 最良外部機能の設定

次の例は、VPNv4 モードで BGP 最良外部機能を設定する方法を示しています。

```
vrf definition test1
 rd 400:1
 route-target export 100:1
 route-target export 200:1
 route-target export 300:1
 route-target export 400:1
 route-target import 100:1
 route-target import 200:1
 route-target import 300:1
 route-target import 400:1
 address-family ipv4
 exit-address-family
 exit
!
interface Ethernet1/0
 vrf forwarding test1
 ip address 10.0.0.1 255.0.0.0
 exit
!
router bgp 64500
 no synchronization
 bgp log-neighbor-changes
```

```
 neighbor 10.5.5.5 remote-as 64500
 neighbor 10.5.5.5 update-source Loopback0
 neighbor 10.6.6.6 remote-as 64500
 neighbor 10.6.6.6 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4

bgp advertise-best-external
  neighbor 10.5.5.5 activate
  neighbor 10.5.5.5 send-community extended
  neighbor 10.6.6.6 activate
  neighbor 10.6.6.6 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf test1
  no synchronization
bgp recursion host
  neighbor 192.168.13.2 remote-as 64511
  neighbor 192.168.13.2 fall-over bfd
  neighbor 192.168.13.2 activate
  neighbor 192.168.13.2 as-override
 exit-address-family
```

例：クラスタ間の RR でのベスト外部パスの設定

次の例では、「クラスタ間の RR でのベスト外部パスの設定」の項に示されている図の RR1 を設定しています。RR1 は、クラスタ間の RR ネイバーへのベスト外部パスを計算、インストール、およびアドバタイズするように設定されています。

RR1

```
router bgp 1
 neighbor 10.5.1.1 remote-as 1
 neighbor 10.5.1.2 remote-as 1
 address-family ipv4 unicast
 neighbor 10.5.1.1 activate
 neighbor 10.5.1.2 activate
 bgp additional-paths select best-external
 bgp additional-paths install
 neighbor 10.5.1.1 advertise best-external
 neighbor 10.5.1.2 advertise best-external
 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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

関連項目	マニュアル タイトル
基本的な MPLS VPN	『*MPLS: Layer 3 VPNs Configuration Guide*』の「Configuring MPLS Layer 3 VPNs」モジュール
マルチプロトコル VRF	『*MPLS: Layer 3 VPNs Configuration Guide*』の「MPLS VPN VRF CLI for IPv4 and IPv6 VPNs」モジュール
リンクまたはノード障害の後に新しいパスを作成するフェールオーバー機能	『MPLS VPN--BGP Local Convergence』

標準

標準	タイトル
draft-marques-idr-best-external	『*BGP Best External, Advertisement of the best external route to iBGP*』

MIB

MIB	MIB のリンク
—	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

RFC

RFC	タイトル
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 最良外部の機能情報

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 *62 : BGP* 最良外部の機能情報

機能名	リリース	機能情報
BGP 最良外部	Cisco IOS XE Release 3.2S	BGP最良外部機能を使用すると、ネットワークにバックアップ外部ルートを用意でき、プライマリ外部ルートの接続が失われるのを回避できます。この機能は、外部ネイバーから受信したルートのうち最も優先するルートを、バックアップ ルートとしてアドバタイズします。 この機能は、Cisco IOS XE Release 3.2S で導入されました。 次のコマンドが導入または変更されました。**bgp advertise-best-external**、**bgp recursion host**、**show ip bgp**、**show ip bgp vpnv4**、 **show ip cef**、 **show ip cef vrf**、 **show ip route**、 **show ip route vrf**

機能名	リリース	機能情報
クラスタ間の RR での BGP ベスト外部パス	Cisco IOS XE リリース 3.4S	クラスタ間の RR での BGP ベスト外部パス機能は、RR クラスタ間におけるパスの多様性を実現します。この機能は、非クライアント iBGP ピアに対する最良外部機能を提供し、「クラスタ間ベスト外部パス」とも呼ばれます。 次のコマンドが導入されました。**bgp additional-pathsselect**、**neighbor advertise best-external**

第 47 章

IP および MPLS-VPN 向け BGP PIC エッジ

IP および MPLS-VPN 向け BGP PIC エッジ機能により、ネットワーク障害後の BGP コンバージェンスが向上します。このコンバージェンスは、IP ネットワークと MPLS ネットワークで使用可能であり、コア障害とエッジ障害の両方に適用されます。IP および MPLS-VPN 向け BGP PIC エッジ機能は、障害が検出された場合、即座にバックアップ/代替パスが引き継ぎ、すばやくフェールオーバーが有効化されるように、ルーティング情報ベース（RIB）、転送情報ベース（FIB）、および Cisco Express Forwarding にバックアップ/代替パスを作成、保存します。

（注） このドキュメントでは、IP および MPLS-VPN 向け BGP PIC エッジ機能は BGP PIC と呼ばれます。

- 機能情報の確認 （847 ページ）
- BGP PIC の前提条件 （848 ページ）
- BGP PIC の制約事項 （848 ページ）
- BGP PIC の概要 （849 ページ）
- BGP PIC の設定方法 （859 ページ）
- BGP PIC の設定例 （862 ページ）
- その他の参考資料 （866 ページ）
- BGP PIC の機能情報 （867 ページ）

機能情報の確認

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

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

BGP PIC の前提条件

- ボーダー ゲートウェイ プロトコル（BGP）および IP またはマルチプロトコル ラベル スイッチング（MPLS）ネットワークが稼働中であること、およびカスタマー サイトが複数のパスによってプロバイダー サイトと接続されていること（マルチホーム）を確認します。
- バックアップ/代替パスには、最良パスのネクスト ホップと異なる固有のネクスト ホップがあることを確認します。
- Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）プロトコルを有効にして、直接接続されたネイバーのリンク障害をすばやく検出できるようにします。

BGP PIC の制約事項

BGP PIC 機能には、次のような制約事項が適用されます。

- BGP マルチパスでは、プレフィックス独立コンバージェンス（PIC）機能はすでにサポートされています。
- MPLS VPN では、MPLS VPN 相互自律システム オプション B を使った BGP PIC 機能はサポートされていません。
- BGP PIC 機能は、IPv4、IPv6、VPNv4、および VPNv6 アドレス ファミリのプレフィックスをサポートします。
- BGP PIC 機能は、マルチキャストまたは L2VPN Virtual Routing and Forwarding（VRF）のアドレス ファミリで設定できません。
- ルート リフレクタがコントロール プレーンのみの場合、BGP PIC は必要ありません。これは BGP PIC はデータ プレーン コンバージェンスに対応しているためです。
- 2 台の PE デバイスが CE デバイスへの相互のバックアップ パスまたは代替パスになると、CE デバイスで障害が発生した場合にトラフィックがループする可能性があります。その場合、どちらのデバイスも CE デバイスに到達せず、トラフィックは存続可能時間（TTL）タイマーが切れるまで PE デバイス間で転送され続けます。
- BGP PIC 機能は、ノンストップ フォワーディング/ステートフル スイッチオーバー（NSF/SSO）をサポートしていません。ただし、両方のルート プロセッサで BGP PIC 機能が設定されている場合は、ISSU がサポートされます。
- BGP PIC 機能は、エッジとコアの両方で単一のネットワーク障害が発生した場合にのみ、トラフィック転送を解決します。

- BGP PIC 機能と BGP 最良外部機能を同時に使用することはできません。BGP 最良外部機能を設定した後に BGP PIC 機能を設定しようとすると、エラーが表示されます。

BGP PIC の概要

以下の各項では、BGP PIC 機能の詳細、障害を検出する方法、シナリオ、および設定方法について説明します。

利点

- プライマリ パスが無効になった場合や取り消された場合でも、フェールオーバー用の追加パスにより、接続を迅速に復元できます。
- トラフィック損失の軽減。
- コンバージェンス時間が一定なので、すべてのプレフィックスで切り替え時間が同じ。

BGP コンバージェンス

通常の状況では、BGP はネットワークの変更後に収束するのに数秒から数分かかることがあります。概要としては、BGP は次のプロセスの手順を実行します。

1. BGP は内部ゲートウェイ プロトコル（IGP）または BFD イベント、もしくはインターフェイス イベントを通じて不具合を確認します。
2. BGP はルーティング情報ベース（RIB）からルートを取り消し、RIB は Forwarding Information Base（FIB; 転送情報ベース）および分散 FIB（dFIB）からルートを取り消します。このプロセスにより、障害の影響を受けたプレフィックスへのデータ パスがクリアされます。
3. BGP は取り消しのメッセージをネイバーに送信します。
4. BGP は影響を受けたプレフィックスへの次に適したパスを計算します。
5. BGP は影響を受けたプレフィックスの次に適したパスを RIB に挿入し、RIB はそのパスを FIB および dFIB にインストールします。

このプロセスが完了するまでには数秒から数分かかることがあります。これは、ネットワークの遅延、ネットワーク全体のコンバージェンス時間、およびデバイスでのローカル ロードによって異なります。コントロール プレーンのコンバージェンスが行われて初めて、データ プレーンのコンバージェンスが行われます。

コンバージェンスの改善

BGP PIC 機能は、BGP、RIB、Cisco Express Forwarding、MPLS の追加機能によって実現されます。

• BGP の機能

BGP PIC は、IPv4 および VPNv4 アドレス ファミリのプレフィックスに影響を与えます。これらのプレフィックスについて、BGP は、プライマリ ベスト パスに加え、2 番目に適したパスも計算します（2 番目に適したパスは、バックアップ パスまたは代替パスと呼ばれます）。BGP は、影響を受けたプレフィックスのベスト パスとバックアップ パスまたは代替パスを BGP RIB にインストールします。バックアップ パスまたは代替パスにより、単一のネットワーク障害に対処する高速再ルーティング機能が提供されます。また、BGP は、IP RIB に対するアプリケーション プログラミング インターフェイス（API）に代替パスまたはバックアップ パスを追加します。

• RIB の機能

BGP PIC では、RIB はルートごとに代替パスをインストールします（使用可能な場合）。RIB は、バックアップ パスまたは代替パスを含む BGP ルートを選択した場合、ベスト パスとともにそのバックアップ パスまたは代替パスをインストールします。また、RIB は、この代替パスを FIB との API にも追加します。

• Cisco Express Forwarding 機能

BGP PIC では、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）はプレフィックスごとに代替パスを保存します。プライマリ パスがダウンした場合、Cisco Express Forwarding は、プレフィックスに依存しない方法でバックアップ パスまたは代替パスを検索します。また、シスコ エクスプレス フォワーディングは、局地的な障害を迅速に検出するために、BFD イベントをリッスンします。

• MPLS 機能

MPLS 転送は、プライマリ パスがダウンした場合には代替パスを保存して代替パスに切り替えるという点で、Cisco Express Forwarding と似ています。

BGP PIC 機能が有効な場合、BGP はプレフィックスごとにバックアップ パスまたは代替パスを計算し、BGP RIB、IP RIB、および FIB にインストールします。これにより、ネットワーク障害後のコンバージェンスが向上します。BGP PIC 機能によって検出されるネットワーク障害には、次の 2 種類があります。

- コア ノードまたはリンク障害（内部ボーダー ゲートウェイ プロトコル（iBGP）ノード障害）：PE ノードまたはリンクで障害が発生した場合、IGP コンバージェンスによって障害が検出されます。IGP は、RIB を通じて FIB に障害を伝達します。
- ローカル リンクまたは直近にあるネイバー ノードの障害（外部ボーダー ゲートウェイ プロトコル（eBGP）ノードまたはリンク障害）：ローカル リンク障害または eBGP シングルホップ ピア ノード障害を瞬時に検出するには、BFD を有効にする必要があります。Cisco Express Forwarding は eBGP シングルホップ ピアの障害を検出するために BFD イベントを探します。

データ プレーンでのコンバージェンス

障害を検出すると、Cisco Express Forwarding は、その障害の影響を受けるすべてのプレフィックスに対する代替ネクスト ホップを検出します。データ プレーン コンバージェンスは、BGP PIC の実装がソフトウェアに存在するかハードウェアに存在するかに応じて、瞬時に達成されます。

コントロール プレーンでのコンバージェンス

障害を検出すると、BGP は、IGP コンバージェンスまたは BFD イベントによってその障害を確認し、該当のプレフィックスについて取り消しのメッセージを送信し、ベスト パスとバックアップ パスまたは代替パスを再計算し、ネットワーク全体で次に適したパスをアドバタイズします。

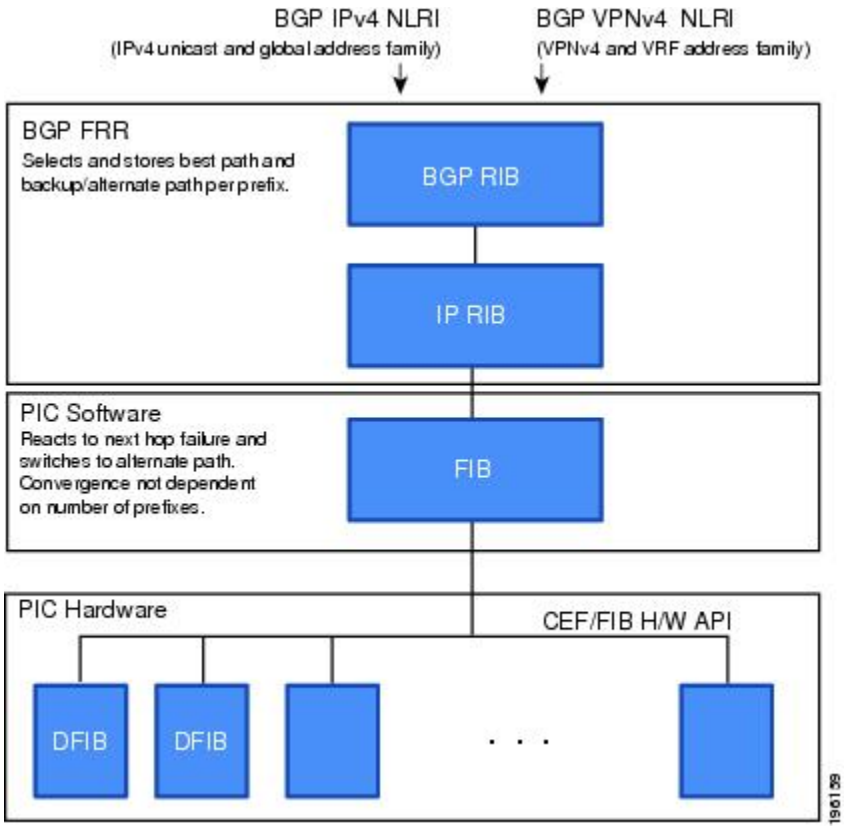
BGP Fast Reroute

BGP Fast Reroute（FRR; 高速再ルーティング）は、BGP、RIB、および Cisco Express Forwarding でのベスト パスとバックアップ パスまたは代替パスを提供します。BGP FRR は、現在のベスト パスが使用できない場合に宛先に到達するためのバックアップ BGP ネクスト ホップに関する高速再ルーティング メカニズムを RIB および Cisco Express Forwarding（CEF）に提供します。

BGP FRR は BGP で次に適したパスを事前に計算し、そのパスをバックアップ パスまたは代替パスとして RIB および Cisco ExpressForwardin に提供し、CEF はそのパスをライン カードにプログラムします。

BGP PIC 機能は、現在のネクスト ホップまたはこのネクスト ホップへのリンクがダウンした場合にCEF でトラフィックを他の出力ポートに迅速に切り替えることができるようにします。

図 *67 : BGP PIC* エッジと *BGP FRR*



障害の検出

IGP は、iBGP（リモート）ピアの障害を検出します。障害が検出されるまでに数秒かかる場合があります。コンバージェンスは、ラインカードでPICがイネーブルにされているかどうかに応じて、瞬時、または数秒以内に行われます。

直接接続されたネイバー（eBGP）で障害が発生した場合や、ネイバーがダウンしたことをBFDを使用して検出する場合。ライン カードで PIC が有効化されているかどうかに応じて、瞬時に検出されることがあり、コンバージェンスも瞬時または数秒以内に行われます。

BGP PIC による瞬時でのコンバージェンスの達成

BGP PIC 機能は Cisco Express Forwarding レベルで動作し、Cisco Express Forwarding はハードウェア ライン カードとソフトウェアの両方で処理できます。

- ラインカードでのシスコエクスプレスフォワーディングの処理をサポートしているプラットフォームでは、BGP PIC 機能は瞬時のコンバージェンスが可能です。
- ハードウェア ライン カードでの Cisco Express Forwarding を使用しないプラットフォームでは、ソフトウェアで Cisco Express Forwarding が実現されます。BGP PIC 機能は、ソフト

ウェアを介して Cisco Express Forwarding と連携し、数秒以内にコンバージェンスを達成します。

BGP PIC による MPLS VPN BGP ローカル コンバージェンスの機能向上

BGP PIC 機能は、ベストパスを再計算してリンク障害後の転送に新しいパスをインストールするフェールオーバー メカニズムを提供する「MPLS VPN—BGP ローカル コンバージェンス」機能への拡張機能です。この機能は、ローカル ラベルを 5 分間保持して、バックアップ パスまたは代替パスがトラフィックで使用されるようにしてトラフィックの損失を最小限に抑えることができます。

BGP PIC 機能は、事前にバックアップ パスまたは代替パスを計算することにより、LoC 時間を 1 秒未満に短縮します。リンク障害が発生すると、トラフィックはバックアップ/代替パスへ送られます。

BGP PIC 機能を設定すると、「MPLS VPN--BGP ローカル コンバージェンス」の機能がオーバーライドされます。設定から **protection local-prefixes** コマンドを削除する必要はありません。

BGP PIC の有効化

さまざまなサービス プロバイダー ネットワークにさまざまな VRF が含まれているため、BGP PIC では、すべての VRF に対して一度に BGP PIC 機能を設定することができます。

- VPNv4 アドレス ファミリ コンフィギュレーション モードはすべての VRF を保護します。
- VRF-IPv4 アドレス ファミリ コンフィギュレーション モードは IPv4 VRF のみを保護します。
- ルータ コンフィギュレーション モードは、グローバル ルーティング テーブルのプレフィックスを保護します。

BGP PIC シナリオ

BGP PIC 機能を設定して、高速コンバージェンスを実現できます。

CE 側での IP PE-CE リンクおよびノード保護（デュアル PE）

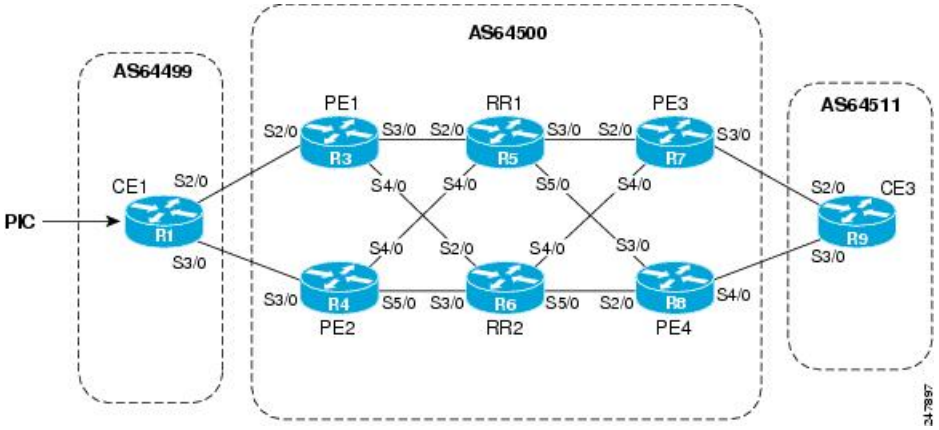
下の図は、BGP PIC 機能を使用するネットワークを示しています。このネットワークは、以下のコンポーネントで構成されています。

- PE デバイスと CE デバイスの間に eBGP セッションが存在します。
- CE1 からのトラフィックは、PE1 を使用して、デバイス CE3 経由でネットワーク 192.168.9.0/24 に到達します。
- CE1 には次の 2 つのパスがあります。

- プライマリ パスとしての PE1。
- バックアップ パスまたは代替パスとしての PE2。

CE1 は BGP PIC 機能を使用して設定されています。BGP は、PE1 をベスト パスとして、PE2 をバックアップ パスまたは代替パスとして計算し、両方のルートを RIB および Cisco Express Forwarding プレーンにインストールします。CE1-PE1 リンクがダウンすると、Cisco Express Forwarding はリンク障害を検出し、転送オブジェクトをバックアップ パスまたは代替パスに送ります。トラフィックは、Cisco Express Forwarding でのローカル高速コンバージェンスによって迅速に再ルーティングされます。

図 *68 : BGP PIC* を使用した *PE-CE* リンクの保護



CE 側での IP PE-CE リンクおよびノード保護（デュアル CE とデュアル PE のプライマリおよびバックアップ ノード）

下の図は、CE1 で BGP PIC 機能を使用するネットワークを示しています。このネットワークは、以下のコンポーネントで構成されています。

- PE デバイスと CE デバイスの間に eBGP セッションが存在します。
- CE1 からのトラフィックは、PE1 を使用して、デバイス CE3 経由でネットワーク 192.168.9.0/24 に到達します。
- CE1 には次の 2 つのパスがあります。
  - プライマリ パスとしての PE1。
  - バックアップ パスまたは代替パスとしての PE2。
- CE1 デバイスと CE2 デバイスの間に iBGP セッションが存在します。

この例では、CE1 と CE2 が BGP PIC 機能を使用して設定されています。BGP は、PE1 をベスト パスとして、PE2 をバックアップ パスまたは代替パスとして計算し、両方のルートを RIB および Cisco Express Forwarding プレーンにインストールします。

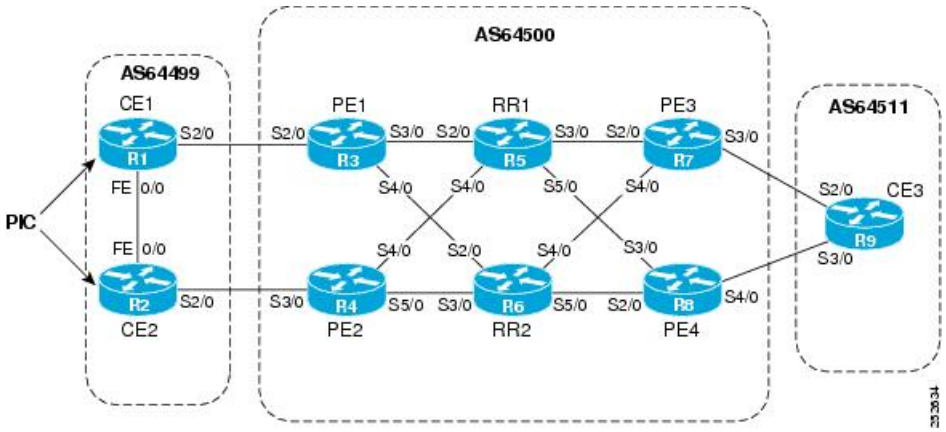
eBGP ピアの PE1 と PE2 についてのポリシーを CE1 と CE2 で設定することはできません。両方の CE デバイスで、ネクスト ホップとして eBGP ルートをポイントする必要があります。

CE1 では、CE3 に到達するためのネクスト ホップは PE1 経由であるため、PE1 は CE3 に到達するためのベストパスとなります。CE2 では、CE3 に到達するためのベストパスは PE2 です。CE2 は自身をネクスト ホップとして CE1 にアドバタイズし、CE1 も CE2 に対して同じことを行います。この結果、CE1 は特定のプレフィックスに対するパスを 2 つ持ち、ベスト パス選択ルールに従って、通常は iBGP パスよりも直接接続された eBGP パスを優先して選択します。同様に、CE2 にも、PE2 を経由する eBGP パスと CE1-PE1 を経由する iBGP パスの 2 つのパスがあります。

CE1-PE1 リンクがダウンすると、Cisco Express Forwarding はリンク障害を検出し、転送オブジェクトをバックアップ ノードまたは代替ノードの CE2 に送ります。トラフィックは、Cisco Express Forwarding でのローカル高速コンバージェンスによって迅速に再ルーティングされます。

CE1-PE1 リンクまたは PE1 がダウンした場合に、CE1 で BGP PIC が有効になっているときは、BGP はベスト パスを再計算し、RIB からネクスト ホップ PE1 を削除して、CE2 をネクスト ホップとして RIB および Cisco Express Forwarding に再インストールします。CE1 でバックアップまたは代替修復パスが Cisco Express Forwarding に自動的に挿入され、転送中のトラフィック損失が瞬時で済むようになるため、高速コンバージェンスが実現されます。

図 *69* : デュアル *CE*、デュアル *PE* ネットワークでの *BGP PIC* の使用



プライマリまたはバックアップ/代替パスの IP MPLS PE-CE リンク保護

上の図は、CE1 および CE2 で BGP PIC 機能を使用するネットワークを示しています。このネットワークは、以下のコンポーネントで構成されています。

- PE デバイスと CE デバイスの間に eBGP セッションが存在します。
- PE デバイスは、MPLS ネットワーク内のリフレクト デバイスを含む VPNv4 iBGP ピアです。
- CE1 からのトラフィックは、PE1 を使用して、デバイス CE3 経由でネットワーク 192.168.9.0/24 に到達します。
- CE3 は PE3 および PE4 とデュアルホーム接続されています。
- PE1 は、リフレクト ルータから CE3 に到達するためのパスを 2 つ持っています。

- PE3 は、PE3 アドレスとしてネクスト ホップを持つプライマリ パスです。
- PE4 は、PE4 アドレスとしてネクスト ホップを持つバックアップ/代替パスです。

この例では、すべての PE デバイスは、IPv4 または VPNv4 アドレス ファミリで BGP PIC 機能を使用して設定できます。

BGP PIC を PE-CE リンク保護のために BGP で動作させるには、PE デバイスの 1 つがプライマリとして、残りのデバイスがバックアップまたは代替として機能するように、CE3 から受信されるプレフィックスについてのポリシーを PE3 および PE4 で設定します。通常、これはローカル プリファレンスを使用して行いますが、PE3 により優位なローカル プリファレンスを与えます。MPLS クラウドでは、トラフィックは内部的に PE3 経由でフローし、CE3 に到達します。したがって、PE1 は PE3 をベスト パスとして、PE4 を次に適したパスとして認識します。

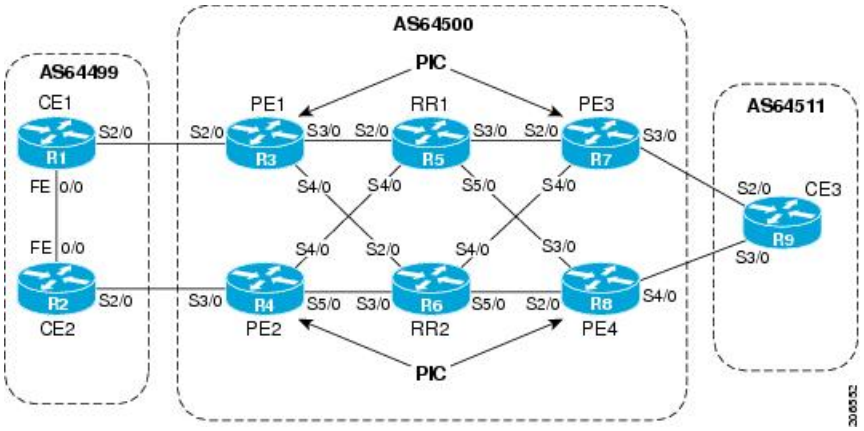
PE3-CE3 リンクがダウンすると、Cisco Express Forwarding はリンク障害を検出し、PE3 はベスト パスを再計算して、PE4 をベスト パスとして選択し、PE3 プレフィックスの取り消しメッセージをリフレクト ルータに送信します。BGP が PE4 をベスト パス ルートとして RIB および Cisco Express Forwarding にインストールするまで、一部のトラフィックは PE3-PE4 を通過します。PE1 は取り消しメッセージを受信し、ベスト パスを再計算して、PE4 をベスト パスとして選択し、このルートを RIB および Cisco Express Forwarding プレーンにインストールします。

これにより、PE3 および PE4 で BGP PIC が有効になっている場合、Cisco Express Forwarding はリンク障害を検出し、Cisco Express Forwarding にすでに存在するバックアップまたは代替ノードの PE4 を宛先として転送オブジェクトのインプレース変更を行います。PE4 はバックアップ/代替パスがローカルに生成されたことを認識し、CE3 に接続された出力ポートにトラフィックをルーティングします。この方法により、トラフィックの損失は最小限に抑えられ、迅速なコンバージェンスが行われます。

プライマリまたはバックアップ/代替パスの IP MPLS PE-CE ノード保護

下の図は、MPLS ネットワーク内のすべての PE デバイスで BGP PIC 機能を使用するネットワークを示しています。

図 *70 : MPLS* ネットワーク内のすべての *PE* デバイスでの *BGP PIC* の有効化



このネットワークは、以下のコンポーネントで構成されています。

- PE デバイスと CE デバイスの間に eBGP セッションが存在します。
- PE デバイスは、MPLS ネットワーク内のリフレクト ルータを含む VPNv4 iBGP ピアです。
- CE1 からのトラフィックは、PE1 を使用して、デバイス CE3 経由でネットワーク 192.168.9.0/24 に到達します。
- CE3 は PE3 および PE4 とデュアルホーム接続されています。
- PE1 は、リフレクト ルータから CE3 に到達するためのパスを 2 つ持っています。
  - PE3 は、PE3 アドレスとしてネクスト ホップを持つプライマリ パスです。
  - PE4 は、PE4 アドレスとしてネクスト ホップを持つバックアップ/代替パスです。

この例では、すべての PE デバイスは、IPv4 または VPNv4 アドレス ファミリで BGP PIC 機能を使用して設定されています。

BGP PIC を PE-CE ノード保護のために BGP で動作させるには、PE デバイスの 1 つがプライマリとして、残りのデバイスがバックアップまたは代替として機能するように、CE3 から受信されるプレフィックスについてのポリシーを PE3 および PE4 で設定します。通常、これはローカル プリファレンスを使用して行いますが、PE3 により優位なローカル プリファレンスを与えます。MPLS クラウドでは、トラフィックは内部的に PE3 経由でフローし、CE3 に到達します。したがって、PE1 は PE3 をベストパスとして、PE4 を次に適したパスとして認識します。

PE3 がダウンすると、PE1 は IGP によるホスト プレフィックスの削除を瞬時に認識し、ベストパスを再計算して、PE4 をベスト パスとして選択し、このルートを RIB および Cisco Express Forwarding プレーンにインストールします。通常の BGP コンバージェンスが行われ、その一方で、BGP PIC は PE4 経由でトラフィックをリダイレクトするため、パケットが失われることはありません。

これにより、PE3 で BGP PIC が有効になっている場合、Cisco Express Forwarding は PE3 でのノード障害を検出し、バックアップまたは代替ノードの PE4 に転送オブジェクトを送ります。PE4 はバックアップ パスまたは代替パスがローカルに生成されたことを認識し、バックアップ パスまたは代替パスを使用してトラフィックを出力ポートにルーティングします。これにより、トラフィック損失が最小限に抑えられます。

PE デバイスでローカル ポリシーが設定されていない場合

PE1 および PE2 は、ローカル ポリシーを使用せずに、ネクスト ホップとして eBGP CE パスをポイントします。各 PE デバイスはもう一方のパスを受け取り、BGP はバックアップ パスまたは代替パスを計算し、そのパスを、CE に対する独自の eBGP パスとともにベスト パスとして Cisco Express Forwarding にインストールします。MPLS PE-CE リンクおよびノード保護ソリューションの制限は、BGP ポリシーを変更できないことです。そのため、ベスト外部パスなしで動作する必要があります。

PE デバイスでローカル ポリシーが設定されている場合

出力 CE に到達するためのプライマリ パスとしていずれかの PE デバイスを選択するローカル ポリシーが PE デバイス上にある場合は、常に、バックアップまたは代替ノードの PE3 で、

バックアップ/代替ラベルを付けて外部 CE ルートをルート リフレクタおよび遠端 PE デバイスに伝播するために **bgp advertise-best-external** コマンドが必要となります。

Cisco Express Forwarding の再帰

再帰は、プライマリ パスがダウンしたときに、次に一致率の高いパスを発見する機能です。

BGP PIC がインストールされていない場合に、プレフィックスへのネクスト ホップで障害が発生すると、Cisco Express Forwarding は、プレフィックスへ向かう別のパスを見つけるために、FIB を再帰処理して、このプレフィックスと一致する部分が 2 番目に長いパスを探します。この再帰メカニズムは、ネクスト ホップが複数ホップ離れており、ネクスト ホップに到達する経路が複数ある場合に役立ちます。

ただし、BGP PIC 機能を使用する場合は、次の理由により、Cisco Express Forwarding の再帰の無効化が必要になることがあります。

- Cisco Express Forwarding ですべての FIB エントリを検索する場合、再帰によって収束が遅くなります。
- BGP PIC エッジでは、代替パスが事前に計算済みです。したがって、Cisco Express Forwarding の再帰は不要です。

BGP PIC 機能が有効になっている場合、次の 2 つの条件に合致していると、Cisco Express Forwarding の再帰はデフォルトで無効になります。

- ネクスト ホップが /32 ネットワーク マスクを使って認識されている場合（ホスト ルート）
- ネクスト ホップが直接接続されている場合

それ以外の場合は、Cisco Express Forwarding の再帰は有効になります。

bgp recursion host コマンドを発行すると、BGP ホスト ルートに対する Cisco Express Forwarding の再帰を無効または有効にすることができます。このプロビジョニングは、BGP PIC 機能の一部です。

（注） BGP PIC 機能が有効になっている場合、デフォルトでは、**bgp recursion host** は、VPNv4 および VPNv6 アドレス ファミリに対して設定され、IPv4 および IPv6 アドレス ファミリに対して無効になります。

BGP で直接接続されたネクスト ホップに対する Cisco Express Forwarding の再帰を無効または有効にするには、**disable-connected-check** コマンドを実行します。

BGP PIC の設定方法

BGP PIC の設定

さまざまなサービス プロバイダー ネットワークにさまざまな VRF が含まれているため、BGP PIC 機能では、すべての VRF に対して一度に BGP PIC 機能を設定することができます。

- VPNv4 アドレス ファミリ コンフィギュレーション モードはすべての VRF を保護します。
- VRF-IPv4 アドレス ファミリ コンフィギュレーション モードは IPv4 VRF のみを保護します。
- ルータ コンフィギュレーション モードは、グローバル ルーティング テーブルのプレフィックスを保護します。

マルチプロトコル VRF の設定方法、および機能が有効になっていることを確認するための出力を示す完全な設定例については、例：BGP PIC の設定 （862 ページ）を参照して下さい。

始める前に

- MPLS VPN で BGP PIC 機能を実装している場合は、BGP PIC 機能を設定する前にネットワークが正しく動作していることを確認します。詳細については、「Configuring MPLS Layer 3 VPNs」を参照してください。
- MPLS VPN に BGP PIC 機能を実装している場合は、マルチプロトコル VRF を設定して、ルート ターゲット ポリシー（インポートおよびエクスポート）を IPv4 と IPv6 との間で共有したり、IPv4 VPN と IPv6 VPN に別々のルート ターゲット ポリシーを設定したりすることができるようにします。マルチプロトコル VRF の設定については、「MPLS VPN--VRF CLI for IPv4 and IPv6 VPNs」を参照してください。
- CE デバイスが少なくとも 2 つのパスによってネットワークに接続されていることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. 次のいずれかを実行します。
   - **address-family ipv4** [**unicast** | **vrf** *vrf-name*]
   - **address-family vpnv4** [**unicast**]
5. **bgp additional-paths install**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **activate**
8. **bgp recursion host**

9. **neighbor** *ip-address* **fall-over** [**bfd** |**route-map** *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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **address-family ipv4** [**unicast** | **vrf** *vrf-name*]
	• **address-family vpnv4** [**unicast**]
	例：
	`Device(config-router)# address-family ipv4 unicast`
	例：
	`Device(config-router)# address-family vpnv4`
		IPv4 または VPNv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
		• **unicast** キーワードは、IPv4 または VPNv4 ユニキャスト アドレス ファミリを指定します。
		• **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。

ステップ 5	**bgp additional-paths install** 例： `Device(config-router-af)# bgp additional-paths install`	バックアップ/代替パスを計算し、これを RIB およびシスコ エクスプレス フォワーディングにインストールします。
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャス

	コマンドまたはアクション	目的
		トアドレスプレフィックスだけを交換します。その他のアドレス プレフィックス タイプを交換するには、そのプレフィックス タイプについて、アドレスファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用してネイバーをアクティブ化する必要もあります。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	ネイバーが IPv4 ユニキャスト アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。
ステップ 8	**bgp recursion host** 例： `Device(config-router-af)# bgp recursion host`	（任意）IPv4、VPNv4、VRF アドレス ファミリの recursive-via-host フラグを有効にします。 • BGP PIC 機能が有効になっている場合、Cisco Express Forwarding の再帰は無効になります。ほとんどの場合、BGP PIC がイネーブルのときに、再帰をイネーブルにする必要はありません。
ステップ 9	**neighbor** *ip-address* **fall-over** [**bfd** | **route-map** *map-name*] 例： `Device(config-router-af)# neighbor 192.168.1.1 fall-over bfd`	ネイバーで障害が発生したことを検出する BFD プロトコル サポートを有効にします。検出は瞬時に行われることがあります。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP PIC コアの無効化

BGP PIC コア機能はデフォルトで有効になっています。BGP PIC コア機能を無効にするには、次の設定を使用します。

（注） BGP PIC コア機能を再度有効にするには、グローバル コンフィギュレーション モードで **cef table output-chain build favor convergence-speed** コマンドを使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **cef table output-chain build favor memory-utilization**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**cef table output-chain build favor memory-utilization** 例： `Device(config)# cef table output-chain build favor memory-utilization`	ネットワークを介してパケットを転送できるように、Cisco Express Forwarding テーブル出力チェーンの構築に関するメモリ特性を設定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

BGP PIC の設定例

例：BGP PIC の設定

次の例は、VPNv4 アドレス ファミリ コンフィギュレーション モードで BGP PIC 機能を設定して、すべての VRF で機能を有効にする方法を示しています。次の例では、blue と green という 2 つの VRF を定義しています。VRF blue と VRF green 内の VRF を含む、すべての VRF は、バックアップ パスまたは代替パスにより保護されています。

```
vrf definition test1
 rd 400:1
 route-target export 100:1
 route-target export 200:1
 route-target export 300:1
 route-target export 400:1
```

```
 route-target import 100:1
 route-target import 200:1
 route-target import 300:1
 route-target import 400:1
 address-family ipv4
 exit-address-family
 exit
!

 vrf forwarding test1
 ip address 10.0.0.1 255.0.0.0
 exit
router bgp 3
 no synchronization
 bgp log-neighbor-changes
 redistribute static
 redistribute connected
 neighbor 10.6.6.6 remote-as 3
 neighbor 10.6.6.6 update-source Loopback0
 neighbor 10.7.7.7 remote-as 3
 neighbor 10.7.7.7 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  bgp additional-paths install
  neighbor 10.6.6.6 activate
  neighbor 10.6.6.6 send-community both
  neighbor 10.7.7.7 activate
  neighbor 10.7.7.7 send-community both
 exit-address-family
 !
 address-family ipv4 vrf blue
  import path selection all
  import path limit 10
  no synchronization
  neighbor 10.11.11.11 remote-as 1
  neighbor 10.11.11.11 activate
 exit-address-family
 !
 address-family ipv4 vrf green
  import path selection all
  import path limit 10
  no synchronization
  neighbor 10.13.13.13 remote-as 1
  neighbor 10.13.13.13 activate
 exit-address-family
```

次の **show vrf detail** コマンド出力は、 BGP PIC 機能が有効になっていることを示しています。

```
Router# show vrf detail
VRF test1 (VRF Id = 1); default RD 400:1; default VPNID <not set>
  Interfaces:
    Se4/0
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:100:1                RT:200:1                RT:300:1
    RT:400:1
  Import VPN route-target communities
    RT:100:1                RT:200:1                RT:300:1
    RT:400:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

```
  Prefix protection with additional path enabled
Address family ipv6 not active.
```

例：BGP PIC のバックアップ/代替パスの表示

次の例のコマンド出力は、VRF blue 内の VRF にバックアップ パスまたは代替パスがあることを示しています。

```
Device# show ip bgp vpnv4 vrf blue 10.0.0.0

BGP routing table entry for 10:12:12.0.0.0/24, version 88
Paths: (4 available, best #1, table blue)
  Additional-path
  Advertised to update-groups:
     6
  1, imported path from 12:23:12.0.0.0/24
    10.3.3.3 (metric 21) from 10.6.6.6 (10.6.6.6)
      Origin incomplete, metric 0, localpref 200, valid, internal, best
      Extended Community: RT:12:23
      Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
      mpls labels in/out nolabel/37
  1, imported path from 12:23:12.0.0.0/24
    10.13.13.13 (via green) from 10.13.13.13 (10.0.0.2)
      Origin incomplete, metric 0, localpref 100, valid, external
      Extended Community: RT:12:23 , recursive-via-connected
  1, imported path from 12:23:12.0.0.0/24
    10.3.3.3 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 200, valid, internal
      Extended Community: RT:12:23
      Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
      mpls labels in/out nolabel/37
  1
    10.11.11.11 from 10.11.11.11 (1.0.0.1)
      Origin incomplete, metric 0, localpref 100, valid, external, backup/repair
      Extended Community: RT:11:12 , recursive-via-connected
```

次の例のコマンド出力は、VRF green 内の VRF にバックアップ パスまたは代替パスがあることを示しています。

```
Device# show ip bgp vpnv4 vrf green 12.0.0.0

BGP routing table entry for 12:23:12.0.0.0/24, version 87
Paths: (4 available, best #4, table green)
  Additional-path
  Advertised to update-groups:
     5
  1, imported path from 11:12:12.0.0.0/24
    10.11.11.11 (via blue) from 10.11.11.11 (1.0.0.1)
      Origin incomplete, metric 0, localpref 100, valid, external
      Extended Community: RT:11:12 , recursive-via-connected
  1
    10.3.3.3 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 200, valid, internal
      Extended Community: RT:12:23
      Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
      mpls labels in/out nolabel/37
  1
    10.13.13.13 from 10.13.13.13 (10.0.0.2)
      Origin incomplete, metric 0, localpref 100, valid, external, backup/repair
      Extended Community: RT:12:23 , recursive-via-connected
```

```
  1
    10.3.3.3 (metric 21) from 10.6.6.6 (10.6.6.6)
      Origin incomplete, metric 0, localpref 200, valid, internal, best
      Extended Community: RT:12:23
      Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
      mpls labels in/out nolabel/37
```

次の例のコマンド出力は、バックアップ パスおよび代替パスの BGP ルーティング テーブルのエントリを示しています。

```
Device# show ip bgp 10.0.0.0 255.255.0.0

BGP routing table entry for 10.0.0.0/16, version 123
Paths: (4 available, best #3, table default)
  Additional-path
  Advertised to update-groups:
     2          3
  Local
    10.0.101.4 from 10.0.101.4 (10.3.3.3)
      Origin IGP, localpref 100, weight 500, valid, internal
  Local
    10.0.101.3 from 10.0.101.3 (10.4.4.4)
      Origin IGP, localpref 100, weight 200, valid, internal
  Local
    10.0.101.2 from 10.0.101.2 (10.1.1.1)
      Origin IGP, localpref 100, weight 900, valid, internal, best
  Local
    10.0.101.1 from 10.0.101.1 (10.5.5.5)
      Origin IGP, localpref 100, weight 700, valid, internal, backup/repair
```

次の例のコマンド出力は、バックアップ パスおよび代替パスのルーティング情報ベースのエントリを示しています。

```
Device# show ip route repair-paths 10.0.0.0 255.255.0.0

Routing entry for 10.0.0.0/16
  Known via "bgp 10", distance 200, metric 0, type internal
  Last update from 10.0.101.2 00:00:56 ago
  Routing Descriptor Blocks:
  * 10.0.101.2, from 10.0.101.2, 00:00:56 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: none
    [RPR]10.0.101.1, from 10.0.101.1, 00:00:56 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: none
```

次の例のコマンド出力は、バックアップ パスおよび代替パスの Cisco ExpressForwarding/転送情報ベースのエントリを示しています。

```
Device# show ip cef 10.0.0.0 255.255.0.0 detail

10.0.0.0/16, epoch 0, flags rib only nolabel, rib defined all labels
  recursive via 10.0.101.2
    attached to
  recursive via 10.0.101.1, repair
    attached to
```

例：BGP PIC コアの無効化

次の例は、グローバル コンフィギュレーション モードで BGP PIC コアを無効にする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# cef table output-chain build favor memory-utilization
Device(config)# end
```

その他の参考資料

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
基本的な MPLS VPN	『*MPLS: Layer 3 VPNs Configuration Guide*』の「Configuring MPLS Layer 3 VPNs」モジュール
リンクまたはノード障害の後に新しいパスを作成するフェールオーバー機能	『*MPLS: Layer 3 VPNs Configuration Guide*』の「MPLS VPN—BGP Local Convergence」モジュール
マルチプロトコル VRF の設定	『*MPLS: Layer 3 VPNs Configuration Guide*』の「MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs」モジュール

関連資料

標準

標準	タイトル
draft-walton-bgp-add-paths-04.txt	『*Advertisement of Multiple Paths in BGP*』

MIB

MIB	MIB のリンク
—	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

RFC

RFC	タイトル
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 PIC 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 *63 : BGP PIC* の機能情報

機能名	リリース	機能情報
IP および MPLS-VPN 向け BGP PIC エッジ		IP および MPLS-VPN 向け BGP PIC エッジ機能により、ネットワーク障害後の BGP コンバージェンスが向上します。このコンバージェンスは、IP ネットワークと MPLS ネットワークで使用可能であり、コア障害とエッジ障害の両方に適用されます。IP および MPLS-VPN 向け BGP PIC エッジ機能は、障害が検出された場合、即座にバックアップ/代替パスが引き継ぎ、すばやくフェールオーバーが有効化されるように、ルーティング情報ベース（RIB）、転送情報ベース（FIB）、および Cisco Express Forwarding にバックアップ/代替パスを作成、保存します。 次のコマンドが導入または変更されました。**bgp additional-paths install**、**bgp recursion host**、**show ip bgp**、**show ip cef**、 **show ip route**、**show vrf**

第 48 章

BGP 低速ピアの検出と軽減

ネットワーク管理者は、BGP 低速ピア機能を使用して BGP 低速ピアを検出し、ピアを低速ピアとして静的に設定したり、ダイナミックにマークしたりすることができます。

- BGP 低速ピアの検出では、設定した時間内にアップデート メッセージを送信していない BGP ピアを特定します。低速ピアの存在は、ネットワーク輻輳やレシーバが時間内にアップデートを処理しないなどのネットワークに問題があることを示しており、低速ピアがあるかどうかを知ることは、管理者が問題を解決するために役に立ちます。
- BGP 低速ピア設定では、ピアをその通常のアップデート グループから低速アップデート グループに移動するか、分割するため、通常のアップデート グループが速度を落とさずに動作し、迅速にコンバージできます。

- 機能情報の確認 （869 ページ）
- BGP 低速ピアの検出と軽減について （870 ページ）
- BGP 低速ピアの検出と軽減の方法 （873 ページ）
- BGP 低速ピアの検出と軽減の設定例 （888 ページ）
- その他の参考資料 （890 ページ）
- iBGP ローカル AS に対する BGP サポートの機能情報 （892 ページ）

機能情報の確認

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

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

BGP 低速ピアの検出と軽減について

BGP 低速ピアの問題

BGP アップデート生成では、アップデート グループの概念を使用して、パフォーマンスを最適化しています。アップデート グループは、同じアウトバウンド ポリシーを持つピアの集まりです。アップデートの生成時に、グループ ポリシーを使用して、メッセージがフォーマットされ、グループのメンバーに送信されます。

リソース使用の公平性を維持するため、各アップデート グループに、フォーマット済みのメッセージのクォータが割り当てられ、キャッシュに保存されます。メッセージがグループによってフォーマットされると、キャッシュに追加され、グループのすべてのメンバーに送信されるときに削除されます。

低速ピアとは、Cisco IOS ソフトウェアがアップデート メッセージを生成する速度に追い付いていけず、長時間（数分程度）存続しているピアのことです。ピアが低速になる原因はいくつかあります。

- パケットの損失やピアへのリンクの大量のトラフィックがあり、BGP TCP 接続のスループットが著しく低い
- ピアの CPU 負荷が高く、必要な頻度で TCP 接続にサービスできない

アップデート グループに低速ピアが存在すると、送信保留中のフォーマット済みのアップデート数が増加します。キャッシュの制限に達すると、グループに新しいメッセージをフォーマットするためのクォータが割り当てられなくなります。新しいメッセージをフォーマットするためには、既存のメッセージの一部を低速ピアで送信し、キャッシュから削除する必要があります。アドバタイズされるか、取り消されることを待機している新しく変更された BGP ネットワークがある場合でも、低速ピアより高速で、フォーマット済みの送信を完了したグループの残りのメンバーには、新しく送信するメッセージがなくなります。いずれかのピアでアップデートの処理が遅い場合に、グループ内のすべてのピアのフォーマットがブロックされるこの影響が「低速ピア」の問題です。

一時的な低速は低速ピアにならない

BGP テーブルの大規模な変更（接続のリセットなど）を発生させるイベントによって、アップデート生成レートに短時間のスパイクが発生することがあります。そのようなイベントの発生時に一時的に遅延しても、イベント後にすぐに回復するピアは、低速ピアとみなされません。ピアが低速とマークされるのは、長時間（数分程度）、生成されるアップデートの平均速度に追い付いていくことができない場合のみです。

BGP 低速ピア機能

BGP 低速ピア機能には、ネットワーク管理者向けの 3 つのオプションが用意されています。

- BGP低速ピア検出のみを設定できます。この場合、低速ピアが検出され、それに関する情報が提供されるだけです。低速ピアを検出すると、低速ピアの原因となっているネットワークの問題を解決できるため、特に大規模な BGP ピアのネットワークでは重要な機能です。
- ダイナミック BGP 低速ピアを設定できます。このような低速ピア保護を設定した場合、デフォルトで低速ピア検出が有効になります。低速ピアが通常のアップデート グループから低速アップデート グループに移動されるか「分割」されるため、通常のアップデート グループは速度を落とさずに動作し、低速ピアより速く収束できます。（**permanent** キーワードを指定して）低速ピアを消去するまで低速アップデート グループで低速ピアを維持するか、または状況が改善したら、低速ピアをその通常のアップデート グループにダイナミックに戻せるようにするかを選択できます。低速ピアの状態を解消する前に、**permanent** キーワードを使用してネットワークの問題を解決することをお勧めします。
- リンクの問題または低速な CPU 処理能力のために、すでにどのピアが低速かわかっている場合は、スタティック BGP 低速ピアを設定できます。検出は不要です。静的設定のために、低速ピアがそこに留まる可能性が高くなります。

BGP 低速ピア検出

低速ピアが低速ピア アップデート グループに移動されるように設定するかどうかに関係なく、BGP 低速ピアを検出することを選択できます。BGP 低速ピアを検出するだけで、アップデート グループを分割しなくても低速ピアに関する有益な情報が得られます。その後、低速ピアの原因となっているネットワークの問題を解決する必要があります。

アップデート メッセージのタイムスタンプ

BGP 低速ピア検出は、アップデート グループ内のアップデート メッセージのタイムスタンプに依存します。アップデート メッセージのタイムスタンプは、フォーマットされるときに設定されます。BGP 低速ピア検出が設定されている場合、ピア キュー内の最も古いメッセージのタイムスタンプが現在の時刻と比較され、ピアが設定された低速ピア時間しきい値よりも遅れているかどうかが判断されます。

たとえば、ピア キュー内の最も古いメッセージが 3 分以上前にフォーマットされているものの、BGP 低速ピア検出のしきい値が 3 分に設定されている場合、そのアップデート メッセージをフォーマットしたピアが低速ピアであると判断されます。

Cisco IOS ソフトウェアは、低速ピアが検出されるか回復された場合（そのアップデート グループがコンバージされ、しきい値の時間より前にフォーマットされたメッセージがない場合）に syslog イベントを生成します。

BGP 低速ピア検出の利点

低速ピア検出により、低速ピアに関する情報が得られ、ピアを別のアップデート グループに移動せずに根本的原因を解決できます。そのため、低速ピア検出で必要とされるのは、ネットワークで何を改善できるかを識別するための 1 つのコマンドだけです。

ダイナミックまたはスタティック BGP 低速ピアの設定の利点

アップデート グループに低速ピアが存在すると、送信保留中のフォーマット済みのアップデート数が増加します。未処理分が減るまで、新しいメッセージをフォーマットして送信することができません。その状況では、BGP アップデート パケットが遅延するため、BGP ネットワークへのアドバタイズが遅延します。この問題は、ダイナミック低速ピアまたはスタティック低速ピアを設定すると、解決したり、防止したりできます。この設定により、低速ピアが新しい低速ピア アップデート グループのメンバーとなるため、低速ピアによる低速でない BGP ピアの遅延を防止できます。

スタティック低速ピア

ピアが低速であると確信できる場合は、そのピアを低速ピアとして静的に設定できます。低速リンクがあるか、処理能力が低いために低速になることがわかっているピアに対しては、スタティック低速ピアが推奨されます。

スタティック低速ピア設定により、Cisco IOS ソフトウェアで、そのピア用の個別のアップデート グループが作成されます。同じアップデート グループに属する 2 つのピアを低速として設定する場合、これらの 2 つのピアはポリシーが一致するために、単一の低速ピア アップデート グループに移動されます。低速アップデート グループは、最も遅い低速ピアの速度で動作します。

スタティック低速ピアは次の 2 つのいずれかの方法で設定できます。

- BGP ネイバー（アドレス ファミリ）レベルで
- ピア ポリシー テンプレートを使用して

たとえば、ネットワーク輻輳やレシーバが時間内にアップデートを処理しないなど、ピアが低速になる根本的原因を特定する必要がある場合があります。スタティック低速ピアが元のアップデート グループに自動的に戻されることはありません。スタティック低速ピアを元のアップデート グループに復元するには、**no neighbor slow-peer split-update-group static** コマンドまたは **no slow-peer split-update-group static** コマンドを使用します。

ダイナミック低速ピア

スタティック低速ピアとしてマークする代わりに、ピア キュー内の最も古いメッセージのタイムスタンプが現在の時刻から遅れている時間に基づいて、低速ピアをダイナミックに設定します。デフォルトのしきい値は 300 秒で、これは設定可能です。任意の **permanent** キーワードを指定することをお勧めします。このキーワードにより、低速ピアの根本的原因を解決する間、ピアが低速ピア グループ内に維持されます。その後、**clear bgp slow** コマンドを使用して、ピアを元のグループに戻すことができます。

permanent キーワードを設定しない場合、そのピアが低速でない動作に回復すると、元のグループに戻されます。

ダイナミック低速ピアを設定すると、検出が自動的にイネーブルになります。

ダイナミック低速ピアは次の 3 つの方法で設定できます。

- アドレス ファミリ ビュー レベルで
- ネイバー トポロジ（つまり、ネイバー アドレスファミリ）レベルで
- ピア ポリシー テンプレートを使用して

BGP 低速ピアの検出と軽減の方法

低速ピアの検出

低速ピアをそのアップデート グループから移動せずに、低速ピアの検出のみを行う必要がある場合があります。そのような検出では、syslog メッセージにより、BGP ピアが設定可能な時間内にアップデート メッセージを送信していないことが通知されます。ピアはそのアップデート グループに留まり、アップデート グループは分割されません。syslog メッセージ レベルは、検出と回復の両方で通知レベルです。

BGP低速ピアをダイナミックに設定する場合は、ダイナミック低速ピア保護の設定（880ページ）を参照してください。タスクには低速ピアを検出する手順が含まれ、必須です。

次のいずれかのタスクを実行して、低速ピアを検出します。

アドレスファミリ レベルでのダイナミック低速ピアの検出

このタスクを実行して、アドレスファミリ レベルですべてのダイナミック低速ピアを検出します（特定の低速ピアを検出する場合、ネイバー レベルで、またはピア ポリシー テンプレートを使用して低速ピアを検出します）。

最後の手順は任意です。特定のピアの低速ピア検出をディセーブルにする場合に使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4**
6. **bgp slow-peer detection** [**threshold** *seconds*]
7. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection disable**

手順の詳細

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

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Router(config-router)# neighbor 10.4.4.4 remote-as 5`	（任意）BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • この手順は、下の手順 7 に示すように、特定のピアのダイナミック低速ピア保護をディセーブルにする場合に必要です。
ステップ 5	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**bgp slow-peer detection** [**threshold** *seconds*] 例： `Router(config-router-af)# bgp slow-peer detection threshold 600`	グローバル低速ピア検出を設定し、ピアが低速ピアとして判断される前に、ピア キュー内の最も古いアップデート メッセージのタイムスタンプが現在の時刻から遅れてもかまわない時間を秒単位で指定します。 • このしきい値の範囲は 120 ～ 3600 です。コマンドを設定する場合、デフォルトは 300 です。
ステップ 7	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection disable** 例： `Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection disable`	（任意）特定のピアの低速ピア検出をディセーブルにします。 • 手順 5 でグローバル低速ピア検出を設定しており、特定のピアまたはピア ウループに対して低速ピア検出をディセーブルにする場合にのみ、このコマンドを使用します。

ネイバー レベルでのダイナミック低速ピアの検出

特定のネイバー アドレスにあるか、または特定のピア グループに属するダイナミック低速ピアを検出するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4**
5. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection**[**threshold** *seconds*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection**[**threshold** *seconds*] 例： `Router(config-router-af)# neighbor 172.60.2.3 slow-peer detection threshold 1200`	（任意）ピアが低速ピアとして判断される前に、ピア キュー内の最も古いメッセージのタイムスタンプが現在の時刻から遅延してもかまわない時間を秒単位で指定します。 • しきい値の範囲は 120 ～ 3600 秒です。このコマンドを設定する場合、デフォルトは 300 秒です。

ピア ポリシー テンプレートを使用したダイナミック低速ピアの検出

ピア ポリシー テンプレートを使用して BGP 低速ピアを検出するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **slow-peer detection** [**threshold** *seconds*]
6. **exit**
7. **address-family ipv4**
8. **neighbor** *ip-address* **inherit peer-policy** *policy-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Router(config-router)# template peer-policy global`	ポリシーテンプレート コンフィギュレーション モードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**slow-peer detection** [**threshold** *seconds*] 例： `Router(config-router-ptmp)# slow-peer detection threshold 600`	ピアが低速ピアとして判断される前に、ピア キュー内の最も古いアップデート メッセージのタイムスタンプが現在の時刻から遅延してもかまわない時間を秒単位で指定します。 • このしきい値の範囲は 120 ～ 3600 です。コマンドを設定する場合、デフォルトは 300 です。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-router-ptmp)# exit`	上位のコンフィギュレーション モードに戻ります。
ステップ 7	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例： `Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy global`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。

ピアをスタティック低速ピアとしてマークする

低速ピアを静的に設定する方法は 2 つあります。低速ピアを静的に設定するには、このセクションのいずれかのタスクを実行します。

ネイバー レベルでスタティック低速ピアとしてピアをマークする

特定のネイバー アドレスにあるか、または特定のピア グループに属するスタティック低速ピアを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4**
5. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static** 例： `Router(config-router-af)# neighbor 172.16.1.1 slow-peer split-update-group static`	指定したアドレスのネイバーを低速ピアとして設定します。 • ピアを元の低速でないアップデート グループに復元する場合は、**no neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static** コマンドを使用します。

ピア ポリシー テンプレートを使用して、スタティック低速ピアとしてピアをマークする

ピア ポリシー テンプレートを使用してスタティック低速ピアを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **slow-peer split-update-group static**
6. **exit**
7. **address-family ipv4**
8. **neighbor** *ip-address* **inherit peer-policy** *policy-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Router(config-router)# template peer-policy global`	ポリシーテンプレートコンフィギュレーションモードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**slow-peer split-update-group static** 例： `Router(config-router-ptmp)# slow-peer split-update-group static`	指定したアドレスのネイバーを低速ピアとして設定します。 • ピアを通常の状態に復元する場合は、**no slow-peer split-update-group static** コマンドを使用します。
ステップ 6	**exit** 例： `Router(config-router-ptmp)# exit`	上位のコンフィギュレーションモードに戻ります。
ステップ 7	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例： `Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy global`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。

ダイナミック低速ピア保護の設定

低速ピア保護とも呼ばれる低速ピアをダイナミックに設定する方法は 3 つあります。ダイナミック低速ピアを設定するには、このセクションの 1 つ以上のタスクを実行します。

アドレスファミリ レベルでのダイナミック低速ピアの設定

アドレスファミリ レベルでダイナミック低速ピアを設定すると、指定したアドレス ファミリのすべてのピアに適用されます（特定の低速ピアを設定する場合、ネイバー レベルで、またはピア ポリシー テンプレートを使用して次の作業を実行します）。

最後の手順は任意です。特定のピアの低速ピア保護をディセーブルにする場合にのみ実行してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4**
6. **bgp slow-peer detection** [**threshold** *seconds*]
7. **bgp slow-peer split-update-group dynamic** [**permanent**]
8. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic disable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* 例：	（任意）BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。

	コマンドまたはアクション	目的
	`Router(config-router)# neighbor 10.4.4.4 remote-as 5`	• この手順は、下の手順 8 に示すように、特定のピアのダイナミック低速ピア保護をディセーブルにする場合に必要です。
ステップ 5	**address-family ipv4** 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**bgp slow-peer detection** [**threshold** *seconds*] 例： `Router(config-router-af)# bgp slow-peer detection threshold 600`	（任意）ピアが低速ピアとして判断される前に、ピア キュー内の最も古いアップデート メッセージのタイムスタンプが現在の時刻から遅延してもかまわない時間を秒単位で指定します。 • 次の手順のように、ダイナミック低速ピアを設定すると、この検出が自動的にイネーブルになります。 • このしきい値の範囲は 120 ～ 3600 です。デフォルトは 300 です。
ステップ 7	**bgp slow-peer split-update-group dynamic** [**permanent**] 例： `Router(config-router-af)# bgp slow-peer split-update-group dynamic permanent`	ダイナミックに検出した低速ピアを低速アップデート グループに移動します。 • スタティック低速ピア アップデート グループが存在する（スタティック低速ピアのため）場合、ダイナミック低速ピアはスタティック低速ピア アップデート グループに移動されます。 • スタティック低速ピア アップデート グループが存在しない場合、新しい低速ピア アップデート グループが作成され、ピアがそのグループに移動されます。 • **permanent** キーワードを使用することをお勧めします。**permanent** キーワードを使用すると、ピアが元のアップデート グループに自動的に移動されることはありません。ネットワーク輻輳などの低速の根本的原因を特定した後は、**clear bgp slow** コマンドを使用して、ピアを元のアップデート グループに移動することができます。ダイナミック低速ピアを元のアップデート グループに戻すには、ダイナミック低速ピアを通常のピアとして回復 （887 ページ）を参照してください。

	コマンドまたはアクション	目的
		• **permanent** キーワードを使用しない場合、低速ピアが通常のピアになる（収束する）と、通常の元のアップデート グループに戻されます。
ステップ 8	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic disable** 例： `Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic disable`	（任意）特定のピアのダイナミック低速ピア保護をディセーブルにする場合にのみ、次の手順を実行します。

ネイバー レベルでのダイナミック低速ピアの設定

特定のネイバー アドレスにあるか、または特定のピア グループに属するダイナミック低速ピアを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4**
5. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection** [**threshold** *seconds*]
6. **neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic** [**permanent**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv4** 例：	アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-router)# address-family ipv4`	
ステップ 5	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer detection** [**threshold** *seconds*] 例： `Router(config-router-af)# neighbor 172.60.2.3 slow-peer detection threshold 1200`	（任意）ピアが低速ピアとして判断される前に、ピア キュー内の最も古いアップデート メッセージのタイムスタンプが現在の時刻から遅延してもかまわない時間を秒単位で指定します。 • 次の手順のように、ダイナミック低速ピアを設定すると、この検出が自動的にイネーブルになります。 • このしきい値の範囲は 120 ～ 3600 です。デフォルトは 300 です。
ステップ 6	**neighbor** {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic** [**permanent**] 例： `Router(config-router-af)# neighbor 172.60.2.3 slow-peer split-update-group dynamic permanent`	ダイナミックに検出した低速ピアを低速アップデート グループに移動します。 • スタティック低速ピア アップデート グループが存在する（スタティック低速ピアのため）場合、ダイナミック低速ピアはスタティック低速ピア アップデート グループに移動されます。 • スタティック低速ピア アップデート グループが存在しない場合、新しい低速ピア アップデート グループが作成され、ピアがそのグループに移動されます。 • **permanent** キーワードを使用することをお勧めします。**permanent** キーワードを使用すると、ピアが元のアップデート グループに自動的に移動されることはありません。ネットワーク輻輳などの低速の根本的原因を特定した後は、**clear bgp slow** コマンドを使用して、ピアを元のアップデート グループに移動することができます。ダイナミック低速ピアを元のアップデート グループに戻すには、ダイナミック低速ピアを通常のピアとして回復 （887 ページ）を参照してください。 • **permanent** キーワードを使用しない場合、低速ピアが通常のピアになる（収束する）と、通常の元のアップデート グループに戻されます。

ピア ポリシー テンプレートを使用したダイナミック低速ピアの設定

ピア ポリシー テンプレートを使用して BGP 低速ピアを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **slow-peer detection** [**threshold** *seconds*]
6. **slow-peer split-update-group dynamic** [**permanent**]
7. **exit**
8. **address-family ipv4**
9. **neighbor** *ip-address* **inherit peer-policy** *policy-template-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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 5`	BGP ルーティング プロセスを設定します。
ステップ 4	**template peer-policy** *policy-template-name* 例： `Router(config-router)# template peer-policy global`	ポリシーテンプレートコンフィギュレーションモードを開始し、ピア ポリシー テンプレートを作成します。
ステップ 5	**slow-peer detection** [**threshold** *seconds*] 例： `Router(config-router-ptmp)# slow-peer detection threshold 600`	（任意）ピアが低速ピアとして判断される前に、ピア キュー内の最も古いメッセージのタイムスタンプが現在の時刻から遅延してもかまわない時間を秒単位で指定します。

	コマンドまたはアクション	目的
		• 次の手順のように、ダイナミック低速ピアを設定すると、この検出が自動的にイネーブルになります。 • このしきい値の範囲は 120 ～ 3600 です。デフォルトは 300 です。
ステップ 6	**slow-peer split-update-group dynamic** [**permanent**] **例：** `Router(config-router-ptmp)# slow-peer split-update-group dynamic permanent`	ダイナミックに検出した低速ピアを低速アップデート グループに移動します。 • スタティック低速ピア アップデート グループが存在する（スタティック低速ピアのため）場合、ダイナミック低速ピアはスタティック低速ピア アップデート グループに移動されます。 • スタティック低速ピア アップデート グループが存在しない場合、新しい低速ピア アップデート グループが作成され、ピアがそのグループに移動されます。 • **permanent** キーワードを使用することをお勧めします。**permanent** キーワードを使用すると、ピアが元のアップデート グループに自動的に移動されることはありません。ネットワーク輻輳などの低速の根本的原因を特定した後は、コマンドを使用して、ピアを元のアップデート グループに移動することができます。ダイナミック低速ピアを元のアップデート グループに戻すには、ダイナミック低速ピアを通常のピアとして回復 （887 ページ）を参照してください。 • **permanent** キーワードを使用しない場合、低速ピアが通常のピアになる（収束する）と、通常の元のアップデート グループに戻されます。
ステップ 7	**exit** **例：** `Router(config-router-ptmp)# exit`	上位のコンフィギュレーション モードに戻ります。
ステップ 8	**address-family ipv4** **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例： `Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy global`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。

ダイナミック低速ピアに関する出力の表示

この作業では、1 つ以上の **show** コマンドを使用して、ダイナミックに設定された BGP 低速ピアに関する出力を表示します。

手順の概要

1. **enable**
2. **show ip bgp** [**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all** | **topology**{*****| *routing-topology-instance-name*}] [**update-group**] **summary slow**
3. **show ip bgp** [**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all**] **neighbors slow**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp** [**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all** | **topology**{*****| *routing-topology-instance-name*}] [**update-group**] **summary slow** 例： `Router# show ip bgp summary slow`	概要フォームにダイナミック BGP低速ピアに関する情報を表示します。
ステップ 3	**show ip bgp** [**ipv4** {**multicast** | **unicast**} | **vpnv4 all** | **vpnv6 unicast all**] **neighbors slow** 例： `Router# show ip bgp neighbors slow`	ダイナミック BGP 低速ピア ネイバーに関する情報を表示します。

ダイナミック低速ピアを通常のピアとして回復

ネットワーク管理者として、低速ピアの根本的原因（ネットワーク輻輳やレシーバが時間内にアップデートを処理していないなど）を解決したら、次の作業で **clear** コマンドを使用して、ピアを元のグループに戻します。両方のコマンドは同じ機能を実行します。

（注） 静的に設定された低速ピアは、このような **clear** コマンドによる影響を受けません。静的に設定された低速ピアを元のアップデート グループに復元するには、ピアをスタティック低速ピアとしてマークする（877 ページ）のいずれかの作業に示されているコマンドの **no** 形式を使用してください。

手順の概要

1. **enable**
2. **clear ip bgp** {[*af*] ***| *neighbor-address* | **peer-group** *group-name*} **slow**
3. **clear bgp** *af* {***| *neighbor-address* | **peer-group** *group-name*} **slow**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip bgp** {[*af*] ***| *neighbor-address*	**peer-group** *group-name*} **slow** 例： `Router# clear ip bgp * slow`	（任意）ネイバーを低速アップデート ピア グループから元のアップデート ピア グループに復元します。 • *af* は、**ipv4**、**vpnv4**、または **vpnv6** のアドレス ファミリのいずれかです。IPv4、VPNv4、または VPNv6 アドレス ファミリのすべてのピアを元のアップデート グループに戻します。 • * はすべてのピアを元のアップデート グループに戻します。
ステップ 3	**clear bgp** *af* {***| *neighbor-address*	**peer-group** *group-name*} **slow** 例： `Router# clear bgp ipv4 * slow`	（任意）ネイバーを低速アップデート ピア グループから元のアップデート ピア グループに復元します。 • *af* は、**ipv4**、**vpnv4**、または **vpnv6** のアドレス ファミリのいずれかです。IPv4、VPNv4、または VPNv6 アドレス ファミリのピアを元のアップデート グループに戻します。

	コマンドまたはアクション	目的
		• * はアドレス ファミリのすべてのピアを元のアップデート グループに戻します。

BGP 低速ピアの検出と軽減の設定例

例：スタティック低速ピア

次の例では、192.168.12.10 のネイバーをスタティック低速ピアとしてマークします。

```
router bgp 5
address-family ipv4
 neighbor 192.168.12.10 slow-peer split-update-group static
```

例：ピア ポリシー テンプレートを使用したスタティック低速ピア

次の例では、ipv4_ucast_pp2 というピア ポリシー テンプレートを使用して、スタティック低速ピアを設定します。10.0.101.4 のネイバーがポリシーを継承します。

```
router bgp 13
template peer-policy ipv4_ucast_pp2
slow-peer split-update-group static
exit-peer-policy
!
no bgp default route-target filter
no bgp enforce-first-as
bgp log-neighbor-changes
neighbor 10.0.101.4 remote-as 13
address-family ipv4
neighbor 10.0.101.4 inherit peer-policy ipv4_ucast_pp2

RouterA# show ip bgp template peer-policy ipv4_ucast_pp2

Template:ipv4_ucast_pp2, index:2.
Local policies:0x180000000, Inherited polices:0x0
Local disable policies:0x0, Inherited disable policies:0x0
Locally configured policies:
  slow-peer split-update-group static
  Inherited policies:
```

例：ネイバー レベルでのダイナミック低速ピア

次の例では、ネイバー レベルで低速ピアを設定します。10.0.101.3 のネイバーは、300 秒のデフォルトのしきい値で、ダイナミック低速ピア保護で設定されます。

```
router bgp 13
no bgp default route-target filter
no bgp enforce-first-as
```

```
bgp log-neighbor-changes
 neighbor 10.0.101.3 remote-as 13
address-family ipv4
 neighbor 10.0.101.3 slow-peer split-update-group dynamic
```

例：ピア ポリシー テンプレートを使用したダイナミック低速ピア

次の例では、ルータ A が ipv4_ucast_pp1 というピア ポリシー テンプレートを使用して、120 秒の検出しきい値を設定します。**permanent** キーワードを指定すると、ネットワーク管理者が **clear ip bgp slow** コマンドを使用してピアを元のアップデート グループに移動するまで、低速ピアが低速アップデート グループに留まります。10.0.101.2 のネイバーはピア ポリシーを継承します。これは、そのネイバーが低速であると判断された場合に、低速アップデート グループに移動されることを意味します。

```
router bgp 13
 template peer-policy ipv4_ucast_pp1
 slow-peer detection threshold 120
 slow-peer split-update-group dynamic permanent
 exit-peer-policy
!
no bgp default route-target filter
no bgp enforce-first-as
bgp log-neighbor-changes
 neighbor 10.0.101.2 remote-as 13
!
address-family ipv4
 neighbor 10.0.101.2 activate
 neighbor 10.0.101.2 inherit peer-policy ipv4_ucast_pp1
```

次の出力に、ローカルに設定されたポリシーを示します。

```
RouterA# show ip bgp template peer-policy ipv4_ucast_pp1

Template:ipv4_ucast_pp1, index:1.
Local policies:0x300000000, Inherited polices:0x0
Local disable policies:0x0, Inherited disable policies:0x0
Locally configured policies:
  slow-peer detection threshold is 120
  slow-peer split-update-group dynamic permanent
Inherited policies:
```

例：ピア グループを使用したダイナミック低速ピア

次の例では、2 つのピア グループ ipv4_ucast_pg1 と ipv4_ucast_pg2 を設定します。10.0.101.1 のネイバーは ipv4_ucast_pg1 に属し、低速ピア検出が 120 秒に設定されます。10.0.101.5 のネイバーは ipv4_ucast_pg2 に属し、低速ピア検出が 140 秒に設定されます。

```
router bgp 13
no bgp default route-target filter
no bgp enforce-first-as
bgp log-neighbor-changes
 neighbor ipv4_ucast_pg1 peer-group
 neighbor ipv4_ucast_pg2 peer-group
 neighbor ipv4_ucast_pg1 remote-as 13
 neighbor ipv4_ucast_pg2 remote-as 13
```

```
 neighbor 10.0.101.1 peer-group ipv4_ucast_pg1
 neighbor 10.0.101.5 peer-group ipv4_ucast_pg2
address-family ipv4
 neighbor ipv4_ucast_pg1 slow-peer detection threshold 120
 neighbor ipv4_ucast_pg1 slow-peer split-update-group dynamic
 neighbor ipv4_ucast_pg2 slow-peer detection threshold 140
 neighbor ipv4_ucast_pg2 slow-peer split-update-group dynamic
```

次の出力に、ピア グループ ipv4_ucast_pg1 に関する情報を示します。

```
RouterA# show ip bgp peer-group ipv4_ucast_pg1

BGP peer-group is ipv4_ucast_pg1,  remote AS 13
  BGP version 4
  Neighbor sessions:
    0 active, is multisession capable
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  BGP neighbor is ipv4_ucast_pg1, peer-group internal, members:
  10.0.101.1
  Index 0
  Slow-peer detection is enabled, threshold value is 120
  Slow-peer split-update-group dynamic is enabled
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
```

次の出力に、ピア グループ ipv4_ucast_pg2 に関する情報を示します。

```
RouterA# show ip bgp peer-group ipv4_ucast_pg2

BGP peer-group is ipv4_ucast_pg2,  remote AS 13
  BGP version 4
  Neighbor sessions:
    0 active, is multisession capable
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
  BGP neighbor is ipv4_ucast_pg2, peer-group internal, members:
  10.0.101.5
  Index 0
  Slow-peer detection is enabled, threshold value is 140
  Slow-peer split-update-group dynamic is enabled
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
MPLS レイヤ 3 VPN の設定作業	『*MPLS: Layer 3 VPNs Configuration Guide*』の「Configuring MPLS Layer 3 VPNs」モジュール

関連項目	マニュアル タイトル
ポリシーベースルーティングを使用した VRF 選択	『*MPLS: Layer 3 VPNs Configuration Guide*』の「MPLS VPN VRF Selection Using Policy-Based Routing」モジュール

標準

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

MIB

MIB	MIB のリンク
—	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

RFC

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

テクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

iBGP ローカル AS に対する BGP 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 *64 : iBGP* ローカル *AS* に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
iBGP ローカル AS に対する BGP サポート		ローカル AS に対する BGP サポート機能が提供される前は、ルートリフレクタで **neighbor local-as** コマンドを使用して、eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズしていました。現在は、**neighbor local-as** コマンドを使用して、iBGP ローカル AS セッションでの iBGP 属性（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_ID、CLUSTER_LIST）の送信を有効にすることができます。この機能は、ルートで iBGP 属性を保持することが有効な場合に、2 つの自律システムをマージするのに役立ちます。 iBGP ローカル AS に対する BGP サポート機能が提供される前は、iBGP 属性を変更するように RR を設定することはできませんでした。この機能の導入により、iBGP 属性を変更するように RR を設定できるため、柔軟性が向上します。 次のコマンドが導入されました。 • **neighbor allow-policy** 次のコマンドが変更されました。 • **neighbor local-as** • **show ip bgp vpnv4**

第 49 章

BGP：RT 制約ルート配布の設定

BGP：RT 制約ルート配布は、ルート リフレクタ（RR）からプロバイダー エッジ（PE）ルータに送信される不要なルーティング アップデートを減らすために、サービス プロバイダーがマルチプロトコル ラベル スイッチング（MPLS）レイヤ 3 VPN で使用できる機能です。ルーティング アップデートを減らすことにより、RR、自律システム境界ルータ（ASBR）、PE で伝送するルートが少なくなるため、リソースを節約できます。ルーティング アップデートを制限するためにルート ターゲットが使用されます。

- 機能情報の確認 （893 ページ）
- BGP：RT 制約ルート配布の前提条件 （894 ページ）
- BGP：RT 制約ルート配布の制限事項 （894 ページ）
- BGP に関する情報：RT 制約ルート配布 （894 ページ）
- RT 制約ルート配布の設定方法 （898 ページ）
- BGP：RT 制約ルート配布の設定例 （909 ページ）
- その他の参考資料 （911 ページ）
- BGP RT 制約ルート配布の機能情報 （913 ページ）

機能情報の確認

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

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

BGP：RT 制約ルート配布の前提条件

BGP：RT 制約ルート配布を設定する前に、次の項目を設定する方法を理解している必要があります。

- マルチプロトコル ラベル スイッチング（MPLS）VPN
- ルート識別子（RD）
- ルート ターゲット（RT）
- マルチプロトコル BGP（MBGP）

BGP：RT 制約ルート配布の制限事項

BGP：RT 制約ルート配布では、すべての VPN ルート アドバタイズメントが制限されます。

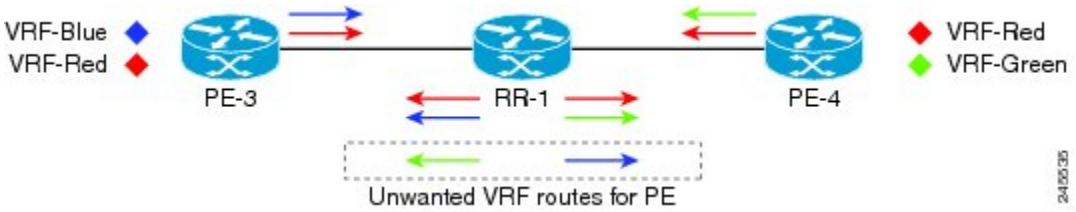
BGP に関する情報：RT 制約ルート配布

BGP：RT 制約ルート配布により解決できる問題

一部のサービス プロバイダーでは、RR から PE に大量のルーティング アップデートが送信され、大量のリソース使用が必要となることがあります。PE では、PE にない VRF のルーティング アップデートは必要ではありません。そのため、PE は受信するルーティング アップデートの大部分を「不要」であると判断します。PE はこの不要なアップデートを除外します。

下の図に、2 つの PE に不要なルーティング アップデートが送信される場合の例を示します。

図 *71 : PE* での不要なルーティング アップデート



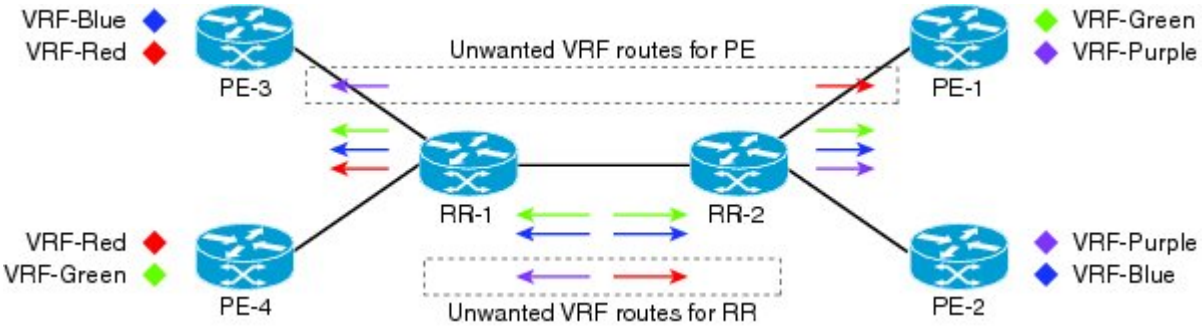
上の図に示すとおり、PE は次のように不要なルートを受信しています。

1. PE-3 は VRF Blue および VRF Red ルートを RR-1 にアドバタイズします。PE-4 は VRF Red および VRF Green ルートを RR-1 にアドバタイズします。
2. RR-1 にすべての VRF（Blue、Red、Green）に対するすべてのルートが集まります。
3. ルートの更新または VRF プロビジョニングの実行時に、RR-1 はすべての VRF ルートを PE-3 と PE-4 の両方にアドバタイズします。

4. VRF Green のルートは PE-3 では不要です。VRF Blue のルートは PE-4 では不要です。

次に、2 つの RR と、もう 1 組の PE がある場合を見てみましょう。RR から PE に不要なルーティング アップデートが送信されており、RR 間でも不要なルーティング アップデートが送信されています。下の図に、不要なルートが RR に送信される場合の例を示します。

図 *72 : RR* での不要なルーティング アップデート



上の図に示すとおり、RR-1 と RR-2 は次のように不要なルーティング アップデートを受信しています。

1. PE-3 と PE-4 は VRF Blue、VRF Red、VRF Green の各 VPN ルートを RR-1 にアドバタイズしています。
2. RR-1 はすべての VPN ルートを RR-2 に送信します。
3. PE-1 と PE-2 には VRF Red がないため、VRF Red ルートは RR-2 では不要です。
4. 同様に、PE-3 と PE-4 には VRF Purple がないため、VRF Purple ルートは RR-1 では不要です。

そのため、RR と PE の間で不要なルートが大量にアドバタイズされる可能性があります。BGP：RT 制約ルート配布機能を使用すると、不要なルーティング アップデートを除外することによりこの問題を解決できます。

BGP：RT 制約ルート配布を使用しない場合、アップデートのフィルタリングは PE が行います。この機能を使用すると、アップデートのフィルタリングは RR が行うようになります。

BGP の利点：RT 制約ルート配布

MPLS L3VPN では、PE ルータが BGP とルート ターゲット（RT）拡張コミュニティを使用して VRF との間での VPN ルートの配布を制御し、VPN を分離します。PE と自律システム境界ルータ（ASBR）では、一般に、受信した VPN ルートをフィルタ処理して、不要な VPN ルートを除外します。

ただし、不要な VPN ルートの受信とフィルタリングの処理はリソースの浪費につながります。送信元が VPN ルーティング アップデートを生成および送信して、受信側で不要なルートを除外します。VPN ルート アップデートの生成を抑えることで、リソースが節約されます。

ルート ターゲット制約（RTC）は、RR から VPN に関与していない PE に VPN ネットワーク層到達可能性情報（NLRI）が伝播されるのを防ぐメカニズムです。この機能により、CPU サイクルと一時メモリの使用量が大幅に削減されます。RT 制約により、VPN ルートの数が制限され、VPN メンバーシップが規定されます。

BGP RT-Constrain SAFI

BGP：RT 制約ルート配布機能では、BGP RT-Constrain Subsequent Address Family Identifier（SAFI）が導入されています。アドレス ファミリを入力するためのコマンドは **address-family rtfilter unicast** コマンドです。

BGP：RT 制約ルート配布の動作

「BGP：RT 制約ルート配布により解決できる問題」で説明したように不要なルートをフィルタ処理により除外するには、PE と RR に BGP：RT 制約ルート配布機能を設定する必要があります。

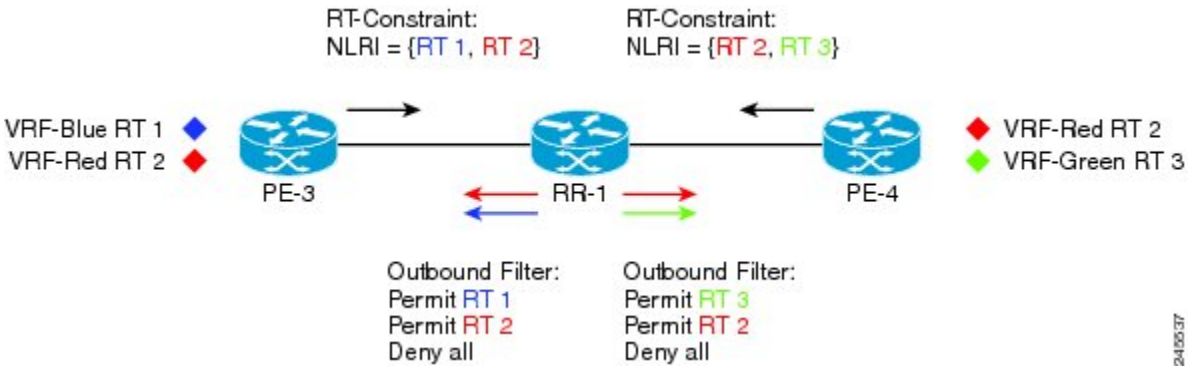
この機能により、PE は RT メンバーシップを伝播させ、その RT メンバーシップを使用して PE と RR で維持する VPN ルーティング情報を制限できるようになります。PE は MP-BGP UPDATE メッセージを使用してメンバーシップ情報を伝播させます。RR は受信した RT メンバーシップに基づいて VPN ルートのアドバタイズメントを制限します。

この機能により、次の 2 種類の情報が交換されます。

- PE は RT 制約（RTC）ネットワーク層到着可能性情報（NLRI）を RR に送信します。
- RR はアウトバウンド ルート フィルタをインストールします。

下の図に、RTC NLRI とアウトバウンド ルート フィルタの交換を示します。

図 *73 : PE と RR の間での RTC NLRI とフィルタの交換*



上の図に示されているように、PE と RR の間では次の情報交換が行われます。

1. PE-3 が RTC NLRI（RT 1、RT 2）を RR-1 に送信します。
2. PE-4 が RTC NLRI（RT 2、RT 3）を RR-1 に送信します。

3. RR-1 は NLRI をアウトバウンド ルート フィルタに変換し、このフィルタ（Permit RT 1、RT 2）を PE-3 にインストールします。
4. RR-1 は NLRI をアウトバウンド ルート フィルタに変換し、このフィルタ（Permit RT 2、RT 3）を PE-4 にインストールします。

RT 制約 NLRI プレフィックス

RT 制約 NLRI の形式は、長さが 12 バイトのプレフィックスで、次の項目で構成されています。

- 4 バイトの送信元自律システム
- 8 バイトの RT 拡張コミュニティ値

次に、RT 制約プレフィックスの例を示します。

- 65000:2:100:1
  - 送信元自律システム番号：65000
  - BGP 拡張コミュニティのタイプ コード：2
  - ルート ターゲット：100:1
- 65001:256:192.0.0.1:100
  - 送信元 ASN：65001
  - BGP 拡張コミュニティのタイプ コード：256
  - ルート ターゲット：192.0.0.1:100
- 1.10:512:1.10:2
  - 送信元 ASN は 4 バイトで一意の 1.10
  - BGP 拡張コミュニティのタイプ コード：512
  - ルート ターゲット：1.10:2

BGP 拡張コミュニティのタイプ コードの意味については、RFC 4360『*BGP Extended Communities Attribute*』を参照してください。最初に示した例では、2 は 16 進数の 0x002 に変換されます。RFC 4360 では、0x002 はタイプ コードの後に続く値が 2 オクテットの AS 固有のルート ターゲットであることを示します。

RT 制約ルート配布のプロセス

この項では、RT 制約ルート配布のプロセスを示します。この例では、PE1 に接続されている AS 100 に 2 つの CE ルータがあります。PE1 は同様に CE ルータに接続されている PE2 と通信します。PE 間にはルート リフレクタ（RR）があります。PE1 と PE2 は AS 65000 に属しています。

この機能の一般的なプロセスは次のとおりです。

1. ユーザは **address-family rtfilter unicast** コマンドを使用して、PE1 が BGP ピアをアクティブにするよう設定します。
2. たとえば、AS 65000 の PE1 に対して **route-target import 100:1** を設定します。
3. PE1 はこのコマンドを 65000:2:100:1 という RT プレフィックスに変換します。65000 はサービス プロバイダーの AS 番号、2 は BGP 拡張コミュニティのタイプ コード、100:1 は CE の RT（AS 番号および別の番号）です。
4. PE1 は RT 制約（RTC）プレフィックス 65000:2:100:1 を iBGP ピア RR にアドバタイズします。
5. RR は RTC 65000:2:100:1 を RTC RIB にインストールします。VRF にはそれぞれ独自の RIB があります。
6. また、RR は RTC 65000:2:100:1 をネイバー PE1 のアウトバウンド フィルタにインストールします。
7. RR のフィルタは RT を許可または拒否します（iBGP は 1 つの AS で動作していて、AS 番号を追跡する必要はないため、AS 番号は無視されます）。
8. RR は、そのアウトバウンド フィルタを調べて、PE1 への RT 100:1 のアウトバウンド VPN パケットを許可することを確認します。したがって、RR は、RT 100:1 の VPN アップデート パケットのみを PE1 に送信し、その他の RT の VPN アップデートを拒否します。

デフォルトの RT フィルタ

デフォルトの RT フィルタは、値が 0、長さが 0 に設定されています。デフォルトの RT フィルタは次の場合に使用されます。

- RT 値にかかわらずすべての VPN ルートをピアに送信するようにピアで指定される
- PE がすべての VPN ルートを RR にアドバタイズするように RR で要求される

デフォルトの RT フィルタを作成するには、**address-family rtfilter unicast** コマンド下で **neighbor default-originate** コマンドを設定します。RR では、このフィルタは address-family rtfilter での route-reflector-client という設定とともにデフォルトとして送られてきます。

RT 制約ルート配布の設定方法

プロバイダー エッジ（PE）ルータおよびルート リフレクタでのマルチプロトコル BGP の設定

PE ルータおよびルート リフレクタでマルチプロトコル BGP（MP-BGP）接続を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family vpnv4** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	（任意）IPv4 ユニキャスト アドレス ファミリをすべてのネイバーで無効にします。 • ネイバーを MPLS ルートだけに使用している場合は、**bgp default ipv4-unicast** コマンドを **no** 形式で使用します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* 例：	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。

	コマンドまたはアクション	目的
	`Device(config-router)# neighbor pp.0.0.1 remote-as 100`	• *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**address-family vpnv4** [**unicast**] 例： `Device(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワード（任意）は、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor pp.0.0.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor pp.0.0.1 activate`	ネイバー BGP ルータとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

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

MPLS VPN カスタマーの接続

MPLS VPN カスタマーを VPN に接続するには、次の作業を実行します。

カスタマーの接続を可能にするための PE ルータでの VRF の定義

仮想ルーティング/転送（VRF）インスタンスを定義するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • *vrf-name* 引数は、VRF に割り当てる名前です。

ステップ 4	**rd** *route-distinguisher*
	例：
	`Device(config-vrf)# rd 100:1`
		ルーティング テーブルと転送テーブルを作成します。
		• *route-distinguisher* 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。RD は、次のいずれかの形式で入力できます。
		  • 16 ビットの AS 番号:32 ビットの番号。101:3 など。
		  • 32 ビットの IP アドレス:16 ビットの番号。192.168.122.15:1 など。

	コマンドまたはアクション	目的
ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • **export** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • **both** キーワードを使用すると、ターゲット VPN 拡張コミュニティとの間でルーティング情報がインポートおよびエクスポートされます。 • *route-target-ext-community* 引数により、RT 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の RT 拡張コミュニティの VRF リストに追加されます。
ステップ 6	**import map** *route-map* 例： `Device(config-vrf)# import map vpn1-route-map`	（任意）VRF のインポート ルート マップを設定します。 • *route-map* 引数には、VRF のインポート ルート マップとして使用されるルートマップを指定します。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	（任意）終了して、グローバル コンフィギュレーション モードに戻ります。

各 VPN カスタマー用の PE ルータでの VRF インスタンスの設定

PE ルータ上のインターフェイスまたはサブインターフェイスに VRF を関連付けるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 Ethernet 5/0`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 • *type* 引数で、設定するインターフェイスのタイプを指定します。 • *number* 引数には、ポート、コネクタ、またはインターフェイス カード番号を指定します。
ステップ 4	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	指定したインターフェイスまたはサブインターフェイスに VRF を関連付けます。 • *vrf-name* 引数は、VRF に割り当てる名前です。
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）終了して、特権 EXEC モードに戻ります。

BGP を PE ルータと CE ルータ間のルーティング プロトコルに設定

BGP を使用して PE と CE の間のルーティング セッションを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf** *vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number* 例： `Device(config-router-af)# neighbor pp.0.0.1 remote-as 200`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor pp.0.0.1 activate`	ネイバーBGPルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 8	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

PE での RT 制約の設定

この作業を PE で行うと、指定したネイバーで BGP：RT 制約ルート配布が設定されます。また、RT フィルタリングが発生しているかどうかを確認することもできます（任意）。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family rtfilter unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **activate**
6. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
7. **end**
8. **show ip bgp rtfilter all**
9. **show ip bgp rtfilter all summary**
10. **show ip bgp vpnv4 all**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 1`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family rtfilter unicast** 例： `Device(config-router)# address-family rtfilter unicast`	RT フィルタ アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	指定した BGP ネイバーと自動 RT フィルタ情報を交換できるようにします。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor pp.0.0.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**end** 例： `Device(config-router-af)# end`	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	**show ip bgp rtfilter all** 例： `Device# show ip bgp rtfilter all`	（任意）すべての BGP RT フィルタ情報を表示します。
ステップ 9	**show ip bgp rtfilter all summary** 例： `Device# show ip bgp rtfilter all summary`	（任意）BGP RT フィルタのサマリー情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**show ip bgp vpnv4 all** 例： `Device# show ip bgp vpnv4 all`	（任意）BGP VPNv4 フィルタのサマリー情報を表示します。

RR での RT 制約の設定

この作業を RR で行うと、指定したネイバーで BGP：RT 制約ルート配布が設定されます。また、RT フィルタリングが発生しているか確認することもできます（任意）。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family rtfilter unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **activate**
6. **neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client**
7. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
8. **end**
9. **show ip bgp rtfilter all**
10. **show ip bgp rtfilter all summary**
11. **show ip bgp vpnv4 all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 1`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family rtfilter unicast** 例： `Device(config-router)# address-family rtfilter unicast`	RT フィルタ アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.2 activate`	指定した BGP ネイバーでの RT 制約をイネーブルにします。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 10.0.0.2 route-reflector-client`	指定した BGP ネイバーでの RT 制約で route-reflector-client 機能を有効にします。 • BGP 設定に自動的に追加されるデフォルトの「neighbor 10.0.0.2 default-originate」機能とともに、RT 制約アドレスファミリの route-reflector-client が送られてくることに注意してください。これが保持されるのは、ルートリフレクタはそのピアからすべての VPN プレフィックスを取得するためです。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor 10.0.0.2 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp rtfilter all** 例： `Device# show ip bgp rtfilter all`	（任意）すべての BGP RT フィルタ情報を表示します。
ステップ 10	**show ip bgp rtfilter all summary** 例： `Device# show ip bgp rtfilter all summary`	（任意）BGP RT フィルタのサマリー情報を表示します。

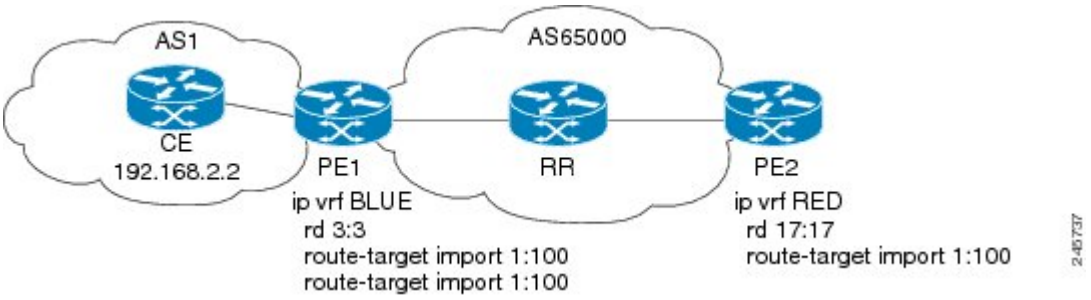
	コマンドまたはアクション	目的
ステップ 11	**show ip bgp vpnv4 all** 例： `Device# show ip bgp vpnv4 all`	（任意）BGP VPNv4 フィルタのサマリー情報を表示します。

BGP：RT 制約ルート配布の設定例

例：PE と RR の間での BGP RT 制約ルート配布

次の例は、下の図のルータの設定を示しています。PE1 と PE2 はいずれも RR に接続されていて、AS 65000 に属しています。

図 *74*：*PE* と *RR* の間での *BGP*：*RT* 制約ルート配布



PE1 の設定

```
ip vrf BLUE
 rd 3:3
 route-target export 1:100
 route-target import 1:100
!
router bgp 65000
 bgp log-neighbor-changes
 neighbor 192.168.2.2 remote-as 65000
 neighbor 192.168.2.2 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 send-community extended
 exit-address-family
 !
 address-family rtfilter unicast
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf BLUE
  redistribute static
```

```
 exit-address-family
 !
ip route vrf BLUE 51.51.51.51 255.255.255.255 Null0
!
```

RR の設定

```
!
router bgp 65000
 bgp log-neighbor-changes
 neighbor 192.168.6.6 remote-as 65000
 neighbor 192.168.6.6 update-source Loopback0
 neighbor 192.168.7.7 remote-as 65000
 neighbor 192.168.7.7 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.6.6 activate
  neighbor 192.168.6.6 send-community extended
  neighbor 192.168.6.6 route-reflector-client
  neighbor 192.168.7.7 activate
  neighbor 192.168.7.7 send-community extended
  neighbor 192.168.7.7 route-reflector-client
 exit-address-family
 !
 address-family rtfilter unicast
  neighbor 192.168.6.6 activate
  neighbor 192.168.6.6 send-community extended
  neighbor 192.168.6.6 route-reflector-client
  neighbor 192.168.6.6 default-originate
  neighbor 192.168.7.7 activate
  neighbor 192.168.7.7 send-community extended
  neighbor 192.168.7.7 route-reflector-client
  neighbor 192.168.7.7 default-originate
 exit-address-family
!
```

PE2 の設定

```
!
ip vrf RED
 rd 17:17
 route-target export 150:15
 route-target import 150:1
 route-target import 1:100
!
router bgp 65000
 bgp log-neighbor-changes
 neighbor 192.168.2.2 remote-as 65000
 neighbor 192.168.2.2 update-source Loopback0
 neighbor 192.168.2.2 weight 333
 no auto-summary
 !
 address-family vpnv4
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 send-community extended
exit-address-family
 !
 address-family rtfilter unicast
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 send-community extended
```

```
  exit-address-family
!
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BGP 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、コマンド履歴、使用上の注意事項、および例	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概要	「Cisco BGP 概要」モジュール
BGP 基本作業の設定	「基本 BGP ネットワークの設定」モジュール
BGP の基礎と説明	『*Large-Scale IP Network Solutions*』Khalid Raza、Mark Turner（Cisco Press, 2000）
拡張可能なネットワークへの BGP の実装と制御	『*Building Scalable Cisco Networks*』Catherine Paquet、Diane Teare（Cisco Press, 2001）
ドメイン間ルーティングの基本	『*Internet Routing Architectures*』Bassam Halabi（Cisco Press, 1997）

標準

標準	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB のリンク
CISCO-BGP4-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

RFC

RFC	タイトル
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2519	『*A Framework for Inter-Domain Route Aggregation*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 4271	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4684	『*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*』
RFC 4893	『*BGP Support for Four-Octet AS Number Space*』
RFC 5291	『*Outbound Route Filtering Capability for BGP-4*』
RFC 5396	『*Textual Representation of Autonomous system (AS) Numbers*』
RFC 5398	『*Autonomous System (AS) Number Reservation for Documentation Use*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

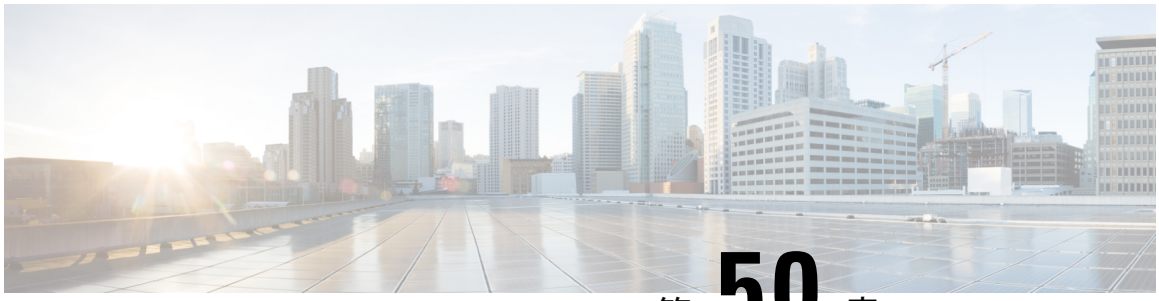
BGP RT 制約ルート配布の機能情報

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 *65 : BGP*：*RT* 制約ルート配布の機能情報

機能名	リリース	機能情報
BGP：RT 制約ルート配布	Cisco IOS XE Release 3.2S	BGP：ルート ターゲット（RT）制約ルート配布は、RR が PE に送信する不要なルーティング アップデートを減らすことによりリソースを節約するためにサービス プロバイダーが MPLS L3VPN で使用する機能です。 次のコマンドが導入されました。 • **address-family rtfilter unicast** • **show ip bgp rtfilter**



第 50 章

BGP ルーティング サーバの設定

BGP ルーティング サーバは、インターネット エクスチェンジ（IX）オペレータ向けに設計された機能で、IX に存在するサービス プロバイダー間の eBGP フル メッシュ ピアリングに代わる手段を提供します。ルーティング サーバは、サービス プロバイダーごとにカスタマイズされたポリシーをサポートする eBGP ルート リフレクションを提供します。つまり、ルーティング サーバのコンテキストによって、プレフィックスの通常の BGP ベスト パスをポリシーに基づく別のパスでオーバーライドすることや、プレフィックスのすべてのパスを抑制してプレフィックスをアドバタイズしないようにすることが可能です。BGP ルーティング サーバは、各境界ルータでの設定の複雑さや CPU およびメモリ要件を低減します。また、個別のピアリング契約によって発生するオーバーヘッド コストも削減できます。

- 機能情報の確認 （915 ページ）
- BGP ルーティング サーバに関する情報 （916 ページ）
- BGP ルーティング サーバの設定方法 （921 ページ）
- BGP ルーティング サーバの設定例 （929 ページ）
- その他の参考資料 （933 ページ）
- BGP ルーティング サーバの機能情報 （934 ページ）

機能情報の確認

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

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

BGP ルーティング サーバに関する情報

BGP ルーティング サーバにより解決できる問題

BGP ルーティング サーバによって解決される問題については、サービス プロバイダー（SP）のピアリング、およびパブリック ピアリングから生じる eBGP メッシュに関する以下の情報を確認すると理解しやすくなります。

サービス プロバイダーのプライベート ピアリングとパブリック ピアリング

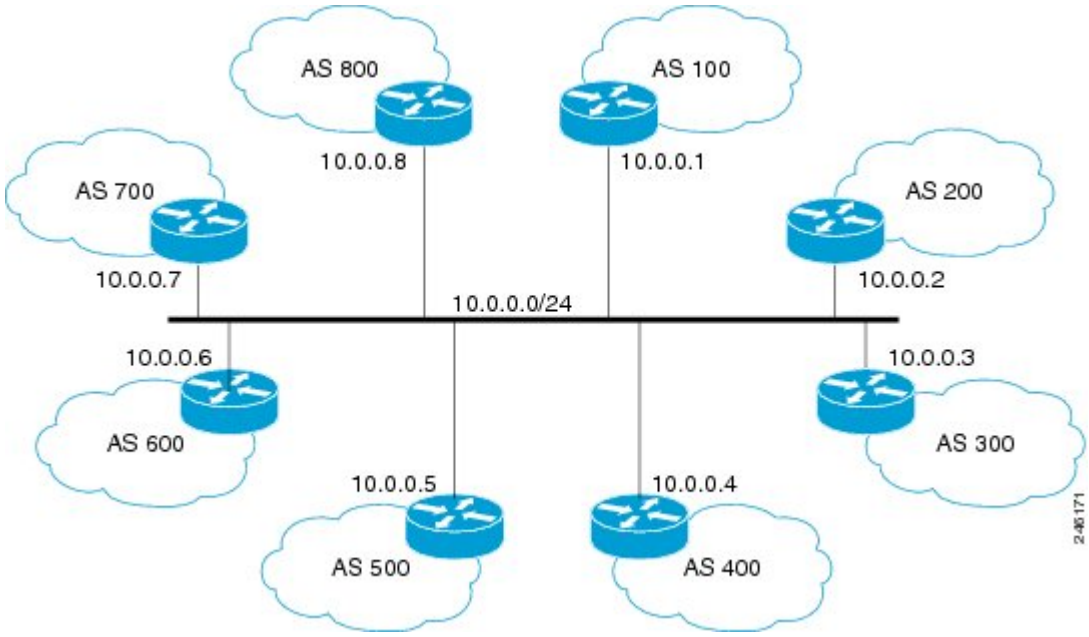
ピアリングとは、2つのサービスプロバイダー（SP）を接続して、それらの間でネットワークトラフィックを交換できるようにすることです。ピアリングはプライベートまたはパブリックのいずれかです。

- プライベート ピアリングでは、接続を必要としている 2 つの SP が、ネットワークを接続できる物理サイトを決定し、接続の取り決めの詳細を規定する契約についてネゴシエートします。この 2 つの当事者は、ピアリング接続の運用に必要な物理的スペース、ネットワーク機器、およびサービス（電気や冷却など）をすべて提供します。
- パブリック インターネット エクスチェンジ（IX）は、ネットワーク アクセス ポイント（NAP）とも呼ばれ、共有インフラストラクチャを使用して複数の SP ネットワークの相互接続を促進するために運用される物理的な場所です。IX は、ネットワーク デバイス用のラック スペース、電気、冷却、SP によるネットワークの直接接続に必要な共通のスイッチング インフラストラクチャなど、物理的な必需品を提供します。通常は 1 対 1 であるプライベート ピアリングとは異なり、IX では、エクスチェンジに存在する SP が 1 つの物理的な場所で複数のピアに接続できます。IX は、多数のプライベート ピアリング接続を維持するために必要なリソースを持たない小規模 SP に対して、プライベート ピアリングに代わる手段を提供します。

BGP を使用した IX 内での SP のパブリック ピアリング

下の図に示すように、IX 内では、各 SP は共通のスイッチング インフラストラクチャまたはサブネットに接続された BGP 境界ルータを維持します。この例では、AS 番号 100 から 800 までの 8 つの異なる SP が、10.0.0.1 から 10.0.0.8 までのアドレスが指定された BGP 境界ルータを介して 10.0.0.0/24 サブネットに接続されています。

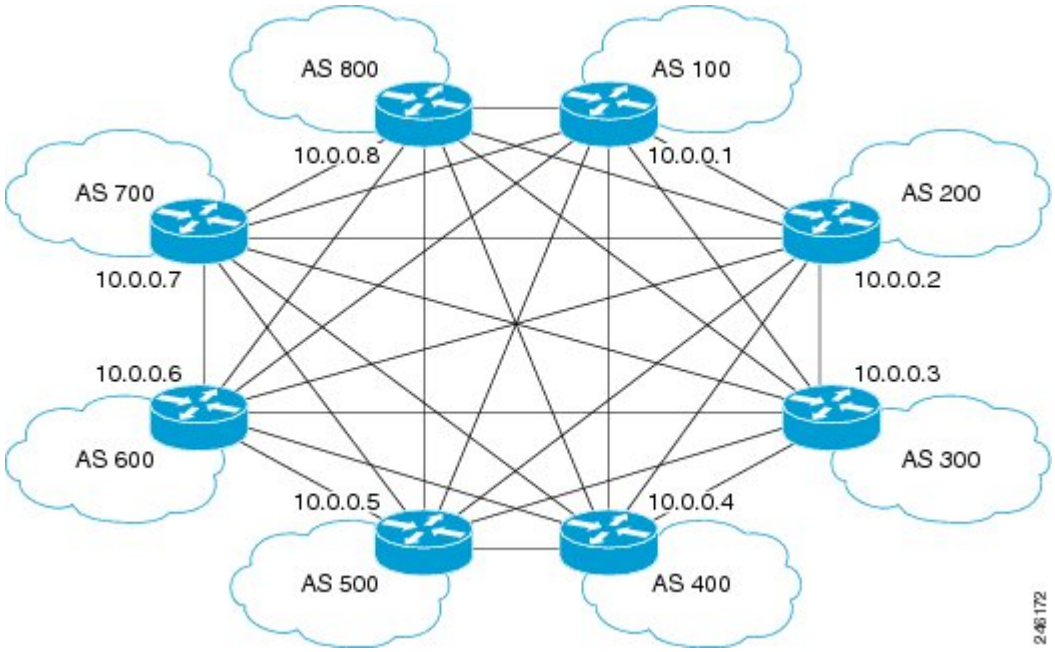
図 *75 : IX* 共有スイッチング インフラストラクチャ



各 SP の境界ルータは共有サブネットに接続されていますが、各 SP 間の BGP セッションは、特定の SP がピアリング関係を確立しようとしている他の SP ごとに、個別に設定して維持する必要があります。

各 SP が他のすべての SP に接続すると仮定した場合、結果として確立される BGP セッションのフル メッシュは、下の図のようになります。

図 *76 : IX eBGP* フル メッシュ



自律システムで必要とされる iBGP フル メッシュには SP ネットワーク内でのスケーリングや管理に関する課題が伴うのと同様に、IX でのピアリングに必要な eBGP フル メッシュは、次の理由により、eBGP に関する課題を伴います。

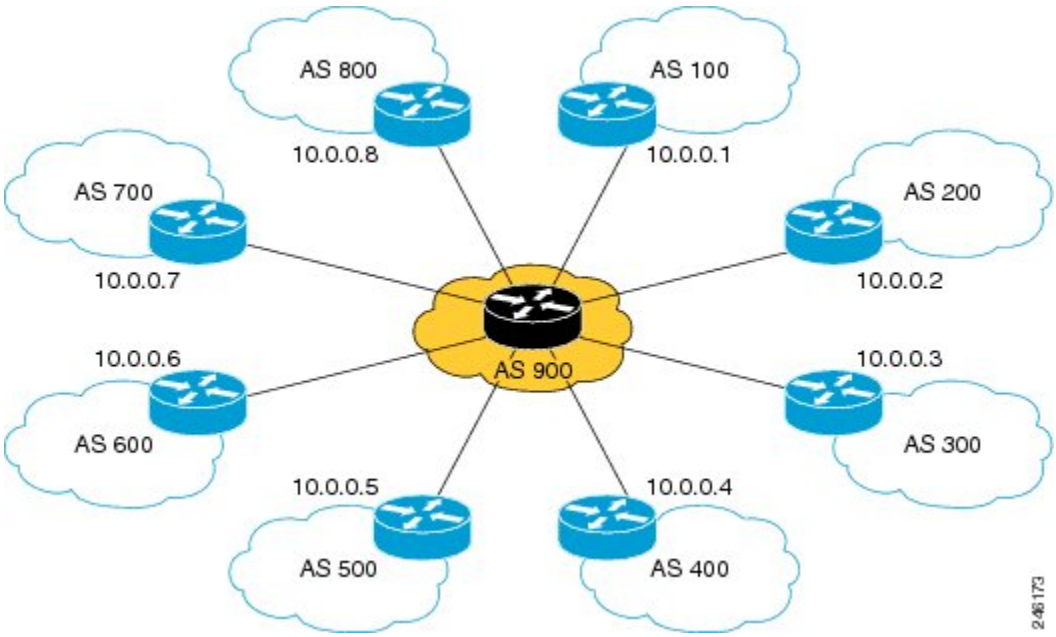
- 直接ピアリング セッションのフル メッシュでは、接続ごとに BGP セッションを設定して維持する必要があります。
- IX で特定のプロバイダーに接続する各 SP ピアとネゴシエートする必要がある契約により、運用コストが追加で発生します。

大規模なグローバル SP は世界中の数十や数百のインターネット エクスチェンジに存在する場合があり、各 IX に数十や数百のピアがある可能性があるため、小規模なプロバイダーのすべてに接続するには多大な運用コストを要します。そのため、BGP ルーティング サーバ機能を導入する前のピアリングでは、大規模なグローバル SP は、他の大規模なプロバイダーのサブセットのみに接続して、管理および運用コストを抑制することになります。直接ピアリングよりも拡張性に優れた代替手段を使用すれば、大規模なグローバル SP が小規模なプロバイダーにも接続できるようになります。

BGP ルーティング サーバによる SP 相互接続の簡素化

下の図に示すように、BGP ルーティング サーバにより、IX での SP の相互接続が簡素化されます。

図 *77 : eBGP* ルーティング サーバを使用した *IX*



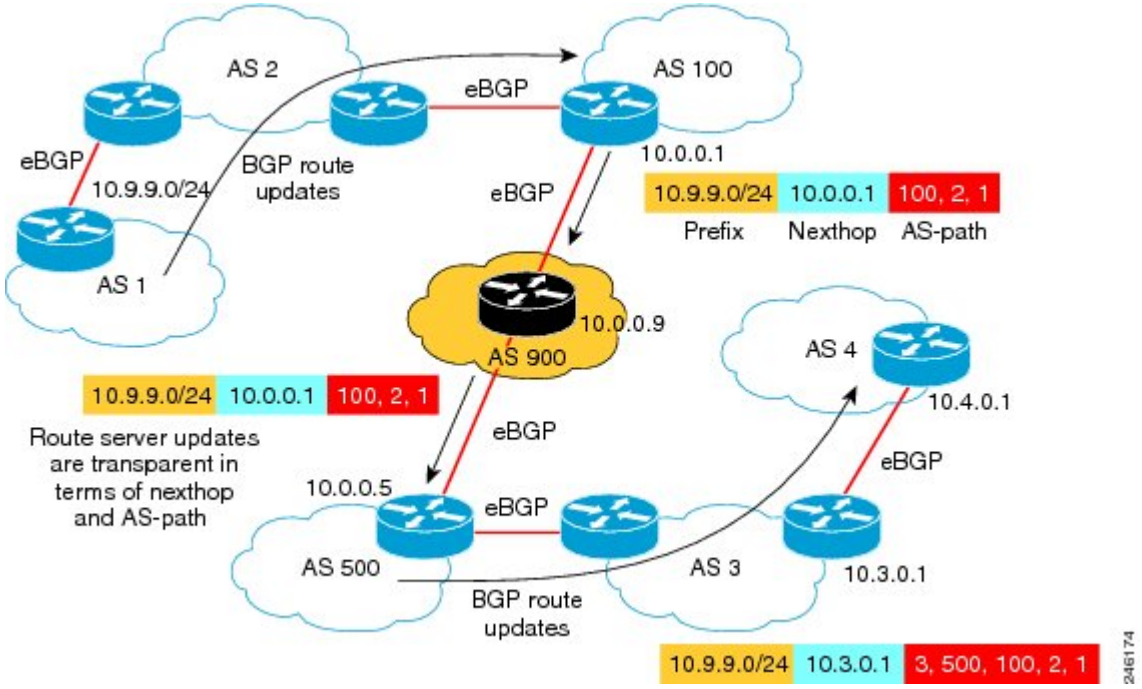
SP は、他のすべてのプロバイダーとの個別の直接 eBGP ピアリングを維持するのではなく、IX で運用されるルーティング サーバへの 1 つの接続だけを維持します。ルーティング サーバのみとのピアリングでは、各境界ルータでの設定の複雑さが軽減され、境界ルータでの CPU

およびメモリ要件が低減され、個別のピアリング契約によって発生する運用コストが大幅に抑制されます。

ルーティング サーバによってASパス、MED、およびネクストホップの透過性が提供されるため、IXでのSPのピアリングも、直接接続されているように見えます。実際には、IXルーティング サーバがこのピアリングを仲介しますが、その関係はIXの外部からは見えません。

下の図に、IX でのルーティング サーバによる透過的なルート伝播の例を示します。

図 *78 : IX* でのルーティング サーバによる透過的なルート伝播



上の図では、ルーティング アップデートはAS 1からAS 2を経由してAS 100に向かいます。アップデートは、プレフィックス10.9.9.0/24に到達し、10.0.0.1をネクスト ホップとして使用し、AS100、AS2、AS1のASパスを使用できることをアドバタイズするAS 100のルータから送出されます。

AS 900のルータはルーティング サーバであり、AS 500のルータはルーティング サーバ クライアントです。ルーティング サーバ クライアントは、ルーティング サーバからアップデートを受信します。上の図に示すように、AS 900のルータではアップデートは変更されません。ルーティング サーバ アップデートは、MED、ネクスト ホップ、およびASパスに関して透過的です。アップデートは、10.0.0.1のルータから送られてきたときと同じプレフィックス、ネクスト ホップ、およびASパスを保持してクライアントに向かいます。

BGP ルーティング サーバの利点

BGP ルーティング サーバには、次の利点があります。

- 各境界ルータでの設定の複雑さが軽減される。

- 各境界ルータでの CPU およびメモリ要件が低減される。
- 個別のピアリング契約によって発生する運用コストが削減される。
- ルーティング サーバ コンテキストによって、通常の BGP ベスト パスをポリシーに基づく代替パスでオーバーライドすることができる。
- ルーティング サーバ コンテキストによって、プレフィックスのすべてのパスを抑制してプレフィックスをアドバタイズしないようにすることができる。

ルーティング サーバ コンテキストが提供する柔軟なルーティング ポリシー

BGP ルーティング サーバは、柔軟なルーティング ポリシーを提供できます。ネットワーク環境には、カスタマイズされた（柔軟な）ポリシー処理を必要とするルートがある場合も、ない場合もあります。

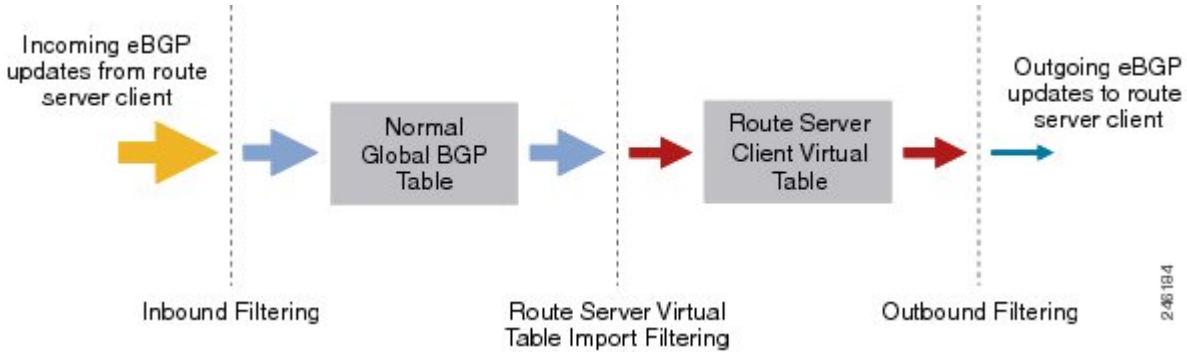
柔軟なポリシー処理を必要とするルートは、インポート マップを設定することでルーティング サーバ コンテキストにインポートするように選択されます。インポート マップは、実際のポリシーが 1 つ以上の **permit** ステートメントによって定義されるルート マップを参照します。ルート マップに一致するルート（パス）は、2 番目の「ベスト パス」計算に含まれます。結果として得られたベスト パスは、グローバルなベスト パスと異なる場合、コンテキストにインポートされます。ルーティング サーバ コンテキストに関連付けられているルーティング サーバ クライアントは、ルーティング アップデートの送信時に、コンテキストのベスト パスでグローバル ベスト パスをオーバーライドします。

複数のコンテキストを作成でき、ルーティング サーバ上で、適切なコンテキストがそのコンテキストを使用するように割り当てられたネイバーによって参照されます（ **neighbor route-server-client** コマンド）。したがって、同じポリシーを共有する複数のネイバーは、同じルーティング サーバ コンテキストを共有できます。

ルーティング サーバ クライアントでの 3 段階のフィルタリング

ルーティング サーバ コンテキストの導入により、下の図に示すように、3 段階のルート フィルタリングをルーティング サーバ クライアントに適用できるようになりました。この 3 段階のフィルタリングを下の図に示します。ルーティング サーバ クライアントに対して、3 つのフィルタリング方法のうち、すべてを適用することも、いずれも適用しないことも、任意の組み合わせを適用することもできます。図では、矢印のサイズを徐々に小さくして、ルートが、フィルタを通過するたびに、フィルタに入力されたときよりも少なくなっていることを表しています。

図 *79 : 3* 段階でのルーティング サーバ フィルタリング



1. 上の図に示されているように、一番左を起点として、着信 eBGP アップデートがルーティング サーバ クライアントから到着すると、ルーティング サーバ以外のクライアントが対象である場合と同様に、ルーティング サーバ クライアントに対するインバウンド ルート フィルタが適用されます（**neighbor route-map in** コマンドで設定）。クライアントのインバウンドフィルタリングで許可されているすべてのルートは、通常どおり、適切なアドレス ファミリのグローバル BGP テーブルにインストールされ、それ以外のルートはすべてドロップされます。
2. **import-map** コマンドを使用して、柔軟なポリシーでルーティング サーバ コンテキストが設定されている場合は、一致するルートのサブセットのうち、ベストパスがコンテキストの仮想テーブルにインポートされます。その後、コンテキストに関連付けられたルーティング サーバ クライアントは、アップデートの生成時に、コンテキストの仮想テーブルのカスタマイズされたルートでグローバル BGP テーブルのルートをオーバーライドします。
3. ルーティング サーバ クライアントのアウトバウンド フィルタリング ポリシー（**neighbor route-map out** コマンドで設定）が、カスタマイズされたポリシーを持たないグローバル アップデートに適用されます。また、アウトバウンド フィルタリング ポリシーは、ルーティング サーバ コンテキストの仮想テーブルから生成されたすべてのアップデートにも適用されます。

BGP ルーティング サーバの設定方法

基本機能を備えたルーティング サーバの設定

IPv4 または IPv6 のルーティング サーバとして BGP ルータを設定するには、この作業を実行します。この作業では、ネクストホップ、AS パス、および MED の透過性を実現するための基本的なルーティング サーバ機能を有効にします。

（注） この作業では、柔軟なポリシー処理は有効化されません。柔軟なポリシー処理を有効にするには、柔軟なポリシー処理を備えたルーティング サーバの設定（925 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ipv4-address*| *ipv6-address*} **remote-as** *remote-as-number*
5. **address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**}
6. **neighbor** {*ipv4-address*| *ipv6-address*} **activate**
7. **neighbor** {*ipv4-address*| *ipv6-address*} **route-server-client**
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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 900`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ipv4-address*| *ipv6-address*} **remote-as** *remote-as-number* 例： `Router(config-router)# neighbor 10.0.0.1 remote-as 100`	エントリを BGP ネイバー テーブルに追加します。
ステップ 5	**address-family** {**ipv4**	**ipv6**} { **unicast**	**multicast**} 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 または IPv6 ユニキャストまたはマルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ipv4-address*| *ipv6-address*} **activate** 例： `Router(config-router-af)# neighbor 10.0.0.1 activate`	BGP ネイバーとの情報交換を有効にします。
ステップ 7	**neighbor** {*ipv4-address*| *ipv6-address*} **route-server-client** 例： `Router(config-router-af)# neighbor 10.0.0.1 route-server-client`	指定されたアドレスのBGPネイバーをルーティング サーバ クライアントとして設定します。
ステップ 8	**end** 例： `Router(config-router-af)# end`	現在の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。

アップデートを受け入れるためのルーティング サーバ クライアントの設定

前の作業では、ルーティング サーバを設定しました。ルーティング サーバでは AS パスに独自の AS 番号を挿入しないため、AS パスには透過性があります。つまり、ルーティング サーバ クライアントは、AS パスの先頭にある AS 番号が送信側ルータの AS 番号ではないアップデートを受信することになります。

デフォルトでは、ルータは、着信アップデートの AS パスの先頭に自身の AS 番号を提示しない eBGP ピアから受信したアップデートを拒否します。したがって、そのようなアップデートをクライアントが受け入れるようにするには、クライアントでこの動作を無効にする必要があります。それには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no bgp enforce-first-as**
5. **neighbor** {*ipv4-address*\| *ipv6-address*} **remote-as** *remote-as-number*
6. **address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**}
7. **neighbor** {*ipv4-address*\| *ipv6-address*} **activate**
8. **exit-address-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 900`	BGP ルーティング プロセスを設定します。
ステップ 4	**no bgp enforce-first-as** 例： `Router(config-router)# no bgp enforce-first-as`	eBGP ピアから受信したアップデートでは AS_PATH の先頭にその AS 番号を示さなければならないという要件を無効にします。 • デフォルトでは、ルータは、着信アップデートの AS_PATH の先頭に自身の自律システム番号を提示しない外部 BGP（eBGP）ピアから受信したアップデートを拒否するように設定されています。 • ルーティング サーバから AS_PATH の先頭に AS 番号が示されていないアップデートを受け入れるには、 **no bgp enforce-first-as** を指定して、前述の要件の適用を無効にします。
ステップ 5	**neighbor** {*ipv4-address*| *ipv6-address*} **remote-as** *remote-as-number* 例： `Router(config-router)# neighbor 10.0.0.1 remote-as 100`	エントリを BGP ネイバー テーブルに追加します。
ステップ 6	**address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**} 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 または IPv6 ユニキャストまたはマルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** {*ipv4-address*| *ipv6-address*} **activate** 例：	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
	`Router(config-router-af)# neighbor 10.0.0.1 activate`	
ステップ 8	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了します。

柔軟なポリシー処理を備えたルーティング サーバの設定

基本的なルーティング サーバ機能に加えて、カスタマイズされた柔軟なポリシーを BGP ルーティング サーバでサポートする必要がある場合は、この作業を実行します。

柔軟なポリシー処理を設定するには、インポート マップを含むルーティング サーバ コンテキストを作成します。インポート マップは、標準のルート マップを参照します。

この特定の設定作業では、ポリシーは自律システム番号に基づくため、**match as-path** コマンドを使用します。実際の AS 番号は **ip as-path access-list** コマンドで識別されます。ネクストホップ、AS パス、コミュニティ、および拡張コミュニティでのマッチングも可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **route-server-context** *context-name*
5. **description** *string*
6. **address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**}
7. **import-map** *route-map-name*
8. **exit-address-family**
9. **exit-route-server-context**
10. **exit**
11. **ip as-path access-list** *access-list-number* {**permit**| **deny**} *regexp*
12. **route-map** *route-map-name* [**permit** | **deny**] *sequence-number*
13. **match as-path** *access-list-number*
14. **exit**
15. **router bgp** *autonomous-system-number*
16. **neighbor** {*ipv4-address*| *ipv6-address*} **remote-as** *remote-as-number*
17. **address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**}
18. **neighbor** {*ipv4-address*| *ipv6-address*} **activate**
19. **neighbor** {*ipv4-address*| *ipv6-address*} **route-server-client context** *ctx-name*
20. **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	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 900`	BGP ルーティング プロセスを設定します。
ステップ 4	**route-server-context** *context-name* 例： `Router(config-router)# route-server-context ONLY_AS27_CONTEXT`	ルーティング サーバ コンテキストを作成します。 • この例では、ONLY_AS27_CONTEXT という名前のコンテキストが作成されます。
ステップ 5	**description** *string* 例： `Router(config-router-rsctx)# description Permit only routes with AS 27 in AS path.`	（任意）コンテキストの説明を記述できます。 • 最大 80 文字まで使用できます。
ステップ 6	**address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**} 例： `Router(config-router-rsctx)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 または IPv6 ユニキャストまたはマルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**import-map** *route-map-name* 例： `Router(config-router-rsctx-af)# import-map only_AS27_routemap`	手順 12 で作成するルート マップを使用して、ルーティング サーバ クライアントの仮想テーブルに追加されるルートを制御することで、柔軟なポリシー処理を設定します。
ステップ 8	**exit-address-family** 例： `Router(config-router-rsctx-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**exit-route-server-context** 例： `Router(config-router-rsctx)# exit-route-server-context`	ルーティング サーバ コンテキスト コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 11	**ip as-path access-list** *access-list-number* {**permit**| **deny**} *regexp* 例： `Router(config)# ip as-path access-list 5 permit 27`	正規表現を使用して AS パス フィルタを設定します。 • **ip as-path** コマンドは、必ずしも使用する必要があるコマンドとは限りません。どのようなポリシーを作成するかを決定します。
ステップ 12	**route-map** *route-map-name* [**permit** | **deny**] *sequence-number* 例： `Router(config)# route-map only_AS27_routemap permit 10`	後続の **match as-path** コマンドと一致する AS パスをルート マップで許可するか拒否するかを定義します。 • 上の **import-map** コマンドで指定したものと同じ *route-map-name* を使用します。
ステップ 13	**match as-path** *access-list-number* 例： `Router(config-route-map)# match as-path 5`	どの AS パスが一致し、前の手順で設定したルート マップの一部になるかを決定するアクセス リストを識別します。 • この例では、**ip as-path access-list** コマンドで設定された *access-list-number* を参照しています。 • **match as-path** コマンドは、必ずしも使用する必要があるコマンドとは限りません。どのようなポリシーを使用するかを決定します。 • ネクストホップ、AS パス、コミュニティ、および拡張コミュニティでのマッチングも可能です。
ステップ 14	**exit** 例： `Router(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。

	コマンドまたはアクション	目的
ステップ 15	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 900`	BGP ルーティング プロセスを設定します。
ステップ 16	**neighbor** {*ipv4-address*| *ipv6-address*} **remote-as** *remote-as-number* 例： `Router(config-router)# neighbor 10.0.0.1 remote-as 500`	エントリを BGP ネイバー テーブルに追加します。
ステップ 17	**address-family** {**ipv4** | **ipv6**} { **unicast** | **multicast**} 例： `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 または IPv6 ユニキャストまたはマルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 18	**neighbor** {*ipv4-address*| *ipv6-address*} **activate** 例： `Router(config-router-af)# neighbor 10.0.0.1 activate`	BGP ネイバーとの情報交換を有効にします。
ステップ 19	**neighbor** {*ipv4-address*| *ipv6-address*} **route-server-client context** *ctx-name* 例： `Router(config-router-af)# neighbor 10.0.0.1 route-server-client context ONLY_AS27_CONTEXT`	指定されたアドレスの BGP ネイバーをルーティング サーバ クライアントとして設定します。 • この例では、指定したアドレスのルーティング サーバ クライアントが ONLY_AS27_CONTEXT というコンテキストに割り当てられます。
ステップ 20	**end** 例： `Router(config-router-af)# end`	現在の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 ルーティング サーバ情報の表示とルーティング サーバのトラブルシューティング

ルーティング サーバに関する情報を表示するには、BGP ルーティング サーバで、この作業のいずれかの手順を特権 EXEC モードから実行します。

BGP ルーティング サーバ クライアント（ルーティング サーバではなく）で、**show ip bgp ipv4 unicast** または **show ip bgp ipv6 unicast** コマンドを使用してルーティング情報を表示できます。

手順の概要

1. **enable**
2. **show ip bgp** {**ipv4** | **ipv6**} **unicast route-server** {**all** | {**context** *context-name*}} [**summary**]
3. **debug ip bgp route-server** {**client** | **context** | **event** | **import** | **policy**} [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp** {**ipv4**	**ipv6**} **unicast route-server** {**all**	{**context** *context-name*}} [**summary**] 例： `Router#`	特定のルーティング サーバ コンテキストに対して選択されたパスを表示します。これには、グローバル ベストパス、オーバーライド ポリシー パス、または抑制されたパスが含まれることがあります。
ステップ 3	**debug ip bgp route-server** {**client**	**context**	**event**	**import**	**policy**} [**detail**] 例： `Router# debug ip bgp route-server client`	BGP ルーティング サーバのデバッグをオンにします。 **注意** **detail** キーワードは、複雑な問題向けであり、シスコの担当者と連携してデバッグを行う場合にのみオンにする必要があります。

BGP ルーティング サーバの設定例

基本機能を備えた BGP ルーティング サーバの例

次の例では、10.0.0.1 のネイバーがルーティング サーバ クライアントです。

```
router bgp 65000
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.5 remote-as 500
 address-family ipv4 unicast
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 route-server-client
!
```

柔軟なポリシーの BGP ルーティング サーバ コンテキストの例（IPv4 アドレス指定）

次の例では、ローカル ルータが BGP ルーティング サーバです。10.10.10.12 と 10.10.10.13 のネイバーが、そのルーティング サーバ クライアントです。ONLY_AS27_CONTEXT という名前のルーティング サーバ コンテキストを作成し、10.10.10.13 のネイバーに適用します。このコンテキストでは、only_AS27_routemap という名前のルート マップを参照するインポート マップを使用します。このルート マップでは、アクセス リスト 27 で許可されているルートのマッチングを行います。アクセス リスト 27 は、AS パスに 27 を含むルートを許可します。

```
router bgp 65000
   route-server-context ONLY_AS27_CONTEXT
      address-family ipv4 unicast
         import-map only_AS27_routemap
      exit-address-family
   exit-route-server-context
   !
   neighbor 10.10.10.12 remote-as 12
   neighbor 10.10.10.12 description Peer12
   neighbor 10.10.10.13 remote-as 13
   neighbor 10.10.10.13 description Peer13
   neighbor 10.10.10.21 remote-as 21
   neighbor 10.10.10.27 remote-as 27
   !
   address-family ipv4
      neighbor 10.10.10.12 activate
      neighbor 10.10.10.12 route-server-client
      neighbor 10.10.10.13 activate
      neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
      neighbor 10.10.10.21 activate
      neighbor 10.10.10.27 activate
   exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
   match as-path 27
!
```

通常のベストパスがルーティング サーバ コンテキストのルートによって上書きされたことを show コマンドで確認する例

次の出力では、BGP ルーティング サーバに、最適として選択された AS 21 からのルートが 2 つあることが示されています。

```
Route-Server# show ip bgp ipv4 unicast
BGP table version is 31, local router ID is 100.100.100.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       10.10.10.21             23             0 21 ?
*                   10.10.10.27            878             0 27 89 ?
*  100.1.1.1/32     10.10.10.27            878             0 27 89 ?
*>                  10.10.10.21             23             0 21 ?
```

次の出力に示されている Peer12 については、ルーティング サーバ クライアントとして設定されていますが、どのコンテキストにも関連付けられていないため、ベストパスがアドバタイズされます。AS パス、MED、およびネクストホップの透過性が維持されていることに注意してください。ルートは、ルーティング サーバを通過していないかのように見えます。

```
Peer12# show ip bgp ipv4 unicast

BGP table version is 31, local router ID is 10.10.10.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       10.10.10.21             23             0 21 ?
*> 100.1.1.1/32     10.10.10.21             23             0 21 ?
```

Peer13 は、同様にルーティング サーバ クライアントとして設定されていますが、ONLY_AS27_CONTEXT という名前のコンテキストに関連付けられています。このコンテキストでは、AS パスに AS 27 を含むルートのみを許可するルート マップを参照しています。これは、AS 27 を含むルート以外のどのルートも、ルーティング サーバから Peer13 に送信してはならないことを意味します。このシナリオでは、AS 21 経由で学習したルートが最適としてマークされていても、実際にはルーティング サーバは AS 27 経由で学習したルートを送信します。下の出力は、ポリシーに基づくベスト パスによって通常のベスト パスがオーバーライドされたことを示しています。この場合も、MED、AS パス、およびネクストホップの透過性が維持されています。

```
Peer13# show ip bgp ipv4 unicast

BGP table version is 25, local router ID is 10.10.10.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       10.10.10.27            878             0 27 89 ?
*> 100.1.1.1/32     10.10.10.27            878             0 27 89 ?
```

ポリシーを満たすルートがない BGP ルーティング サーバ コンテキストの例

パスが存在するにもかかわらず、ポリシーにより、ルートがクライアントに送信されない場合があります。たとえば、前の例で ONLY_AS27_CONTEXT を ONLY_AS100_CONTEXT に変更すると、このポリシーを満たすパスはないため、どのルートもクライアントに送信されません。次に、この設定および結果の show 出力を示します。

```
Route-Server# show run | begin router bgp
router bgp 1
   route-server-context ONLY_AS100_CONTEXT
     !
     address-family ipv4 unicast
        import-map only_AS100_routemap
     exit-address-family
   exit-route-server-context
   !
   neighbor 10.10.10.13 remote-as 13
   neighbor 10.10.10.13 description Peer13
```

```
   neighbor 10.10.10.21 remote-as 21
   neighbor 10.10.10.27 remote-as 27
   !
      address-family ipv4
         neighbor 10.10.10.13 activate
         neighbor 10.10.10.13 route-server-client context ONLY_AS100_CONTEXT
         neighbor 10.10.10.21 activate
         neighbor 10.10.10.27 activate
   exit-address-family

!
ip as-path access-list 100 permit 100
!
!
route-map only_AS100_routemap permit 10
   match as-path 100
!
```

ポリシーを満たすルートがないため、Peer13 のテーブルにルートは 1 つも表示されません。

```
Peer13# show ip bgp ipv4 unicast
```

柔軟なポリシーの BGP ルーティング サーバ コンテキストの例（IPv6 アドレス指定）

アドレス ファミリ IPv6 での次の例では、ローカル ルータが BGP ルーティング サーバです。2001:DB8:1::112 と 2001:DB8:1::113 のネイバーは、そのルーティング サーバ クライアントです。ONLY_AS27_CONTEXT という名前のルーティング サーバ コンテキストを作成し、2001:DB8:1::113 のネイバーに適用します。このコンテキストでは、only_AS27_routemap という名前のルート マップを参照するインポート マップを使用します。このルート マップでは、アクセス リスト 27 で許可されているルートのマッチングを行います。アクセス リスト 27 は、AS パスに 27 を含むルートを許可します。

```
Route-Server# show run | begin router bgp
router bgp 1
   route-server-context ONLY_AS27_CONTEXT
      address-family ipv6 unicast
         import-map only_AS27_routemap
      exit-address-family
   exit-route-server-context
   !
   neighbor 2001:DB8:1::112 remote-as 12
   neighbor 2001:DB8:1::112 description Peer12
   neighbor 2001:DB8:1::113 remote-as 13
   neighbor 2001:DB8:1::113 description Peer13
 !
   address-family ipv6
      neighbor 2001:DB8:1::112 activate
      neighbor 2001:DB8:1::112 route-server-client
      neighbor 2001:DB8:1::113 activate
      neighbor 2001:DB8:1::113 route-server-client context ONLY_AS27_CONTEXT
 exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
   match as-path 27
```

```
!
Route-Server#show ip bgp ipv6 unicast route-server all summary

Route server clients without assigned contexts:
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:1::112 4           12      19      19        4    0    0 00:12:50        2
Route server clients assigned to context ONLY_AS27_CONTEXT:
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:1::113 4           13      23      22        4    0    0 00:16:23        2
```

Peer12 については、ルーティング サーバ クライアントとして設定されていますが、どのコンテキストにも関連付けられていないため、ベストパスがアドバタイズされます。AS パス、MED、およびネクストホップの透過性が維持されていることに注意してください。ルートは、ルーティング サーバを通過していないかのように見えます。

```
Peer12# show ip bgp ipv6 unicast
BGP table version is 9, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
* 2001:DB8:1::/64  2001:DB8::113            0             0 13 ?
*>                  ::                      0         32768 ?
* 2001:DB8:2::/64  2001:DB8::113            0             0 13 ?
*>                  ::                      0         32768 ?
```

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』
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP 設定作業	『*IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S*』

MIB

MIB	MIB のリンク
-	• 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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

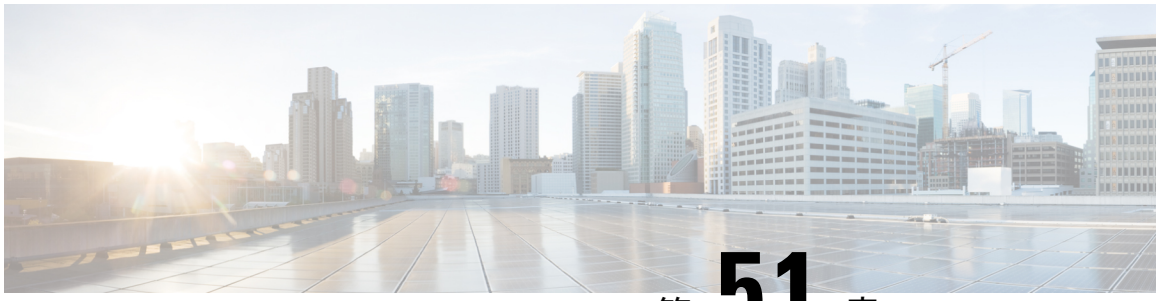
BGP ルーティング サーバの機能情報

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 *66 : BGP* ルーティング サーバの機能情報

機能名	リリース	機能情報
BGP ルーティング サーバ	Cisco IOS XE リリース 3.3S 15.2(3)T	BGP ルーティング サーバは、インターネット エクスチェンジ（IX）オペレータ向けに設計された機能で、IX に存在するサービス プロバイダー間の eBGP フル メッシュ ピアリングに代わる手段を提供します。ルーティング サーバは、サービス プロバイダーごとにカスタマイズされたポリシーをサポートする eBGP ルート リフレクションを提供します。つまり、ルーティング サーバのコンテキストによって、プレフィックスの通常の BGP ベスト パスをポリシーに基づく別のパスでオーバーライドすることや、プレフィックスのすべてのパスを抑制してプレフィックスをアドバタイズしないようにすることが可能です。BGP ルーティング サーバは、各境界ルータでの設定の複雑さや CPU およびメモリ要件を低減します。また、個別のピアリング契約によって発生するオーバーヘッド コストも削減できます。 次のコマンドが導入されました。 • **debug ip bgp route-server** • **description** （ルーティング サーバ コンテキスト） • **exit-route-server-context** • **import-map** • **neighbor route-server-client** • **route-server-context** • **show ip bgp unicast route-server**



第 51 章

ダイバースパス ルート リフレクタを使用した BGP ダイバース パス

ダイバースパス ルート リフレクタを使用した BGP ダイバース パス機能により、ボーダー ゲートウェイ プロトコル（BGP）では、ルート リフレクタが展開されている場合に BGP スピーカー間のベスト パス以外の代替パスを配布できます。この機能は、自律システム（AS）において、単一クラスタ内のみでのパスの多様性を実現することを目的としています。つまり、ルート リフレクタは、そのクライアント ピアに対してのみダイバース パスをアドバタイズできます。

- 機能情報の確認 （937 ページ）
- ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの前提条件 （938 ページ）
- ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの制約事項 （938 ページ）
- ダイバースパス リフレクタを使用した BGP ダイバース パスに関する情報 （938 ページ）
- BGP ダイバースパス ルート リフレクタの設定方法 （942 ページ）
- ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの設定例 （945 ページ）
- その他の参考資料 （948 ページ）
- ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの機能情報 （949 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、ソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの前提条件

BGP 最良外部機能について理解する必要があります。

ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの制約事項

- ダイバース パスはルート リフレクタでのみ設定できます。
- 既存のルート リフレクタごとに、追加のベスト パス（2 番目に適したパス）を 1 つ計算するシャドウ ルート リフレクタを 1 つだけ使用できます。つまり、追加のプレーン（トポロジ）は 1 つしか設定されません。
- パスの多様性は、AS において、単一のルート リフレクタ クラスタ内で設定されます。つまり、ルート リフレクタは、そのルート リフレクタ クライアント ピアに対してのみダイバース パスをアドバタイズします。
- ダイバース パス機能はルーティング サーバではサポートされていません。

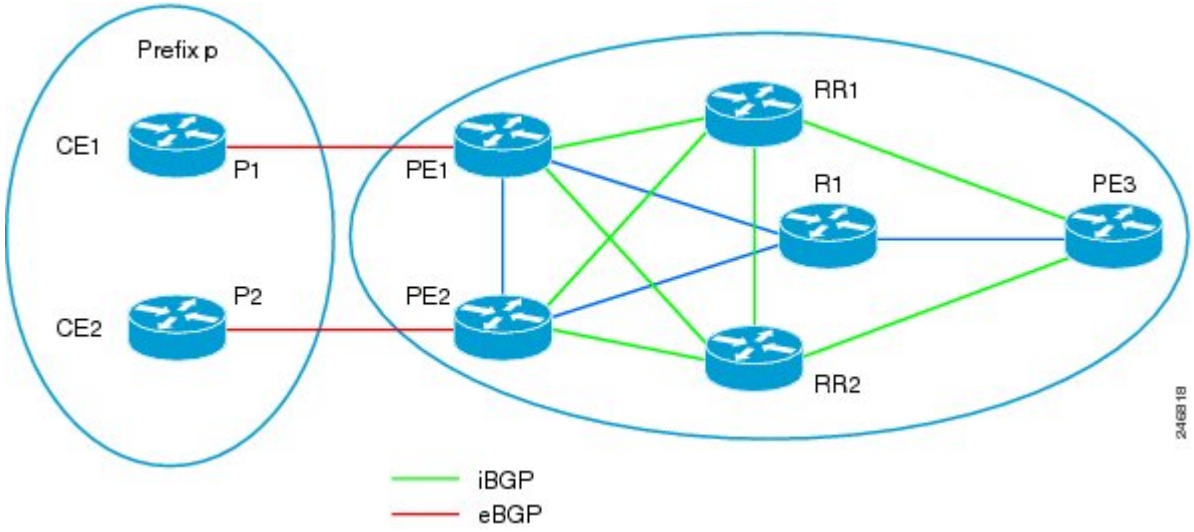
ダイバースパス リフレクタを使用した BGP ダイバース パスに関する情報

BGP ダイバース パスによって解消される制限

パス ベクター ルーティング プロトコルである BGP-4 では、ルータは、そのネイバーに対してのみ宛先のベストパスをアドバタイズする必要があります。ただし、同じ宛先へのパスを複数確保することによって、復元力の向上、障害からの迅速な回復、負荷の分散などを可能にするメカニズムを実現できます。

ルート リフレクタの使用は、自律システム（AS）内でパスの多様性が低くなる主な理由の 1 つです。ルート リフレクタを使用するネットワークでは、ルート リフレクタは、複数の出力ルータからプレフィックスを学習している場合でも、ベストパスのみをクライアントに反映します。下の図は、ルート リフレクタを展開すると、BGP 最良外部機能が展開されていたとしても、AS でパスの多様性が低下する場合があることを示しています。

ダイバースパス ルート リフレクタを使用した BGP ダイバース パス



上の図では、P1 と P2 はプレフィックス p のダイバース パスです。パス 2（P2）は P1 よりも MED が低く、ローカル プリファレンスが高いと仮定します。PE1 の BGP 最良外部機能は、P2 の方が MED が低くローカル プリファレンスが高いということに関係なく、P1 がルート リフレクタに伝播されるようにします。ルート リフレクタにはパスの多様性があります。ルート リフレクタは、それぞれ異なる出力点 PE1、PE2 を持つ P1 と P2 の両方を学習します（PE1 と PE2 で **set ip next-hop self** コマンドが設定されていると仮定）。ただし、両方のルート リフレクタは、MED がより低く、ローカル プリファレンスがより高い P2 をベスト パスとして選択し、PE3 にアドバタイズします。PE3 は P1 を学習しません（つまり、PE3 は既存のパスの多様性に関して学習しません）。

ダイバースパス ルート リフレクタを使用した BGP ダイバース パス機能は、その制限を解消し、パスの多様性を実現する方法です。

ダイバースパス ルート リフレクタを使用した BGP ダイバース パス

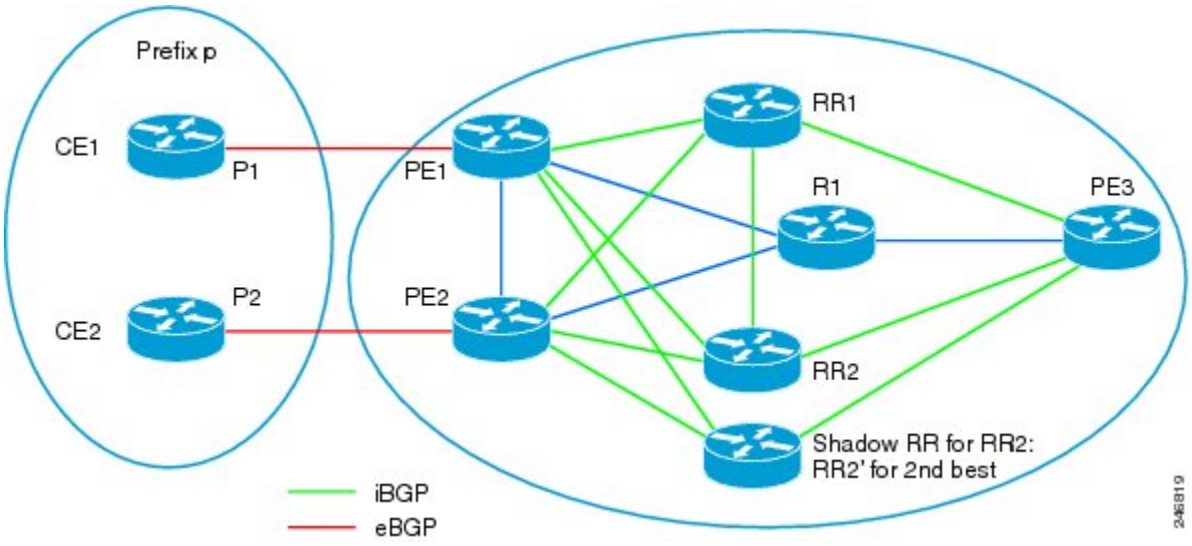
ダイバースパス ルート リフレクタを使用した BGP ダイバース パス機能は、ルート リフレクタを含む AS でのパス多様性の欠如を解決します。この機能は、AS において、単一クラスタ内のみでのパスの多様性を実現することを目的としています。つまり、ルート リフレクタは、そのクライアント ピアに対してのみダイバース パスをアドバタイズできます。

AS 内のルート リフレクタごとに、*2* 番目に適したパス（ダイバース パスとも呼ばれる）を配布するために、シャドウ ルート リフレクタが追加されます。下の図に、RR2 のシャドウ ルート リフレクタを示します。このシャドウ ルート リフレクタにより、PE3 は P1（RR1/RR2 から）と P2（シャドウ ルート リフレクタから）の両方を学習できるようになるため、パスの多様性が向上します。

（注） プライマリ ルート リフレクタとシャドウ ルート リフレクタは、ネットワーク内のその他のルータに対するまったく同じ接続（物理的/コントロール プレーン）を備えている必要があります。

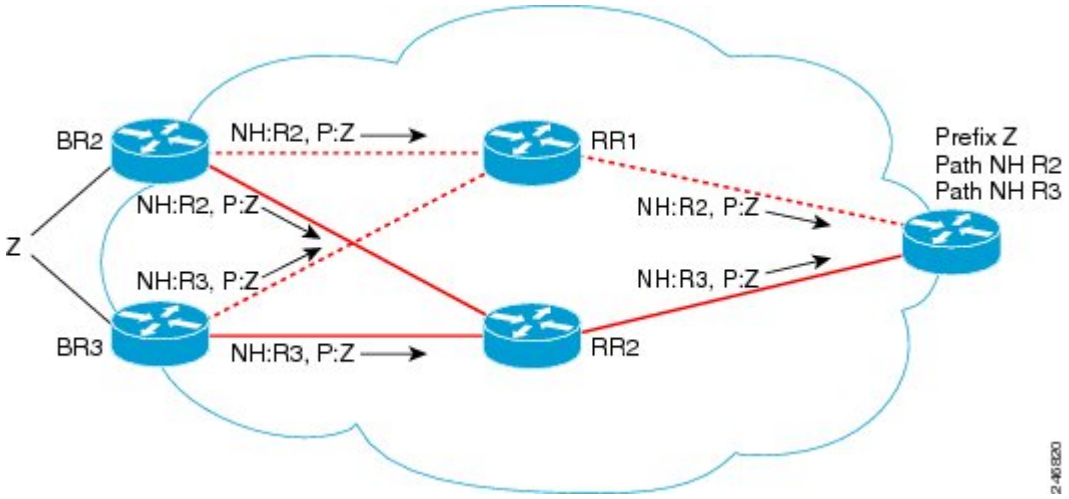
ダイバースパス ルート リフレクタを使用した BGP ダイバース パス

シャドウ ルート リフレクタは、コントロール プレーン ルート リフレクタにすることも、データ プレーン ルート リフレクタにすることもできます。



下の図は、ダイバース パスの詳細であり、ネクスト ホップを示しています。

- BR2 は、プレフィックス Z に到達する必要がある場合のネクスト ホップは R2（BR2）であることを RR1 とシャドー RR2 に通知します。同様に、BR3 は、プレフィックス Z に到達する必要がある場合のネクスト ホップは R3（BR3）であることを RR1 とシャドー RR2 に通知します。
- RR1 は、BR1 がプレフィックス Z に到達しようとしている場合に、ネクスト ホップは R2 であることを通知するパケットを BR1 に送信します。2 番目に適したパス（またはダイバース パス）がシャドウ RR2 から取得され、RR2 は、BR1 がプレフィックス Z に到達しようとしている場合に、ネクスト ホップは R3 であることを通知するパケットを BR1 に送信します。
- BR1（右端）では、プレフィックス Z に対する 2 つの（ダイバース）パスがあることを確認できます。



BGP ダイバース パスを計算するためのトリガー

アドレスファミリごとのダイバースパスの計算は、次のコマンドのいずれかによってトリガーされます。

- **bgp additional-paths install**
- **bgp additional-paths select**
- **maximum-paths ebgp**
- **maximum-paths ibgp**

bgp additional-paths install コマンドは、**bgp additional-paths select** コマンドで指定されたタイプのパスをインストールします。**bgp additional-paths select** コマンドで両方のキーワード オプション（**best-external** と **backup**）が指定されている場合は、バックアップ パスがインストールされます。

maximum-paths ebgp および **maximum-paths ibgp** コマンドによってマルチパスの計算がトリガーされ、マルチパスがプライマリ パスとして自動的にインストールされます。

一方、**bgp additional-paths install** コマンドは、バックアップ パスまたはベスト外部パスの計算をトリガーします。

bgp additional-paths select コマンドが設定されていない場合は、**bgp additional-paths install** コマンドにより、（BGP PIC 機能で行われる場合と同様に）バックアップ パスの計算とインストールがトリガーされます。

IGP メトリック チェック

内部ゲートウェイ プロトコル（IGP）メトリック チェックの無効化と BGP ダイバース パス機能の設定は互いに独立しています。依存関係はありません。つまり、**bgp bestpath igp-metric ignore** を設定しても、BGP ダイバース パス機能が有効になることはありません。逆に、BGP ダイバース パス機能を有効にする場合に、**bgp bestpath igp-metric ignore** を設定する必要があ

るとは限りません（ルート リフレクタとシャドウ ルート リフレクタが同じ場所に配置されている場合など）。

bgp bestpath igp-metric ignore コマンドは、ルート リフレクタおよびプロバイダー エッジ（PE）で設定できます。

（注） **bgp bestpath igp-metric ignore** コマンドの VRF 単位機能はサポートされていません。使用する場合は、自己の責任において行ってください。

ルート リフレクタの決定

ルータの設定に次のいずれかのコマンドが含まれている場合、そのルータはルート リフレクタになります。

- **bgp cluster-id**
- **neighbor route-reflector-client**

BGP ダイバースパス ルート リフレクタの設定方法

IGP メトリック チェックの無効化が必要かどうかの判断

BGP ダイバース パスを取得するためにシャドウ ルート リフレクタを設定する前に、IGP メトリック チェックを無効にする必要があるかどうかを判断します。IGP メトリックは、物理的距離を示す設定可能な値であり、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などの内部ゲートウェイ プロトコルで使用されます。より小さい IGP メトリックは、より大きな IGP メトリックよりも優先されます。

次のように、ルート リフレクタとシャドウ ルート リフレクタの位置によって、IGP メトリック チェックを無効にする必要があるかどうかが決まります。

- ルート リフレクタとシャドウ ルート リフレクタが同じ場所に配置されている場合：ルート リフレクタは、同じ IP サブネットワーク アドレスを持ち、異なるリンクでイーサネット スイッチに接続されます。このリンクで障害が発生すると、ルート リフレクタがダウンすることになります。RR が同じ場所に配置されている場合、それらの IGP メトリックは同じでなければなりません。したがって、ルート リフレクタでのベスト パス計算時の IGP メトリック チェックを無効にする必要はありません。IGP メトリック チェックを無効にする必要がないため、最初のプレーン ルート リフレクタを Cisco IOS XE Release 3.4S にアップグレードする必要はありません。
- シャドウ ルート リフレクタがルート リフレクタとは異なる IGP の場所にある場合（ベストパス ルート リフレクタと同じ場所に配置されていない場合）：この場合、IGP メトリック チェックは、ベスト パスと 2 番目に適したパスの計算時にベスト パス ルート リフレク

タでもシャドウ ルート リフレクタでも無視されます。**bgp bestpath igp-metric ignore** コマンドを設定して、プライマリ ルート リフレクタで IGP メトリック チェックを無効にする必要があります。このコマンドは Cisco IOS XE Release 3.4S 以降で使用可能であるため、該当のリリースにアップグレードする必要があります。

BGP ダイバース パス用のルート リフレクタの設定

BGP ダイバース パス機能用にルート リフレクタを設定するには、この作業を実行します。この作業では IPv4 アドレス ファミリを指定しますが、その他のアドレス ファミリもサポートされています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4 unicast**
6. **neighbor** *ip-address* **activate**
7. **maximum-paths ibgp** *number-of-paths*
8. **bgp bestpath igp-metric ignore**
9. **bgp additional-paths select** [**backup**]
10. **bgp additional-paths install**
11. **neighbor** *ip-address* **route-reflector-client**
12. **neighbor** *ip-address* **advertise diverse-path** [**backup**] [**mpath**]
13. **end**
14. **show ip bgp neighbor** *ip-address* **advertised-routes**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 1`	BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.1.1.1 remote-as 1`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 5	**address-family ipv4 unicast** 例： `Device(config-router)# address-family ipv4 unicast`	アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • サポートされているアドレスファミリは、IPv4 ユニキャスト、VPNv4 ユニキャスト、IPv6 ユニキャスト、VPNv6 ユニキャスト、IPv4+ラベル、IPv6+ラベルです。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 10.1.1.1 activate`	BGP ネイバーとの情報交換を有効にします。
ステップ 7	**maximum-paths ibgp** *number-of-paths* 例： `Device(config-router-af)# maximum-paths ibgp 4`	ルーティング テーブルにインストールできる並列内部 BGP（iBGP）ルートの最大数を制御します。
ステップ 8	**bgp bestpath igp-metric ignore** 例： `Device(config-router-af)# bgp bestpath igp-metric ignore`	BGP ベスト パス選択時に内部ゲートウェイ プロトコル（IGP）メトリックを無視するようにシステムを設定します。
ステップ 9	**bgp additional-paths select** [**backup**] 例： `Device(config-router-af)# bgp additional-paths select backup`	2 番目の BGP ベスト パスを計算するようにシステムを設定します。
ステップ 10	**bgp additional-paths install** 例： `Device(config-router-af)# bgp additional-paths install`	BGP で特定のアドレス ファミリのバックアップ パスを計算し、ルーティング情報ベース（RIB）および Cisco Express Forwarding（CEF）にインストールできるようにします。

	コマンドまたはアクション	目的
ステップ 11	**neighbor** *ip-address* **route-reflector-client** 例： `Device(config-router-af)# neighbor 10.1.1.1 route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 12	**neighbor** *ip-address* **advertise diverse-path** [**backup**] [**mpath**] 例： `Device(config-router-af)# neighbor 10.1.1.1 advertise diverse-path backup`	（任意）アドバタイズでダイバース パスを受信するようにネイバーを設定します。
ステップ 13	**end** 例： `Device(config-router-af)# end`	（任意）アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp neighbor** *ip-address* **advertised-routes** 例： `Device# show ip bgp neighbor 10.1.1.1 advertised-routes`	（任意）指定したネイバーにアドバタイズされたルートを表示します。

ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの設定例

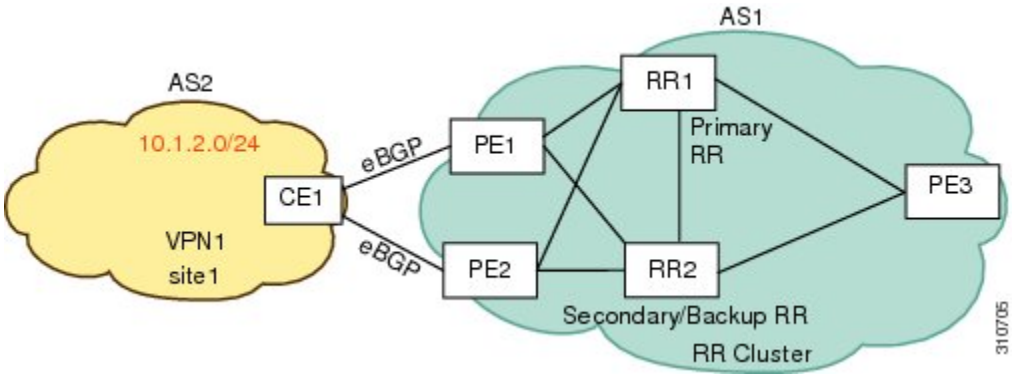
例：追加パスがバックアップ パスである BGP ダイバース パスの設定

ダイバース パス機能は単一のクラスタ内に含まれます。つまり、ダイバース パスのアドバタイズ対象として設定できるのは、ルート リフレクタのクライアントだけです。ダイバース パスは、ルートリフレクタのクライアントのみにアドバタイズされます。また、そのクライアントは追加パスを取得するように設定されている必要もあります。

追加パスを計算してアドバタイズするシャドウ ルート リフレクタを追加することも、追加パスを計算してアドバタイズするように既存のルートリフレクタを設定することもできます。下の図では、シャドウ ルート リフレクタを追加するのではなく、追加パスを計算して特定のネイバーにアドバタイズするように RR2（既存のバックアップ RR）を設定しています。

下の図では、ルート リフレクタから CE1 への PE1 経由のパスが PE2 経由のパスよりも優先されると仮定しています。ダイバース パス機能がない場合、両方のルート リフレクタが、CE1 へのパスは PE1 経由であることを PE3 にアドバタイズします。RR1 と PE1 の間の接続で障害

が発生した場合（または PE1 と CE1 の間のパスで障害が発生した場合）、他のパスはありません。



上の図に基づく次の設定例では、追加パス（バックアップ パス）を使用して RR2 が設定されています。

RR1 と RR2 が同じ場所に配置されていない場合は、追加パスを計算する前に **bgp bestpath igp-metric ignore** コマンドを設定する必要があります（RR1 と RR2 が同じ場所に配置されている場合は、このコマンドを設定しないでください）。

bgp additional-paths select backup コマンドは、バックアップ パス（PE2 経由のパス）の計算を RR2 でトリガーします。

RR2 がフォワーディング プレーンにある場合は、**bgp additional-paths install** コマンドによってバックアップ パスがインストールされます（RR2 がコントロール プレーンにある場合は、このコマンドを設定しないでください）。

PE3 のアドレスは 10.1.1.1 で、このアドレスが RR2 の **neighbor advertise diverse-path backup** コマンドで使用されます。このコマンドは、PE3 へのバックアップ パスのアドバタイズをトリガーします。PE3 は、RR1 からベスト パス（PE1 経由のパス）を学習し、RR2 からバックアップ パスを学習します。

RR2

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 advertise diverse-path backup
```

例：追加パスがマルチパスである BGP ダイバース パスの設定

上の図に基づく次の例では、PE1 および PE2 経由の CE1 へのパスがマルチパスであると仮定しています。**maximum-paths ibgp** コマンドはマルチパスの計算をトリガーします。

PE3 のアドレスは 10.1.1.1 で、このアドレスが RR2 の **neighbor advertise diverse-path mpath** コマンドで使用されます。このコマンドは、PE3 へのマルチパス、つまり 2 番目に適したパスのアドバタイズをトリガーします。PE3 は、RR1 からベスト パス（PE1 経由のパス）を学習し、RR2 から 2 番目に適したパスを学習します。

RR2

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 advertise diverse-path mpath
```

例：マルチパスとバックアップ パスの計算がトリガーされる BGP ダイバース パスの設定

次の例は、上の図に基づいています。**maximum-paths ibgp** コマンドはマルチパスの計算をトリガーします。マルチパスとバックアップ パスの計算がトリガーされると、バックアップ パスと 2 番目のマルチパス（2 番目に適したパス）は同じパスになり、ルート リフレクタがコントロール プレーンにあるかフォワーディング プレーンにあるかにかかわらず、そのパスがアクティブ パスとしてインストールされます。

PE3 のアドレスは 10.1.1.1 で、このアドレスが RR2 の **neighbor advertise diverse-path backup mpath** コマンドで使用されます。このコマンドにより、RR2 は 2 番目に適したパス（2 番目のマルチパス）を PE3 にアドバタイズします。

RR2

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp additional-paths select backup
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 advertise diverse-path backup mpath
```

例：バックアップパスの計算とインストールをトリガーするための設定

bgp additional-paths select backup を設定せずに **bgp additional-paths install** コマンドを設定すると、後者のコマンドにより、（既存の BGP PIC 機能の場合と同様に）バックアップ パスの計算とインストールがトリガーされます。

PE3 のアドレスは 10.1.1.1 で、このアドレスが RR2 の **neighbor advertise diverse-path backup** コマンドで使用されます。このコマンドは、PE3 へのバックアップ パスのアドバタイズをトリガーします。PE3 は、RR1 からベスト パス（PE1 経由のパス）を学習し、RR2 からバックアップ パスを学習します。

RR2

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp additional-paths install
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 advertise diverse-path backup
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
クラスタ間のルート リフレクタでの BGP ベスト外部パスの設定	「BGP 最良外部」モジュール
BGP 設定作業	Cisco IOS XE IP Routing: BGP Configuration Guide

標準

標準	タイトル
draft-ietf-grow-diverse-bgp-path-dist-02	*Distribution of Diverse BGP Paths*

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

RFC

RFC	タイトル
RFC 4271	『A Border Gateway Protocol 4 (BGP-4)』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

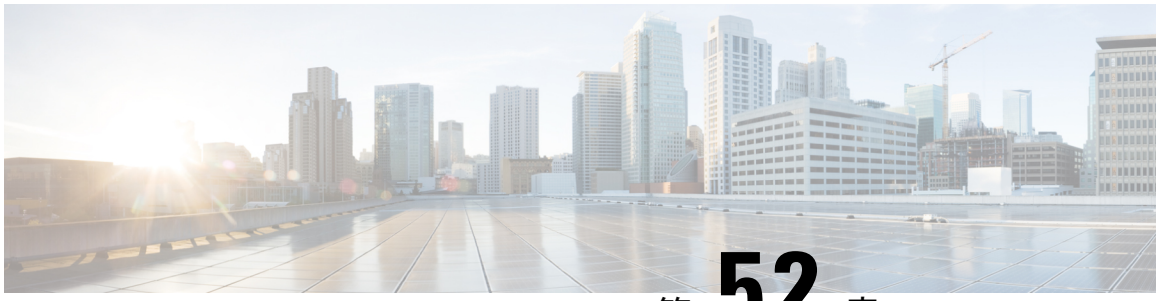
ダイバースパス ルート リフレクタを使用した BGP ダイバース パスの機能情報

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 *67 :* ダイバースパス ルート リフレクタを使用した *BGP* ダイバース パスの機能情報

機能名	リリース	機能情報
ダイバースパス ルート リフレクタを使用した BGP ダイバース パス		この機能により、BGP では、ルート リフレクタが展開されている場合に BGP スピーカー間のベスト パス以外の代替パスを配布できます。 次のコマンドが導入されました。 • **bgp additional-paths select** • **bgp bestpath igp-metric ignore** • **debug ip bgp igp-metric ignore** • **neighbor advertise best-external** • **neighbor advertise diverse-path**



第 52 章

BGP 拡張ルート リフレッシュ

BGP 拡張ルート リフレッシュ機能は、ボーダー ゲートウェイ プロトコル（BGP）でルートの不整合を検出し、万一不整合があった場合には、ハード リセットなしに BGP ピアを同期する方法を提供します。この機能はデフォルトで有効になっています。オプションのタイマーが 2 つあります。

- 機能情報の確認 （951 ページ）
- BGP 拡張ルート リフレッシュに関する情報 （951 ページ）
- BGP 拡張ルート リフレッシュのタイマーの設定方法 （953 ページ）
- BGP 拡張ルート リフレッシュの設定例 （954 ページ）
- その他の参考資料 （954 ページ）
- BGP 拡張ルート リフレッシュの機能情報 （955 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、BGP 拡張ルート リフレッシュの機能情報 （955 ページ） 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

BGP 拡張ルート リフレッシュに関する情報

BGP 拡張ルート リフレッシュ機能

セッションの確立時、BGP ピアは、BGP 拡張ルート リフレッシュ機能を実行するための機能を互いに交換します。この機能は、デフォルトでイネーブルに設定されています。

ピアが互いに不整合になることは想定されていません。これは非常にまれな状況でのみ発生する可能性があり、発生した場合には、この機能により、不整合を特定し、ハードリセットなしにピアを同期できます。

2 つのピアが拡張ルート リフレッシュに対応している場合、各ピアは、Adj-RIB-Out をアドバタイズする前に Route-Refresh Start-of-RIB（SOR）メッセージを生成し、Adj-RIB-Out をアドバタイズした後に Route-Refresh End-of-RIB（EOR）メッセージを生成します。ピアから EOR メッセージを受信した BGP スピーカーは、ピアによるルート リフレッシュ応答の一部として再アドバタイズされなかったルートを削除します。

万一、EOR メッセージの受信後または EOR タイマーの期限切れ後に失効ルートがルータに残っていた場合は、ピア同士の一貫性がなかったことを意味します。この情報を使用すると、ルートの一貫性が確保されているかどうかを確認できます。

BGP 拡張ルート リフレッシュ タイマー

通常の状況では、これらのタイマーを設定する必要はありません。ルートリフレッシュの EOR を生成できない程度までルート フラッピングが続いていることが確認された場合には、一方または両方のタイマーを設定できます。

1 つ目のタイマーは、EOR メッセージを受信する必要があるが受信していないときにルータに適用されます。2 つ目のタイマーは、EOR メッセージを送信する必要があるときにルータに適用されます。

- 失効パス タイマー：**bgp refresh stalepath-time** コマンドが設定されている場合に、ルータが Adj-RIB-Out の後に Route-Refresh EOR メッセージを受信しないときは、このタイマーが期限切れになると BGP テーブルから失効ルートが削除されます。失効パス タイマーは、ルータが Route-Refresh SOR メッセージを受信したときに開始されます。
- 最大 EOR タイマー： **bgp refresh max-eor-time** コマンドが設定されている場合に、ルータが Route-Refresh EOR メッセージを生成できないときは、このタイマーが期限切れになると Route-Refresh EOR メッセージが生成されます。

両方のタイマーが設定可能です。デフォルトでは、両方とも無効になっています（0 秒に設定されています）。

BGP 拡張ルート リフレッシュよって生成される Syslog メッセージ

次に、Route-Refresh EOR メッセージの受信後または失効パス タイマーの期限切れ後にピアが失効ルートを削除したときに生成される Syslog メッセージの例を示します。このメッセージは、ルータの整合性を確認する際に役立ちます。

```
Net 300:300:3.3.0.0/0 from bgp neighbor IPv4 MDT 10.0.101.1 is stale after refresh EOR
(rate-limited)
Net 300:300:3.3.0.0/0 from bgp neighbor IPv4 MDT 10.0.101.1 is stale after refresh
stale-path timer expiry (rate-limited)
```

次に、Route-Refresh EOR の後または失効パス タイマーの期限切れ後にログに記録されたメッセージの例を示します。これには、ネイバーからの失効パスの合計数が示されています。

```
3 stale-paths deleted from bgp neighbor IPv4 MDT 10.0.101.1 after refresh EOR
3 stale-paths deleted from bgp neighbor IPv4 MDT 10.0.101.1 after refresh stale-path
timer expiry
```

BGP 拡張ルート リフレッシュのタイマーの設定方法

BGP 拡張ルート リフレッシュのタイマーの設定

BGP 拡張ルート リフレッシュ機能はデフォルトで有効になっています。タイマーはデフォルトでは無効になっています。オプションのタイマーを設定する場合は、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system*
4. **bgp refresh stalepath-time** *seconds*
5. **bgp refresh max-eor-time** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system* 例： `Router(config)# router bgp 65000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**bgp refresh stalepath-time** *seconds* 例： `Router(config-router)# bgp refresh stalepath-time 1200`	（任意）ルータが Route-Refresh End-of-RIB メッセージを受信していない場合でも、このタイマーの期限が切れると BGP テーブルから失効ルートが削除されるようにします。 • 有効値は 600 ～ 3600、または 0 です。

	コマンドまたはアクション	目的
		• デフォルトは 0 で、失効パス タイマーが無効になっていることを意味します。 • 失効パス タイマーは、ルータが Route-Refresh Start-of-RIB メッセージを受信したときに開始されます。
ステップ 5	**bgp refresh max-eor-time** *seconds* 例： `Router(config-router)# bgp refresh max-eor-time 1200`	（任意）BGP が Route-Refresh End-of-RIB（EOR）メッセージを生成できない場合には、このタイマーの期限が切れると Route-Refresh EOR が生成されるようにします。 • 有効値は 600 ～ 3600、または 0 です。 • デフォルトは 0 で、最大 EOR タイマーが無効になっていることを意味します。

BGP 拡張ルート リフレッシュの設定例

例：BGP 拡張ルート リフレッシュのタイマーの設定

次の例では、800 秒経過しても Route-Refresh EOR メッセージが受信されない場合には、失効ルートが BGP テーブルから削除されます。800 秒経過しても Route-Refresh EOR メッセージが生成されない場合には、EOR メッセージが生成されます。

```
router bgp 65000
 bgp refresh stalepath-time 800
 bgp refresh max-eor-time 800
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

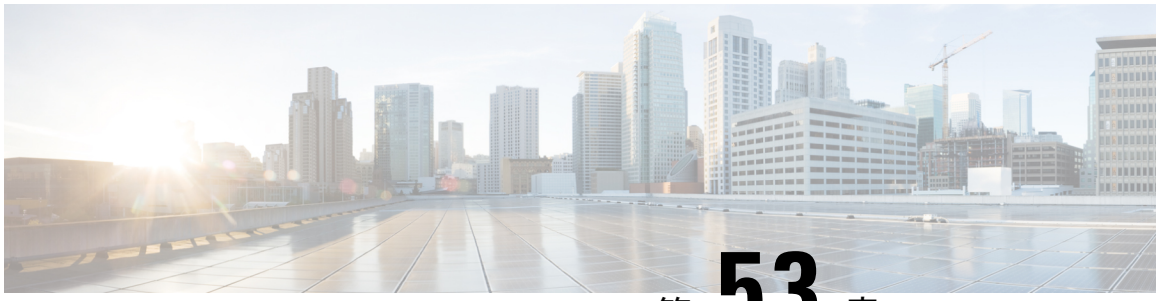
BGP 拡張ルート リフレッシュの機能情報

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 *68 : BGP* 拡張ルート リフレッシュの機能情報

機能名	リリース	機能情報
BGP 拡張ルート リフレッシュ		BGP 拡張ルート リフレッシュ機能は、BGP でルートの不整合を検出し、万一不整合があった場合には、ハード リセットなしに BGP ピアを同期する方法を提供します。 次のコマンドが導入されました。 • **bgp refresh max-eor-time** • **bgp refresh stalepath-time**



第 53 章

BGP 整合性チェッカの設定

BGP の整合性チェッカ機能は、ネクストホップ ラベルの不一致、RIB-out の不一致、集約の不一致など、ピアと BGP ルートの特定タイプの不一致を特定する方法を提供します。このような不一致を検出すると、設定されている場合は syslog エラー メッセージを送信し、適切なアクションを実行します。

- 機能情報の確認 （957 ページ）
- BGP 整合性チェッカに関する情報 （958 ページ）
- BGP 整合性チェッカの設定方法 （959 ページ）
- BGP 整合性チェッカの設定例 （960 ページ）
- その他の参考資料 （960 ページ）
- BGP 整合性チェッカの機能情報 （962 ページ）

機能情報の確認

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

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

BGP 整合性チェッカに関する情報

BGP の整合性チェッカ

更新や取り消しがピアに送信されない場合、ピアとの BGP ルートの不整合が発生し、ブラックホールルーティングにつながる可能性があります。この問題を特定するために、設定可能な間隔でネクストホップ ラベル、RIB-Out、および集約の整合性検査を行う優先順位の低いプロセスとして、BGP 整合性チェッカが作成されました。BGP 整合性チェッカは、有効になっている場合、すべてのアドレス ファミリに対して実行されます。BGP 整合性チェッカを設定することをお勧めします。

このような不整合が特定されると、Syslog メッセージでその不整合が報告され、**auto-repair** キーワードが指定されている場合はオプションでアクションが実行されます。実行されるアクションは、検出された不整合の種類によって決まります。

- ネクストホップ ラベル整合性検査：2 つのパスが同じプロバイダー エッジ ルータ（PE）でアドバタイズされるため、それらのパスのネクストホップが同じである場合は、それらのネクストホップラベルも同じである必要があります。ラベルが異なる場合は、不整合となります。**auto-repair** キーワードが指定されている場合、ルートリフレッシュ リクエストが送信されます。
- RIB-Out整合性検査：ネットワークがアウトバウンドポリシーを通過したのに送信されない場合、またはアウトバウンドポリシーを通過しなかったのに送信される場合、不整合となります。**auto-repair** キーワードが指定されている場合、ルートリフレッシュ リクエストが送信されます。
- 集約整合性検査：特定のルートと集約されたルートが非同期になると、不整合が生じる可能性があります。**error-message** キーワードまたは **auto-repair** キーワードにより、集約の再評価がトリガーされます。

万一、不整合に関する Syslog メッセージを受け取った場合は、シスコ テクニカル サポートの担当者に報告して、実際に表示されたSyslogメッセージを提出してください。次に、このような Syslog メッセージの例を示します。

- “Net 10.0.0.0/32 has Nexthop-Label inconsistency.”
- “Net 10.0.0.0/32 in IPv4 Unicast has rib-out inconsistency for update-group 4 - outbound-policy fails.”

BGP 整合性チェッカの設定方法

BGP 整合性チェッカの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp consistency-checker** {**error-message** | **auto-repair**} [**interval** *minutes*]
5. **end**
6. **show ip bgp** [**vpnv4** | **vpnv6**] **all inconsistency nexthop-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 500`	BGP ルーティング プロセスを設定します。
ステップ 4	**bgp consistency-checker** {**error-message** | **auto-repair**} [**interval** *minutes*] 例： `Router(config-router)# bgp consistency-checker auto-repair interval 720`	BGP 整合性チェッカを有効にします。 • デフォルトの間隔は 1440 分（1 日）です。指定できる範囲は 5 ～ 1440 分です。
ステップ 5	**end** 例： `Router(config-router)# end`	現在の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 6	**show ip bgp［vpnv4	vpnv6］all inconsistency nexthop-label** 例： `Router# show ip bgp all inconsistency nexthop-label`	（任意）ネクストホップ ラベルの不整合が検出されたルートを表示します。 • この手順は、機能設定の一部ではありません。ネクストホップ ラベルの不整合に関する Syslog メッセージを受け取った際にそのルートを表示する場合のために用意されています。

BGP 整合性チェッカの設定例

例：BGP 整合性チェッカの設定

次の例は、デフォルト間隔の 1 日で auto-repair を指定して BGP 整合性チェッカを設定しています。

```
router bgp 65000
 bgp consistency-checker auto-repair
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP MIB サポートの有効化	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP MIB サポート」モジュール
SNMP サポートの設定	*Cisco IOS Network Management Configuration Guide Library* の『*SNMP Configuration Guide* 』
SNMP コマンド	『*Cisco IOS SNMP Support Command Reference*』

標準

標準	タイトル
なし	—

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

RFC

RFC	タイトル
RFC 1657	『*BGP-4 MIB*』
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 2547	『*BGP/MPLS VPNs*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

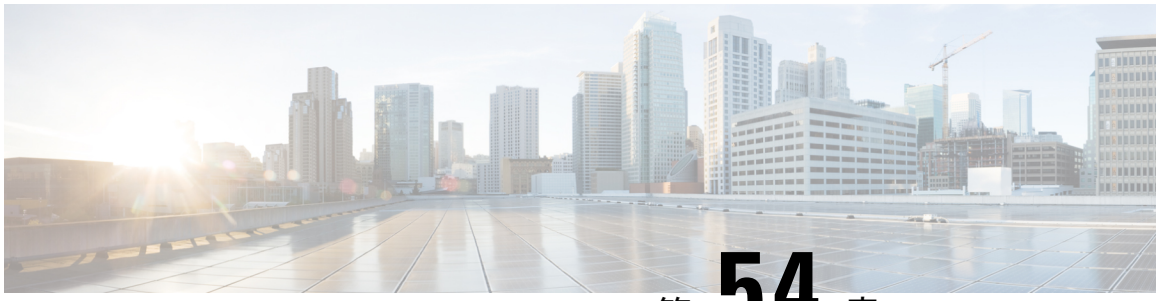
BGP 整合性チェッカの機能情報

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 *69 : BGP* 整合性チェッカの機能情報

機能名	リリース	機能情報
BGP の整合性チェッカ	Cisco IOS XE リリース 3.3S Cisco IOS XE Release 3.4SG	BGP 整合性チェッカ機能は、ネクストホップ ラベルの不整合、RIB-Out の不整合、集約の不整合という、3 種類のピアとの BGP ルートの不整合を特定する方法を提供します。このような不整合が検出されると、Syslog エラー メッセージが送信され、設定に応じて適切なアクションが実行されます。 次のコマンドが導入されました。 **bgp consistency-checker** **show ip bgp vpnv4** コマンドが変更されました。



第 54 章

BGP—起点 AS 検証

BGP—起点 AS 検証機能は、ネットワーク管理者が制御外のネットワークにルートを誤ってアドバタイズすることを防止できます。この機能では、リソース公開キーインフラストラクチャ（RPKI）サーバを使用して、特定の BGP プレフィックスが予期された自律システムから発信されたものであることを認証してから、プレフィックスのアドバタイズを許可します。

- 機能情報の確認 （963 ページ）
- BGP 起点 AS 検証に関する情報 （964 ページ）
- BGP 起点 AS 検証の設定方法 （968 ページ）
- BGP 起点 AS 検証の設定例 （975 ページ）
- その他の参考資料 （977 ページ）
- 非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の機能情報 （978 ページ）

機能情報の確認

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

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

BGP 起点 AS 検証に関する情報

BGP—起点 AS 検証の利点

場合によって、ネットワーク管理者が制御外のネットワークにルートを誤ってアドバタイズしてしまうことがあります。このセキュリティ上の問題は、BGP—起点 AS 検証機能を設定することで回避できます。この機能では、RPKI サーバを使用して、特定の BGP プレフィックスが予期された自律システムから発信されたものであることを認証してから、プレフィックスを承認します。

BGP—起点 AS 検証の仕組み

ネットワーク管理者は、サードパーティ製ソフトウェアを使用して、リソース公開キーインフラストラクチャ（RPKI）サーバをセットアップする必要があります。RPKI サーバは、公開キー証明書の実際の認証を処理します。特定の自律システムを発信元とする特定のプレフィックスまたはプレフィックス範囲を許可するように、サーバをセットアップします。

次に、管理者は、RPKI サーバへの TCP 接続を確立するようにルータを設定します。これは、**bgp rpki server** コマンドを設定することで行います。このように設定したとき、またはルータを起動したとき、ルータは指定された IP アドレスおよびポート番号への TCP 接続を開きます。ルータは、RPKI-Router プロトコル（RTR）を使用して、1 つ以上のルータまたは RPKI サーバからプレフィックスおよび許可された起点 AS 番号のリストをダウンロードします。したがって、ルータは、どの自律システムがどのルートをアドバタイズすることが許可されているか、つまりどの AS がルートの発信元となることができるかに関する情報をサーバから取得します。

TCP 接続の試行が失敗した場合、ルータは 1 分間に 1 回接続を再試行します。その間、BGP は起点検証を実行せずに動作します。

ルータとサーバの間で TCP セッションが確立されると、サーバは、通常、RPKI データベースに追加された新しいプレフィックスを含む差分更新をルータに送信します。ルータは、更新間隔ごとにサーバに対してクエリを行うこともあります。ルータは、シリアル クエリまたはリセット クエリを送信してから、End of Data（EOD）メッセージを受信するまでの間に、シリアル クエリ メッセージまたはリセット クエリ メッセージを送信することはありません。この間のシリアル クエリは削除され、この間のリセット クエリは EOD メッセージの受信時に送信されます。

プレフィックスまたはプレフィックス範囲、およびそれに対応する起点 AS は、SOVC レコードと見なされます。プレフィックス範囲の重複は許可されます。3 つのレコードを含む SOVC テーブルは、次のようになります。

10.0.1.0/20-25 AS 3

10.0.1.0/19-24 AS 4

10.0.1.0/23-27 AS 5

プレフィックス（ネットワーク）が外部 BGP（eBGP）ピアから受信されると、プレフィックスは最初は「Not Found」状態になります。その後、プレフィックスは検査され、Valid、Invalid、または Not Found としてマークされます。

- Valid（有効）：プレフィックスと AS のペアが SOVC テーブル内にあることを示します。
- Invalid（無効）：プレフィックスが次の 2 つの条件のいずれかを満たしていることを示します。1. 1 つ以上の Route Origin Authorization（ROA）に一致しているが、起点 AS が AS-PATH の起点 AS と合致する一致 ROA はない。2. ROA で指定された最小長で 1 つ以上の ROA と一致しているが、最小長で一致するすべての ROA について、その長さが指定された最大長を超えている。起点 AS は条件 2 には関係ありません。
- Not Found（見つからない）：目的のプレフィックスが有効または無効なプレフィックスの中にないことを示します。

デフォルトでは、Invalid とマークされたプレフィックスは、どのピアにもアドバタイズされず、すでにアドバタイズされている場合には BGP ルーティング テーブルから取り消され、ベストパスとしてフラグが付けられることも、マルチパスの候補として見なされることもありません（BGP bestpath コマンドで別の方法が指定されている場合を除く）。別の方法を指定して BGP bestpath コマンドが設定されている場合を除いて、ベストパス計算では、Not Found プレフィックスよりも Valid プレフィックスが優先され、両方のタイプのプレフィックスがアドバタイズされます。

Valid としてマークされたプレフィックスは BGP ルーティング テーブルにインストールされます。

デフォルトでは、Not Found としてマークされたプレフィックスは BGP ルーティング テーブルにインストールされ、代わりとなる Valid の項目がない場合にのみ（ローカル プリファレンスや AS_PATH などのその他の BGP 属性は考慮されない）、ベストパスとしてフラグが付けられるか、マルチパスの候補と見なされます。

複数の RPKI サーバが設定されている場合、ルータは、設定されているすべてのサーバに接続し、すべてのサーバからプレフィックス情報をダウンロードします。SOVC テーブルは、各サーバから受信したすべてのレコードを結合して作られます。

特定のアドレス ファミリに対して **bgp rpki server** コマンド（または **neighbor announce rpki state** コマンド）を設定すると、ルータは、そのアドレス ファミリのすべてのパスについて RPKI 検証の実行を開始します。

RPKI 検証状態をネイバーに通知するためのオプション

オプションで、拡張コミュニティ属性を使用して、プレフィックスの検証状態を内部 BGP（iBGP）ネイバーに（から）通知（受信）することができます。このオプションは、一部のルータでは、RPKI サーバに接続する必要がなくなるため、 **bgp rpki server** コマンドを設定するよりも便利な場合があります。

neighbor announce rpki state コマンドを使用すると、ルータは、BGP 拡張コミュニティ属性でルートとともに RPKI ステータスをその iBGP ネイバーに送信します。また、ルータは、その

iBGP ネイバーからルートとともに RPKI ステータスを受信します。この通知は双方向で機能します。通知される拡張コミュニティ属性は次のとおりです。

0x4300 0x0000（状態を示す 4 バイト）

状態を示す4バイトは、次のいずれかの値を持つ32ビットの符号なし整数として扱われます。

- 0：Valid（有効）
- 1：Not Found（見つからない）
- 2：Invalid（無効）

neighbor announce rpki state コマンドが設定されている場合、ルータは、この拡張コミュニティ属性が付加されたルートを iBGP ピアから受信すると、対応する検証状態をルートに割り当てます。**neighbor announce rpki state** コマンドが設定されていない場合は、iBGP ピアから受信されたすべてのプレフィックスは、Not Found とマークする必要があるプレフィックスを含めて、Valid としてマークされます。

（注） この拡張コミュニティ属性は、この属性の送信を許可するように設定されている場合でも、eBGP ネイバーには送信されません。

RPKI 状態拡張コミュニティは、さらに以下の動作に従います。

- **neighbor announce rpki state** コマンドの設定は、そのアドレス ファミリのそのネイバーに拡張コミュニティを送信するようにルータが設定されている場合にのみ可能です。
- **neighbor announce rpki state** コマンドは、該当のアドレス ファミリに対して RPKI が設定されているかどうかとは無関係に機能します。
- 特定のアドレス ファミリに対して **neighbor announce rpki state** コマンドまたは **bgp rpki server** コマンドを設定すると、ルータは、そのアドレス ファミリのすべてのパスについて RPKI 検証の実行を開始します。
- **neighbor announce rpki state** コマンドを有効または無効にすると、ネイバーは、この部分の設定が同じであるかどうかに基づいて、独自のアップデート グループに分けられます。
- **neighbor announce rpki state** コマンドが設定されていない場合、ルータは他のルータから受信した RPKI 状態を保存しますが、その状態が使用されるのは、アドレス ファミリの少なくとも 1 つの他のネイバーが **neighbor announce rpki state** コマンドを使用して設定されているときだけ、またはトポロジが RPKI の使用に対して別の方法で有効化されているときだけです。
- **neighbor send-community extended** または **neighbor send-community both** コマンドを設定から削除すると、**neighbor announce rpki state** 設定も削除されます。
- ルート リフレクタ（RR）を設定している場合に、**neighbor announce rpki state** コマンドが設定されていないクライアントから RPKI 状態拡張コミュニティを含むネットワークを RR サーバが受信したときは、拡張コミュニティを受け取ることができるすべてのクライアントに反映されます。

- ネットワークに RPKI 状態拡張コミュニティが含まれている場合に、**neighbor announce rpki state** コマンドが設定されているネイバーからそのネットワークを RR が受信したときは、拡張コミュニティを受け入れるように設定されているすべての RR クライアントに反映されます。その際、それらの RR クライアントに対して **neighbor announce rpki state** コマンドが設定されているかどうかは問いません。
- **neighbor announce rpki state** コマンドは、ピア ポリシー テンプレートで使用でき、継承されます。
- ピア ポリシー テンプレートで **neighbor announce rpki state** コマンドを使用する場合は、**send-community extended** コマンドと同じテンプレート内にある必要があります。**neighbor announce rpki state** コマンドと **send-community extended** コマンドは、同じテンプレートから取得するか、同じネイバーに対して設定する必要があります。

BGP ベスト パス決定での検証状態の使用

RPKI 検証状態を使用する場合は、次の 2 つの方法で、デフォルトの BGP ベスト パス選択プロセスを変更できます。

- RPKI サーバによるプレフィックスの検証およびその検証情報の保存を完全に無効にすることができます。これは、**bgp bestpath prefix-validate disable** コマンドを設定することで行います。この方法は設定テストで必要になる場合があります。ルータは引き続き RPKI サーバに接続して検証情報をダウンロードしますが、その情報は使用されません。
- 有効なプレフィックスが使用可能な場合でも、無効なプレフィックスを BGP ベスト パスとして使用することを許可できます。これはデフォルトの動作です。BGP ベスト パスを無効なプレフィックス（BGP 起点 AS 検証機能で決定）にすることを許可するコマンドは、**bgp bestpath prefix-validate allow-invalid** コマンドです。プレフィックスの検証状態は、引き続きパスに割り当てられ、RPKI 状態情報を受信するように設定されている iBGP ネイバーに引き続き通知されます。ルートマップを使用し、検証状態に基づいてローカル プリファレンス、メトリック、またはその他のプロパティを設定できます。

BGP ベスト パス選択時、上記のオプションがいずれも設定されていない場合、デフォルトの動作では、プレフィックスは次の順序で優先されます。

- 検証状態が有効なもの。
- 検証状態が見つからないもの。
- 検証状態が無効なもの（この場合、デフォルトでは、ルーティング テーブルにインストールされません）。

これらの設定は、メトリック、ローカル プリファレンス、およびベストパス計算時に行われたその他の選択をオーバーライドします。標準のベストパス決定ツリーは、2 つのパスの検証状態が同じである場合にのみ適用されます。

両方のコマンドが設定されている場合、**bgp bestpath prefix-validate disable** コマンドにより、検証状態がパスに割り当てられなくなるため、**bgp bestpath prefix-validate allow-invalid** コマンドは無効になります。

これらの設定は、IPv4 ユニキャストまたは IPv6 ユニキャスト アドレス ファミリのルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードのいずれかになります。

ルートマップを使用した有効および無効なプレフィックスの処理のカスタマイズ

任意のRPKI状態に一致するルートマップを作成することにより、有効または無効なプレフィックスを処理するためのカスタム ポリシーを作成できます。

デフォルトでは、ルータは、他のすべての設定をオーバーライドして、無効な状態のルートを拒否します。このようなプレフィックスを許可しながら、デフォルト以外のローカルプリファレンスを使用するといった操作を、ルート マップで行う場合は、**bgp bestpath prefix-validate allow-invalid** コマンドを明示的に設定する必要があります。

BGP 起点 AS 検証の設定方法

BGP—起点 AS 検証の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp rpki server tcp** {*ipv4-address* | *ipv6-address*} **port** *port-number* **refresh** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp rpki server tcp** {*ipv4-address* | *ipv6-address*} **port** *port-number* **refresh** *seconds* 例： `Device(config-router)# bgp rpki server tcp 192.168.2.2 port 1029 refresh 600`	**refresh** *seconds* キーワードおよび引数で指定した間隔で指定の RPKI サーバに接続してプレフィックス情報をダウンロードするようにルータを設定します。

iBGP ネイバーへの RPKI 状態の通知

BGP 拡張コミュニティ属性でルートとともに RPKI 状態をその iBGP ネイバーに通知し、iBGP ネイバーからルートとともに RPKI 状態を受信するようにルータを設定するには、この作業を実行します。この作業は、ルータで BGP—起点 AS 検証機能を設定するよりも便利な場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address*} **send-community extended**
5. **neighbor** {*ip-address* | *ipv6-address*} **announce rpki state**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*} **send-community extended** 例： `Device(config-router)# neighbor 192.168.1.2 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*} **announce rpki state** 例： `Device(config-router)# neighbor 192.168.1.2 announce rpki state`	ルータとその iBGP ネイバーの間で BGP 拡張コミュニティ属性によって RPKI 状態を送受信するようにします。

BGP プレフィックスの検証を無効化しながら、RPKI 情報をダウンロード

BGP—起点 AS 検証機能が有効になっている場合に、起点 AS に基づくプレフィックスの検証を無効にし、検証情報の保存を無効にするには、この作業を実行します。ルータは引き続き RPKI サーバに接続して検証情報をダウンロードしますが、その情報は一切使用されません。この作業は設定テストに役立ちます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** | **ipv6**} **unicast**
5. **bgp bestpath prefix-validate disable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**ipv4** | **ipv6**} **unicast** 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 5	**bgp bestpath prefix-validate disable** 例： `Device(config-router-af)# bgp bestpath prefix-validate disable`	プレフィックスの検証および検証情報の保存を無効にします。

無効なプレフィックスをベスト パスとして許可

BGP—起点 AS 検証機能が有効になっている場合に、有効なプレフィックスが使用可能であっても、無効なプレフィックスをベストパスとして使用することを許可するには、この作業を実行します。つまり、無効なネットワークについて通知するが、有効なプレフィックスおよび見つからないプレフィックスよりも優先度は低くするように制御できます。また、ダウンストリーム ピアでは、無効なプレフィックスを照合するルート マップに基づいてパス属性を変更できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** | **ipv6**} **unicast**
5. **bgp bestpath prefix-validate allow-invalid**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**ipv4** | **ipv6**} **unicast** 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 5	**bgp bestpath prefix-validate allow-invalid** 例： `Device(config-router-af)# bgp bestpath prefix-validate allow-invalid`	有効なプレフィックスが使用可能な場合でも、無効なプレフィックスをベストパスとして使用することを許可します。

RPKI 状態に基づくルート マップの設定

RPKI 状態に基づいてルート マップを作成するには、この作業を実行します。この特定の作業のルート マップでは、ローカル プリファレンスに基づいて 3 つの RPKI 状態すべてに対するポリシーを設定しますが、他の **set** コマンドを使用してポリシーを設定することもできます。この作業には、このルート マップを使用するコマンドは含まれていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** | **ipv6**} **unicast**
5. **bgp bestpath prefix-validate allow-invalid**
6. **exit**
7. **exit**
8. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
9. **match rpki** {**not-found** | **invalid** | **valid**}
10. **set local-preference** *number*
11. **exit**
12. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
13. **match rpki** {**not-found** | **invalid** | **valid**}
14. **set local-preference** *number*
15. **exit**
16. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
17. **match rpki** {**not-found** | **invalid** | **valid**}

18. **set local-preference** *number*
19. **exit**
20. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
21. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**ipv4**	**ipv6**} **unicast** 例： `Device(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 5	**bgp bestpath prefix-validate allow-invalid** 例： `Device(config-router-af)# bgp bestpath prefix-validate allow-invalid`	有効なプレフィックスが使用可能な場合でも、無効なプレフィックスをベスト パスとして使用することを許可します。 • このコマンドは、手順 16 のルート マップ例の一部である無効なプレフィックスを許可するために必要です。
ステップ 6	**exit** 例： `Device(config-router-af)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 7	**exit** 例： `Device(config-router)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルの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 8	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME-1 permit 10`	ルート マップ コンフィギュレーション モードを開始し、後続の match 句で許容されるルートを許可するルート マップを作成します。
ステップ 9	**match rpki** {**not-found** | **invalid** | **valid**} 例： `Device(config-route-map)# match rpki valid`	指定した RPKI 状態のプレフィックスを許可する match 句を作成します。 • この例では、RPKI 状態が valid（有効）であるかどうかを照合します。
ステップ 10	**set local-preference** *number* 例： `Device(config-route-map)# set local-preference 200`	一致したプレフィックスのローカル プリファレンスを 200 に設定する set 句を作成します。
ステップ 11	**exit** 例： `Device(config-route-map)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 12	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME-1 permit 20`	同じルート マップのまま、遅いシーケンス番号を指定して、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 13	**match rpki** {**not-found** | **invalid** | **valid**} 例： `Device(config-route-map)# match rpki not-found`	指定した RPKI 状態のプレフィックスを許可する match 句を作成します。 • この例では、RPKI 状態が not-found（見つからない）であるかどうかを照合します。
ステップ 14	**set local-preference** *number* 例： `Device(config-route-map)# set local-preference 100`	RPKI 状態が not-found であるプレフィックスのローカル プリファレンスを 100 に設定します。
ステップ 15	**exit** 例： `Device(config-route-map)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルの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 16	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME-1 permit 30`	同じルート マップのまま、遅いシーケンス番号を指定して、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 17	**match rpki** {**not-found** | **invalid** | **valid**} 例： `Device(config-route-map)# match rpki invalid`	指定した RPKI 状態のプレフィックスを許可する match 句を作成します。 • この例では、RPKI 状態が invalid（無効）であるかどうかを照合します。
ステップ 18	**set local-preference** *number* 例： `Device(config-route-map)# set local-preference 50`	RPKI 状態が invalid であるプレフィックスのローカル プリファレンスを 50 に設定します。
ステップ 19	**exit** 例： `Device(config-route-map)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 20	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map ROUTE-MAP-NAME-1 permit 40`	同じルート マップのまま、遅いシーケンス番号を指定して、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。 • この例では、他のすべてのルートを拒否するのではなく、他のルートを許可します。
ステップ 21	**end** 例： `Device(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP 起点 AS 検証の設定例

例：起点 AS に基づいてプレフィックスを検証するための BGP の設定

次の例では、ルータは、2 台の RPKI サーバに接続するように設定されており、そのサーバから BGP プレフィックスおよび AS 番号から成る SOVC レコードを受信します。

```
router bgp 65000
 no bgp log-neighbor changes
 bgp rpki server tcp 10.0.96.254 port 32001 refresh 600
 bgp rpki server tcp FEC0::1002 port 32002 refresh 600
```

例：ネイバーへの RPKI 状態の通知

```
router bgp 65000
 neighbor 10.10.10.10 remote-as 65000
 address-family ipv4 unicast
 neighbor 10.10.10.10 send-community extended
 neighbor 10.10.10.10 announce rpki state
```

例：プレフィックス検査の無効化

次の例では、IPv4アドレス ファミリについて、有効であることを確認するプレフィックス検査を無効にします。また、検証情報の保存も無効にします。ただし、ルータは引き続き RPKI サーバに接続して検証情報をダウンロードします。この例は設定テストに役立ちます。

```
router bgp 65000
 bgp rpki server tcp 10.0.96.254 port 32001 refresh 600
 address-family ipv4 unicast
 bgp bestpath prefix-validate disable
```

例：無効なプレフィックスをベスト パスとして許可

次の例では、IPv6アドレス ファミリについて、有効なプレフィックスが使用可能な場合でも、無効なプレフィックスをベスト パスとして使用することを許可します。

```
router bgp 65000
 bgp rpki server tcp FEC0::1002 port 32002 refresh 600
 address-family ipv6 unicast
 bgp bestpath prefix-validate allow-invalid
```

例：RPKI 状態に基づくルート マップの使用

次の例では、rtmap-PEX1-3 という名前のルート マップで、無効なプレフィックスと AS のペアのローカル プリファレンスを 50 に、見つからないプレフィックスと AS のペアのローカル プリファレンスを 100 に、有効なプレフィックスと AS のペアのローカル プリファレンスを 200 に設定します。ローカル プリファレンス値は、10.0.102.1 のネイバーからの着信ルートに対して設定されます。10.0.102.1 のネイバーは eBGP ピ

アです。無効なプレフィックスを許可するためには **bgp bestpath prefix-validate allow-invalid** コマンドが必要であることに注意してください。

```
router bgp 65000
 address-family ipv4 unicast
 neighbor 10.0.102.1 route-map rtmap-PEX1-3 in
 bgp bestpath prefix-validate allow-invalid
!
route-map rtmap-PEX1-3 permit 10
 match rpki invalid
 set local-preference 50
!
route-map rtmap-PEX1-3 permit 20
 match rpki not-found
 set local-preference 100
!
route-map rtmap-PEX1-3 permit 30
 match rpki valid
 set local-preference 200
!
route-map rtmap-PEX1-3 permit 40
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

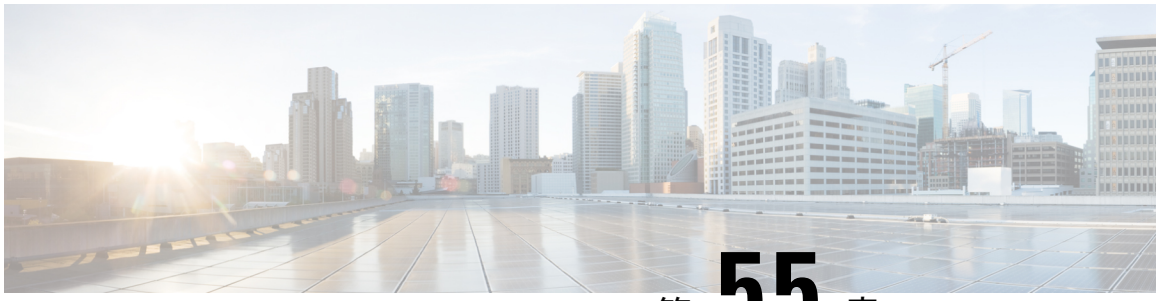
非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）の機能情報

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 *70*：非 *VRF* インターフェイスの *eiBGP* マルチパス（*IPv4/IPv6*）の機能情報

機能名	リリース	機能情報
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）		非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）機能により、ネイティブ IPv4 および IPv6 の外部ボーダー ゲートウェイ プロトコル（eBGP）パスと内部 BGP（iBGP）パスの間でマルチパス ロード シェアリングを設定して、展開環境でのロード バランシングを改善できます。 **maximum-paths eibgp** コマンドが変更されました。



第 55 章

BGP MIB サポート

BGP MIB サポート拡張機能によって、新しい SNMP 通知用に CISCO-BGP4-MIB のサポートが導入されています。

- 機能情報の確認 （979 ページ）
- BGP MIB サポートに関する情報 （979 ページ）
- BGP MIB サポートを有効にする方法 （982 ページ）
- BGP MIB サポートの設定例 （983 ページ）
- その他の参考資料 （984 ページ）
- BGP MIB サポートの機能情報 （985 ページ）

機能情報の確認

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

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

BGP MIB サポートに関する情報

BGP MIB サポート

BGP をサポートする Management Information Base（MIB）は CISCO-BGP4-MIB です。BGP MIB サポート拡張機能によって、新しい SNMP 通知用に CISCO-BGP4-MIB のサポートが導入されています。ここでは、サポートされるオブジェクトと通知（トラップ）について説明します。

BGP FSM 遷移変更のサポート

cbgpRouteTable では、BGP 有限状態マシン（FSM）遷移状態の変更がサポートされます。

cbgpFsmStateChange オブジェクトを使用すると、すべての FSM 遷移状態の変更について SNMP 通知（トラップ）を設定できます。この通知には、次の MIB オブジェクトが含まれています。

- bgpPeerLastError
- bgpPeerState
- cbgpPeerLastErrorTxt
- cbgpPeerPrevState

cbgpBackwardTransition オブジェクトでは、BGP FSM 遷移状態の変更がすべてサポートされます。このオブジェクトは、FSM が大きい番号が付いた状態または小さい番号が付いた状態のいずれかに移行されるたびに送信されます。この通知には、次の MIB オブジェクトが含まれています。

- bgpPeerLastError
- bgpPeerState
- cbgpPeerLastErrorTxt
- cbgpPeerPrevState

snmp-server enable bgp traps コマンドを使用すると、トラップを個別に有効にすることも、既存の FSM 後方遷移および確立状態トラップ（RFC 1657 で定義）と一緒に有効にすることもできます。

BGP ルートが受信したルートのサポート

cbgpRouteTable オブジェクトでは、BGP ネイバーが受信したルートの総数がサポートされます。個別の BGP ピアから取得したルートについて CISCO-BGP4-MIB を照会するために、次の MIB オブジェクトが使用されます。

- cbgpPeerAddrFamilyPrefixTable

ルートには、Address-Family Identifier（AFI）または Subaddress-Family Identifier（SAFI）によって索引が付けられます。このテーブルに表示されるプレフィックス情報は、**show ip bgp** コマンドの出力でも表示できます。

BGP プレフィックスしきい値の通知サポート

BGP ピアが受信したルートの総数をポーリングできるように、cbgpPrefixMaxThresholdExceed オブジェクトと cbgpPrfefixMaxThresholdClear オブジェクトが導入されました。

cbgpPrefixMaxThresholdExceed オブジェクトを使用すると、BGP セッションのプレフィックス数が設定値を超えた場合に送信される SNMP 通知を設定できます。この通知は、アドレス ファミリ単位で設定されます。プレフィックスしきい値は、**neighbor maximum-prefix** コマンドを使用して設定します。この通知には、次の MIB オブジェクトが含まれています。

- cbgpPeerPrefixAdminLimit
- cbgpPeerPrefixThreshold

cbgpPrfefixMaxThresholdClear オブジェクトを使用すると、プレフィックス数がトラップのクリア制限を下回った場合に送信される SNMP 通知を設定できます。この通知は、アドレス ファミリ単位で設定されます。この通知には、次のオブジェクトが含まれています。

- cbgpPeerPrefixAdminLimit
- cbgpPeerPrefixClearThreshold

通知は、プレフィックス数が、cbgpPrefixMaxThresholdExceed 通知の生成後に BGP セッション下でアドレス ファミリのトラップのクリア制限を下回った場合に送信されます。トラップのクリア制限は、**neighbor maximum-prefix** コマンドを使用して設定された最大のプレフィックス制限値から 5 % を減算することで計算します。この通知は、cbgpPrefixMaxThresholdExceed の生成後にその他の理由でセッションが停止した場合は生成されません。

VPNv4 ユニキャスト アドレス ファミリ ルートのサポート

cbgpRouteTable オブジェクトを使用すると、VPNv4 ユニキャスト アドレス ファミリ ルートの SNMP GET 操作を設定できます。

次の MIB オブジェクトを使用すると、複数の BGP 機能（たとえば、ルート リフレッシュ、マルチプロトコル BGP 拡張、およびグレースフル リスタート）を照会できます。

- cbgpPeerCapsTable

次の MIB オブジェクトを使用すると、IPv4 および VPNv4 アドレス ファミリ ルートを照会できます。

- cbgpPeerAddrFamilyTable

それぞれのルートには、ピア アドレス、プレフィックス、およびプレフィックス長によって索引が付けられます。このオブジェクトは、AFI、次に SAFI によって BGP ルートに索引を付けます。AFI テーブルがプライマリ索引であり、SAFI テーブルはセカンダリ索引です。それぞれの BGP スピーカーは、サポートされる AFI と SAFI との組み合わせごとにローカル ルーティング情報ベース（RIB）を維持します。

cbgpPeerTable サポート

cbgpPeerTable は、このマニュアルで説明されている機能拡張をサポートするために変更されました。次の新しいテーブル オブジェクトが CISCO-BGP-MIB.my でサポートされます。

- cbgpPeerLastErrorTxt
- cbgpPeerPrevState

次のテーブル オブジェクトはサポートされません。これらのオブジェクトのステータスは廃止とリストされ、これらのオブジェクトは動作不可能です。

- cbgpPeerPrefixAccepted

- cbgpPeerPrefixDenied
- cbgpPeerPrefixLimit
- cbgpPeerPrefixAdvertised
- cbgpPeerPrefixSuppressed
- cbgpPeerPrefixWithdrawn

BGP MIB サポートを有効にする方法

BGP MIB サポートのイネーブル化

SNMP 通知はルータで設定でき、GET 操作は、BGP SNMP サポートをイネーブルにした後にだけ外部管理ステーションから実行できます。この作業は、BGP MIB の SNMP 通知を設定する場合にルータで実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps bgp** [[**state-changes** [**all**] [**backward-trans**] [**limited**]] | [**threshold prefix**]]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**snmp-server enable traps bgp** [[**state-changes** [**all**] [**backward-trans**] [**limited**]]	[**threshold prefix**]] 例： `Device(config)# snmp-server enable traps bgp`	SNMP 操作に対する BGP サポートをイネーブルにします。キーワードまたは引数を指定せずにこのコマンドを入力すると、すべての BGP イベントに対するサポートがイネーブルになります。 • **state-changes** キーワードは、FSM 遷移イベントに対するサポートを有効にするために使用します。

	コマンドまたはアクション	目的
		• **all** キーワードは、FSM 遷移イベントに対するサポートを有効にします。 • **backward-trans** キーワードは、後方遷移の状態変更イベントに対するサポートだけを有効にします。 • **limited** キーワードは、後方遷移の状態変更および確立状態イベントに対するサポートを有効にします。 • **threshold** キーワードと **prefix** キーワードは、指定したピアで設定済みのプレフィックス最大制限に達した場合に通知を有効にするために使用します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル 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。

BGP MIB サポートの設定例

例：BGP MIB サポートの有効化

次の例では、サポートされるすべての BGP イベントに対する SNMP サポートをイネーブルにします。

```
Device(config)# snmp-server enable traps bgp
```

次の検証例では、実行コンフィギュレーション ファイル内の「snmp-server」を含む行を表示して、BGP に対する SNMP サポートが有効になっていることを示しています。

```
Device# show run | include snmp-server

snmp-server enable traps bgp
```

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』
BGP コマンド	『IP Routing: BGP Command Reference』
CISCO-BGP-MIBv8.1 でサポートされる MIB オブジェクト	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「Cisco-BGP-MIBv2」モジュール
SNMP 操作と SNMP 操作に関する情報	*Network Management Configuration Guide Library* の『SNMP Configuration Guide 』

MIB

MIB	MIB のリンク
CISCO-BGP4-MIB	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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

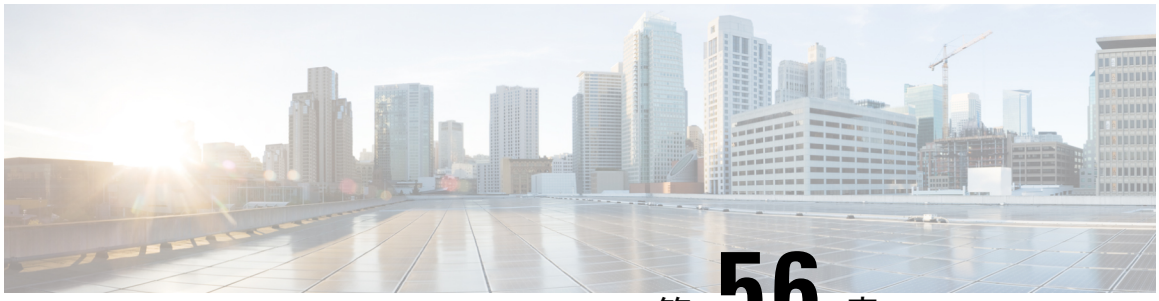
BGP MIB サポートの機能情報

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 *71 : BGP MIB* サポートの機能情報

機能名	リリース	機能情報
BGP MIB サポート拡張機能	12.0(26)S 12.2(25)S 12.3(7)T 12.2(33)SRA 12.2(22)SXH 15.0(1)SY	BGP MIB サポート拡張機能によって、新しい SNMP 通知用に CISCO-BGP4-MIB のサポートが導入されました。 **snmp-server enable traps bgp** コマンドが導入されました。



第 56 章

ピアごとの受信ルートに対する BGP 4 MIB サポート

ここでは、ピアごとの受信ルートに対する BGP 4 MIB サポートについて説明します。この機能は、個別のボーダー ゲートウェイ プロトコル（BGP）ピアから学習したルートを（Simple Network Management Protocol（SNMP）コマンドを使用して）照会する機能を提供するテーブルを CISCO-BGP4-MIB に導入します。

- 機能情報の確認 （987 ページ）
- ピアごとの受信ルートに対する BGP 4 MIB サポートの制約事項 （988 ページ）
- ピアごとの受信ルートに対する BGP 4 MIB サポートに関する情報 （988 ページ）
- 最大プレフィックス制限到達後の BGP ネイバー セッション再起動に関する追加情報 （992 ページ）
- ピアごとの受信ルートに対する BGP 4 MIB サポートの機能情報 （993 ページ）
- 用語集 （993 ページ）

機能情報の確認

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

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

ピアごとの受信ルートに対する BGP 4 MIB サポートの制約事項

ピアごとの受信ルートに対する BGP 4 MIB サポートは、ローカル BGP RIB テーブルの IPv4 AFI およびユニキャスト SAFI に格納されるルートのみをサポートします。ピアごとの受信ルートに対する BGP 4 MIB サポートの拡張は BGP Version 4 でのみサポートされます。

ピアごとの受信ルートに対する BGP 4 MIB サポートに関する情報

ピアごとの受信ルートに対する BGP 4 MIB サポートの概要

ピアごとの受信ルートに対する BGP 4 MIB サポートは、個別の BGP ピアから学習したルートを（SNMP コマンドを使用して）照会する機能を提供するテーブルを CISCO-BGP4-MIB に導入します。

この新しい MIB テーブルが導入される前は、ネットワーク オペレータが SNMP コマンド（**snmpwalk** コマンドなど）でローカル BGP スピーカーを照会して、ローカル BGP 対応ルータによって学習されたルートを取得できました。ネットワーク オペレータは SNMP コマンドを使用して CISCO-BGP4-MIB の bgp4PathAttrTable を照会していました。bgp4PathAttrTable のクエリーから返されたルートは、次の順序でインデックス化されました。

- Prefix
- [Prefix length]
- ピア アドレス

bgp4PathAttrTable は最初にプレフィックスをインデックス化するため、個別の BGP ピアから学習したルートを取得するには、ネットワーク オペレータが完全な bgp4PathAttrTable を「ウォークスルー」して、関心のあるピアからルートをフィルタで除去する必要があります。RIB ルーティング情報ベース（RIB）には 10,000 以上のルートが格納されることがあり、このため、手動の「ウォーク」操作が不可能になり、自動のウォーク操作が著しく非効率的になります。

ピアごとの受信ルートに対する BGP 4 MIB サポートは、cbgpRouterTable という新しいテーブルを定義する Cisco 固有のエンタープライズ拡張を CISCO-BGP4-MIB に導入します。cbgpRouterTable は bgp4PathAttrTable と同じ情報を提供しますが、次の 2 つの違いがあります。

- ルートは次の順序でインデックス化されます。
  - ピア アドレス
  - Prefix
  - [Prefix length]

ピア アドレスがプレフィックスの前にインデックス化されるため、ローカル ルートの SNMP クエリーの検索条件が改善されます。ピア アドレスがプレフィックスの前にインデックス化されるため、この拡張によって、個別のピアから学習されるルートの検索が改善されます。ネットワーク オペレータは、ローカル BGP RIB テーブルの学習されたルートを取得するために、数千の可能性のあるルートをすべて検索する必要がなくなります。

- マルチプロトコル BGP、Address Family Identifier（AFI）、Subsequent Address Family Identifier（SAFI）情報のサポートが追加されました。この情報は、cbgpRouterTable へのインデックスの形式で追加されます。CISCO-BGP4-MIB はローカル BGP スピーカーでサポートされる AFI と SAFI の任意の組み合わせで照会できます。

（注） ルータが BGP プロセスを実行するように設定されている場合にのみ、MIB に値が読み込まれます。ピアごとの受信ルートに対する BGP 4 MIB サポートの現在の実装では、IPv4 AFI およびユニキャスト SAFI BGP ローカル RIB テーブルに格納されるルートのみが表示されます。他のローカル RIB テーブルに格納されるルートの表示のサポートは、将来追加される予定です。

BGP 4 ピアごとの受信ルート テーブルの要素とオブジェクト

次の項では、ピアごとの受信ルートに対する BGP 4 MIB サポート拡張によって導入された新しいテーブル要素、AFI および SAFI テーブルおよびオブジェクト、Network Layer Reachability Information（NLRI）フィールドのネットワーク アドレス プレフィックスについて説明します。

MIB テーブルおよびオブジェクト

下の表で、cbgpRouterTable の MIB インデックスについて説明します。

MIB の完全な説明については、Cisco.com の次の URL から入手可能な CISCO-BGP4-MIB ファイル CISCO-BGP4-MIB.my を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

表 *72 : cbgpRouterTable* の *MIB* インデックス

MIB インデックス	説明
cbgpRouteAfi	ルートに関連付けられたネットワーク層プロトコルの AFI を表します。
cbgpRouteSafi	ルートの SAFI を表します。これは、ルートのタイプに関する追加情報を提供します。AFI と SAFI を共に使用して、特定のルートを格納するローカル RIB（Loc-RIB）を特定します。
cbgpRoutePeerType	cbgpRoutePeer オブジェクトに格納されるネットワーク層アドレスのタイプを表します。
cbgpRoutePeer	ルート情報が学習されたピアのネットワーク層アドレスを表します。

MIB インデックス	説明
cbgpRouteAddrPrefix	BGP アップデート メッセージで伝送されるネットワーク アドレス プレフィックスを表します。 特定のタイプの AFI オブジェクトと SAFI オブジェクトに格納可能なネットワーク層アドレスのタイプについては、下の表を参照してください。
cbgpRouteAddrPrefixLen	NLRI フィールドのネットワーク アドレス プレフィックスのビット単位での長さを表します。 可能性のある 13 個のエントリの説明については、下の表を参照してください。

AFI と SAFI

下の表に、cbgpRouteAfi インデックスと cbgpRouteSafi インデックスに、割り当て可能であるか、またはそれらによって保持される AFI 値と SAFI 値を示します。下の表には、AFI と SAFI の特定の組み合わせによって保持可能なネットワーク アドレス プレフィックス タイプも示します。BGP アップデート メッセージで伝送可能なネットワーク アドレス プレフィックスのタイプは、AFI と SAFI の組み合わせによって異なります。

表 *73 : AFI と SAFI*

AFI	SAFI	タイプ
ipv4(1)	unicast(1)	IPv4 アドレス
ipv4(1)	multicast(2)	IPv4 アドレス
ipv4(1)	vpn(128)	VPN-IPv4 アドレス
ipv6(2)	unicast(1)	IPv6 アドレス

（注） VPN-IPv4 アドレスは 8 バイトのルート識別子（RD）で始まり、4 バイトの IPv4 アドレスで終わる 12 バイトの大きさです。cbgpRouteAddrPrefixLen で指定された長さを超えるすべてのビットは、ゼロで表されます。

NLRI フィールドのネットワーク アドレス プレフィックスの説明

下の表に cbgpRouteTable の NLRI フィールドのネットワーク アドレス プレフィックスのビット単位での長さを示します。テーブルの各エントリは、下の表の 6 つのいずれかのインデックスによって選択されるルートに関する情報を提供します。

表 *74 : NLRI* フィールドのネットワーク アドレス プレフィックスの説明

テーブルまたはオブジェクト（またはインデックス）	説明
cbgpRouteOrigin	ルート情報の最終的な起源。
cbgpRouteASPathSegment	自律システム パス セグメントのシーケンス。
cbgpRouteNextHop	トラフィックが宛先のネットワークに到達するために、通過する必要がある自律システム ボーダー ルータのネットワーク層アドレス。
cbgpRouteMedPresent	ルートの MULTI_EXIT_DISC 属性が存在するか存在しないかを示します。
cbgpRouteMultiExitDisc	隣接する自律システムへの複数の出力点を区別するために使われるメトリック。cbgpRouteMedPresent オブジェクトの値が「false(2)」の場合、このオブジェクトの値は関係ありません。
cbgpRouteLocalPrefPresent	ルートの LOCAL_PREF 属性が、存在するか存在しないかを示します。
cbgpRouteLocalPref	発信元の BGP スピーカーによってアドバイタイズされるルートのプリファレンスのレベルを指定します。 cbgRouteLocalPrefPresent オブジェクトの値が「false(2)」の場合、このオブジェクトの値は関係ありません。
cbgpRouteAtomicAggregate	システムが具体的なルートを選択せずに、あまり具体的でないルートを選択したかどうかを判断します。
cbgpRouteAggregatorAS	ルート集約を実行した最後の BGP スピーカーの自律システム番号。値 0 はこの属性が存在しないことを示します。
cbgpRouteAggregatorAddrType	cbgpRouteAggregatorAddr オブジェクトに格納されるネットワーク層アドレスのタイプを表します。
cbgpRouteAggregatorAddr	ルート集約を実行した最後の BGP 4 スピーカーのネットワーク層アドレス。すべて 0 の値は、この属性が存在しないことを示します。
cbgpRouteBest	このルートが最適な BGP 4 ルートとして選択されたかどうかを示します。
cbgpRouteUnknownAttr	ローカル BGP スピーカーによって理解されない 1 つ以上のパス属性。0 のサイズはこの属性が存在しないことを示します。

ピアごとの受信ルートに対する BGP 4 MIB サポートの利点

- SNMP クエリ機能の向上：プレフィックスの前にピア アドレスがインデックス化されるため、各ピアによってアドバタイズされるルートの SNMP クエリの検索条件が改善されます。ネットワーク オペレータは、ローカル BGP RIB テーブルの学習されたルートを取得するために、数千の可能性のあるルートをすべて検索する必要がなくなります。
- AIM および SAFI のサポートの向上：マルチプロトコル BGP のサポートが追加されます。AFI と SAFI がインデックスとしてテーブルに追加されました。CISCO-BGP4-MIB はローカル BGP スピーカーでサポートされる AFI と SAFI の任意の組み合わせで照会できます。

最大プレフィックス制限到達後の BGP ネイバーセッション再起動に関する追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2918	『*Route Refresh Capability for BGP-4*』
RFC 4486	『*Subcodes for BGP Cease Notification Message*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

ピアごとの受信ルートに対する BGP 4 MIB 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 *75* : ピアごとの受信ルートに対する *BGP 4 MIB* サポートの機能情報

機能名	リリース	機能情報
ピアごとの受信ルートに対する BGP 4 MIB サポート	Cisco IOS XE リリース 2.1	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。
BGP 受信ルート MIB	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。

用語集

AFI：Address Family Identifier（アドレス ファミリ識別子）。ネットワーク アドレスに関連付けられているネットワーク層プロトコルの ID を伝送します。

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。到達可能性情報を他の BGP システムと交換するドメイン間ルーティング プロトコル。これは、RFC 1163『A Border Gateway Protocol（BGP）』で定義されています。BGP の現在の実装は BGP バージョン 4（BGP4）です。BGP4 はインターネットで使われる主要なドメイン間ルーティング プロトコルです。BGP4 は CIDR をサポートし、ルート集約メカニズムを使用して、ルーティング テーブルのサイズを抑制します。

MBGP：Multiprotocol BGP（マルチプロトコル BGP）。BGP の拡張バージョンで、複数のネットワーク層プロトコル、および IP マルチキャスト ルートに関するルーティング情報を伝送します。これは、RFC 2858『Multiprotocol Extensions for BGP-4』で定義されています。

MIB：Management Information Base（管理情報ベース）。仮想情報ストアまたはデータベース内に格納されている管理対象オブジェクトのグループ。MIB オブジェクトは、その値をオブジェクト識別子に割り当てることができるように格納され、実装する必要がある MIB オブジェクトを定義することによって管理対象エージェントをサポートします。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

NLRI：Network Layer Reachability Information（ネットワーク層到達可能性情報）。ルートと宛先への接続方法を記述するルート属性を伝送します。この情報は BGP アップデート メッセージで伝送されます。BGP アップデート メッセージは 1 つ以上の NLRI プレフィックスを伝送できます。

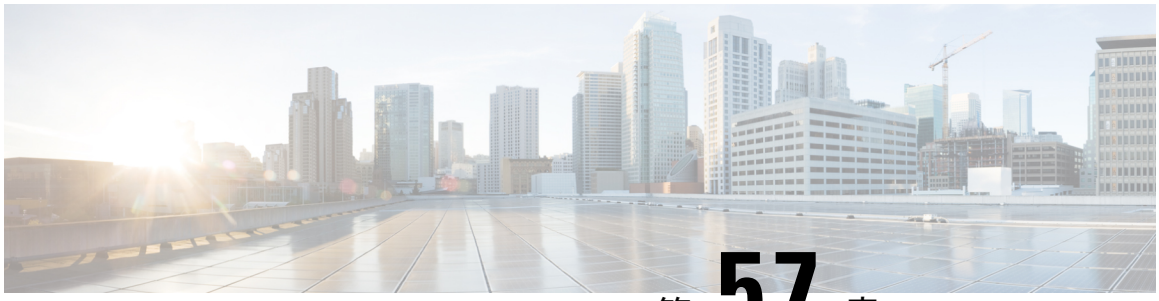
RIB：Routing Information Base（ルーティング情報ベース）。レイヤ 3 到達可能性情報および送信先 IP アドレスまたはプレフィックスを含むルートの中央リポジトリ。RIB は、ルーティング テーブルとも呼ばれます。

SAFI：Subsequent Address Family Identifier（後続アドレス ファミリ識別子）。属性で伝送されるネットワーク層到着可能性情報のタイプに関する追加情報を提供します。

SNMP：Simple Network Management Protocol（シンプル ネットワーク管理プロトコル）。TCP/IP ネットワークで、ほとんど排他的に使用されているネットワーク管理プロトコル。SNMP は、ネットワーク デバイスを監視し制御する手段、およびコンフィギュレーション、統計情報収集、パフォーマンス、およびセキュリティを管理する手段を提供します。

snmpwalk ：**snmpwalk** コマンドは、SNMP を使用したネットワーク エンティティ MIB との通信に使われる SNMP アプリケーションです。

VPN：バーチャル プライベート ネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。



第 57 章

L2VPN VPLS を使用したステートフルスイッチオーバー（SSO）によるノンストップルーティング（NSR）に対する BGP サポート

L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能により、プロバイダー エッジ（PE）ルータはカスタマー エッジ（CE）ルータとともにボーダー ゲートウェイ プロトコル（BGP）の状態を維持でき、ルート プロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的なインサービス ソフトウェア アップグレード（ISSU）中に、継続的なパケットの転送を確実に行えるようになります。CE ルータは、PE ルータの BGP NSR 機能の恩恵を受けるためにノンストップ フォワーディング（NSF）対応または NSF 認識である必要はありません。PE ルータだけをアップグレードし、BGP NSR をサポートする必要があります。CE ルータのアップグレードは必要ありません。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。

- 機能情報の確認 （996 ページ）
- NSR with SSO に対する BGP サポートの前提条件 （996 ページ）
- ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能に関する情報 （996 ページ）
- ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の設定方法 （998 ページ）
- ステートフル スイッチオーバー（SSO）による無停止ルーティング（NSR）に対する BGP サポート機能の設定例 （1007 ページ）
- その他の参考資料 （1009 ページ）
- NSR with SSO に対する BGP サポートの機能情報 （1010 ページ）

機能情報の確認

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

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

NSR with SSO に対する BGP サポートの前提条件

- BGP を実行するようにネットワークを設定する必要があります。
- マルチプロトコル レイヤ スイッチング（MPLS）レイヤ 3 VPN を設定する必要があります。
- NSF および SSO の概念や作業について十分に理解している必要があります。

ステートフルスイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能に関する情報

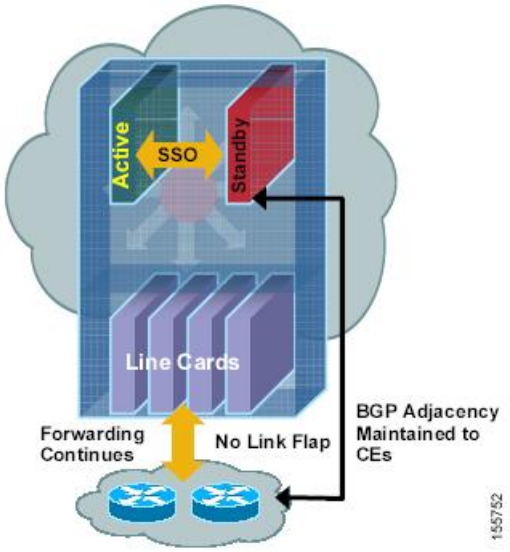
BGP NSR with SSO の概要

Cisco IOS Release 12.2(28)SB で BGP NSR with SSO が導入される以前は、BGP NSF に参加している隣接デバイスが NSF 対応であるか、または（BGP グレースフル リスタート メカニズムをサポートするようにデバイスを設定して）NSF 認識として設定する必要がありました。そのため、BGP NSF ではすべての隣接デバイスを BGP グレースフル リスタートをサポートする Cisco IOS ソフトウェア バージョンへアップグレードする必要がありました。ただし、多くの MPLS VPN 展開では、BGP グレースフル リスタートをサポートしておらず、プロバイダー（P）ルータと同じタイム フレームで BGP グレースフル リスタートがサポートされるソフトウェア バージョンにアップグレードできない CE ルータとの外部 BGP（eBGP）ピアリング セッションに PE ルータが関与していることがあります。

BGP NSR with SSO では、ハイ アベイラビリティ（HA）ソリューションをサービス プロバイダーに提供して、BGP グレースフル リスタートをサポートしない CE ルータとの eBGP ピアリ

ング関係に PE ルータが関与できるようにします。BGP NSR は SSO と連携して、アクティブ RP とスタンバイ RP との間で BGP 状態情報を同期化します。SSO により、スイッチオーバー後にユーザがネットワークを使用できない時間が最小限になります。BGP NSR with SSO 機能を設定した場合、RP のスイッチオーバー時に、PE ルータが BGP NSR with SSO を使用して、NSF 認識でない CE との eBGP ピアリング セッションに関する BGP 状態を維持します（下の図を参照）。また、BGP NSR with SSO 機能では、NSF 認識ピアを動的に検出し、CE ルータでのグレースフル リスタートを実行します。NSF 認識ピアとの eBGP ピアリング セッションと、サービス プロバイダー コアの BGP ルート リフレクタ（RR）との内部 BGP（iBGP）セッションでは、PE が NSF を使用して BGP 状態を維持します。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。

図 *80 : RP* スイッチオーバー時の *BGP NSR with SSO* 操作



BGP NSR with SSO は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレート コンフィギュレーションでサポートされます。BGP ピアおよび BGP ピア グループ コンフィギュレーションで BGP NSR with SSO サポートを設定するには、IPv4 VRF アドレス ファミリ BGP ピア セッションのアドレス ファミリ コンフィギュレーション モードで **neighbor ha-mode sso** コマンドを使用します。ピア セッション テンプレートで Cisco BGP NSR with SSO のサポートを含めるには、セッション テンプレート コンフィギュレーション モードで **ha-mode sso** コマンドを使用します。

BGP NSR with SSO の利点

- サービスの中断を最小限に抑える：ステートフル スイッチオーバー（SSO）によるボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）により、ルート プロセッサ（RP）スイッチオーバー時（スケジュール済みイベントまたはスケジュールされていないイベント）にお客様のトラフィックに与える影響が少なくなり、エッジでの高可用性（HA）の展開および利点が拡張されます。

- エッジにおける高可用性ノンストップ フォワーディング（NSF）および SSO 展開を拡大する：BGP NSR with SSO では、NSR 機能を使用してプロバイダー エッジをアップグレードすることにより、段階的な展開が可能です。これにより、お客様側のエッジデバイスは自動的に同期され、お客様側にあるシスコ製または他社製のカスタマー エッジ デバイスでの調整や NSF 認識が不要になります。BGP NSR 機能では、NSF 認識ピアを動的に検出して、そのような CE デバイスとのグレースフル リスタートを実行します。
- 透過的ルート収束を提供する：BGP NSR with SSO では、アクティブ RP とスタンバイ RP の両方で BGP 状態を維持することにより、ルート フラップを取り除き、パケット転送を継続して RP フェールオーバー時のパケット損失を最小限に抑えます。

ステートフルスイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の設定方法

BGP NSR with SSO をサポートする PE デバイスの設定

プロバイダー エッジ（PE）デバイスがカスタマー エッジ（CE）デバイスとの BGP 状態を維持し、ルート プロセッサ（RP）スイッチオーバー時または計画された ISSU 時にパケット転送を継続できるようにするには、次の作業を実行します。ステートフル スイッチオーバー（SSO）によるボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）により、BGP グレースフル リスタートをサポートするための CE デバイスのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともにノンストップ フォワーディング（NSF）の利点を提供できます。

BGP NSR with SSO は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレート コンフィギュレーションでサポートされます。BGP NSR with SSO のサポートをピア、ピア グループ、セッション テンプレートのどのコンフィギュレーションで設定するかに応じて、PE デバイスでこの項の次のいずれかの作業を実行します。

前提条件

- これらの作業は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレートの概念に精通していることを前提にしています。詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。
- アクティブ RP およびスタンバイ RP が SSO モードになっている必要があります。SSO モードの設定については、『*High Availability Configuration Guide*』の「Configuring Stateful Switchover」モジュールを参照してください。
- PE デバイスでグレースフル リスタートが有効になっている必要があります。プロバイダー コアで BGP NSF に参加するすべての BGP ピアでグレースフル リスタートをイネーブルに

することをお勧めします。グレースフル リスタートの設定の詳細については、「BGP の拡張機能の設定」モジュールを参照してください。

- CE デバイスは、ルート リフレッシュ機能をサポートしていなければなりません。詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。

BGP NSR with SSO をサポートするピアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*]
5. **address-family ipv4 vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **ha-mode sso**
8. **neighbor** *ip-address* **activate**
9. **end**
10. **show ip bgp vpnv4 all sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart`	ボーダー ゲートウェイ プロトコル（BGP）グレースフル リスタート機能と BGP ノンストップ フォワーディング（NSF）認識を有効にします。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。

	コマンドまたはアクション	目的
		• このコマンドは、再起動デバイスとそのすべてのピア（NSF 対応と NSF 認識）で使用してください。
ステップ 5	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf test`	IPv4 VRF アドレス ファミリ セッションでアドレス ファミリ コンフィギュレーション モードを開始します。 • **vrf** キーワードおよび *vrf-name* 引数は、*IPv4 VRF* インスタンス情報が交換されることを示します。 （注） この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするようにネイバーを設定します。
ステップ 8	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor testgroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。 （注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、ユニキャスト アドレス プレフィックスだけを交換します。
ステップ 9	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp vpnv4 all sso summary** 例：	（任意）SSO モードである BGP ネイバーの番号を表示します。

	コマンドまたはアクション	目的
	`Device# show ip bgp vpnv4 all sso summary`	

BGP NSR with SSO をサポートするピア グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*]
5. **address-family ipv4 vrf** *vrf-name*
6. **neighbor** *peer-group-name* **peer-group**
7. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
8. **neighbor** *ip-address* **peer-group** *peer-group-name*
9. **neighbor** *peer-group-name* **ha-mode sso**
10. **neighbor** *peer-group-name* **activate**
11. **end**
12. **show ip bgp vpnv4 all sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart`	ボーダー ゲートウェイ プロトコル（BGP）グレースフル リスタート機能と BGP ノンストップ フォワーディング（NSF）認識を有効にします。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換す

	コマンドまたはアクション	目的
		る機能のセッションを再開する必要があります。 • このコマンドは、再起動デバイスとそのすべてのピア（NSF 対応と NSF 認識）で使用してください。
ステップ 5	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf cisco`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **vrf** キーワードおよび *vrf-name* 引数は、IPv4 VRF インスタンス情報が交換されることを示します。 （注） この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 6	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router-af)# neighbor testgroup peer-group`	BGP ピア グループを作成します。
ステップ 7	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 8	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 peer-group testgroup`	BGP ネイバーの IP アドレスを BGP ピア グループに割り当てます。
ステップ 9	**neighbor** *peer-group-name* **ha-mode sso** 例： `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするように BGP ピア グループを設定します。
ステップ 10	**neighbor** *peer-group-name* **activate** 例：	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。

	コマンドまたはアクション	目的
	`Device(config-router-af)# neighbor testgroup activate`	
ステップ 11	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了し、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	**show ip bgp vpnv4 all sso summary** 例： `Device# show ip bgp vpnv4 all sso summary`	（任意）SSO モードである BGP ネイバーの番号を表示します。

BGP NSR with SSO をサポートするピア セッション テンプレートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **ha-mode sso**
6. **exit-peer-session**
7. **end**
8. **show ip bgp template peer-session** [*session-template-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 101`	ルータ コンフィギュレーション モードを開始して、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
ステップ 4	**template peer-session** *session-template-name* 例： `Device(config-router)# template peer-session CORE1`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**ha-mode sso** 例： `Device(config-router-stmp)# ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするようにネイバーを設定します。
ステップ 6	**exit-peer-session** 例： `Device(config-router-stmp)# exit-peer-session`	セッション テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
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 bgp template peer-session** [*session-template-name*] 例： `Device# show ip bgp template peer-session`	（任意）ローカル設定のピア セッション テンプレートを表示します。 • *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

ピア セッション テンプレートの設定の詳細については、『*Cisco IOS IP Routing: BGP Configuration Guide*』の「基本 BGP ネットワークの設定」の章を参照してください。

NSR with SSO の BGP サポートの確認

手順の概要

1. **enable**
2. **show ip bgp vpnv4 all sso summary**
3. **show ip bgpl2vpnvpls all neighbors**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

例：

```
Device> enable
```

ステップ 2 show ip bgp vpnv4 all sso summary

このコマンドは、ステートフル スイッチオーバー（SSO）モードであるボーダー ゲートウェイ プロトコル（BGP）ネイバーの番号を表示するために使用します。

次に、**show ip bgp vpnv4 all sso summary** コマンドの出力例を示します。

例：

```
Device# show ip bgp vpnv4 all sso summary
   Stateful switchover support enabled for 40 neighbors
```

ステップ 3 show ip bgpl2vpnvpls all neighbors

このコマンドは、BGP テーブルの VPN アドレス情報を表示します。

次に、**show ip bgp l2vpnvpls all neighbors** コマンドの出力例を示します。[Stateful switchover support] フィールドは、SSO が有効か無効かを示します。[SSO Last Disable Reason] フィールドは、SSO 機能が失われた最後の BGP セッションに関する情報を表示します。

例：

```
Device# show ip bgp l2vpn vpls all neighbors 10.3.3.3
BGP neighbor is 10.3.3.3,  vrf vrf1,  remote AS 3, external link
  Inherits from template 10vrf-session for session parameters
   BGP version 4, remote router ID 10.1.105.12
   BGP state = Established, up for 04:21:39
   Last read 00:00:05, last write 00:00:09, hold time is 30, keepalive interval is 10 seconds
   Configured hold time is 30, keepalive interval is 10 seconds
   Minimum holdtime from neighbor is 0 seconds
   Neighbor capabilities:
     Route refresh: advertised and received(new)
     Address family IPv4 Unicast: advertised and received
     Stateful switchover support enabled
   Message statistics:
     InQ depth is 0
     OutQ depth is 0
                          Sent       Rcvd
     Opens:                  1          1
     Notifications:          0          0
     Updates:                1          4
     Keepalives:          1534       1532
     Route Refresh:          0          0
     Total:               1536       1537
   Default minimum time between advertisement runs is 30 seconds
  For address family: L2VPN VPLS
   BGP table version 25161, neighbor version 25161/0
   Output queue size : 0
```

```
   Index 7, Offset 0, Mask 0x80
   7 update-group member
   Inherits from template 10vrf-policy
   Overrides the neighbor AS with my AS before sending updates
   Outbound path policy configured
   Route map for outgoing advertisements is Deny-CE-prefixes
                                Sent       Rcvd
   Prefix activity:             ----       ----
     Prefixes Current:            10         50 (Consumes 3400 bytes)
     Prefixes Total:              10         50
     Implicit Withdraw:            0          0
     Explicit Withdraw:            0          0
     Used as bestpath:           n/a          0
     Used as multipath:          n/a          0
                                  Outbound    Inbound
   Local Policy Denied Prefixes:  --------    -------
     route-map:                        150          0
     AS_PATH loop:                     n/a        760
     Total:                            150        760
   Number of NLRIs in the update sent: max 10, min 10
   Address tracking is enabled, the RIB does have a route to 10.3.3.3
   Address tracking requires at least a /24 route to the peer
   Connections established 1; dropped 0
   Last reset never
   Transport(tcp) path-mtu-discovery is enabled
   TCP session must be opened passively
Connection state is ESTAB, I/O status: 1, unread input bytes: 0 Connection is ECN Disabled Local
host: 10.0.21.1, Local port: 179 Foreign host: 10.0.21.3, Foreign port: 51205 Connection tableid
(VRF): 1
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1625488):
Timer          Starts    Wakeups            Next
Retrans          1746        210             0x0
TimeWait            0          0             0x0
AckHold          1535       1525             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 2241977291  snduna: 2242006573  sndnxt: 2242006573     sndwnd:  13097
irs:  821359845  rcvnxt:  821391670  rcvwnd:      14883  delrcvwnd:   1501
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms Status Flags: passive open, retransmission timeout,
 gen tcbs
   0x1000
Option Flags: VRF id set, always push, md5
Datagrams (max data segment is 4330 bytes):
Rcvd: 3165 (out of order: 0), with data: 1535, total data bytes: 31824
Sent: 3162 (retransmit: 210 fastretransmit: 0),with data: 1537, total data
bytes: 29300
SSO Last Disable Reason: Application Disable (Active)
```

トラブルシューティングのヒント

BGP NSR with SSO をトラブルシューティングするには、必要に応じて特権 EXEC モードで次のコマンドを使用します。

- **debug ip bgp sso** ：BGP 関連の SSO イベント、またはアクティブ RP とスタンバイ RP の間の BGP に関連するインタラクションのデバッグ情報を表示します。このコマンドは、RP スイッチオーバー時または計画された ISSU 時に PE ルータの BGP セッションを監視またはトラブルシューティングを行う際に役立ちます。
- **debug ip tcp ha** ：TCP HA イベント、またはアクティブ RP とスタンバイ RP の間の TCP スタック インタラクションのデバッグ情報を表示します。このコマンドは、SSO 認識 TCP 接続のトラブルシューティングを行う際に役立ちます。
- **show tcp** ：TCP 接続の状態を表示します。ディスプレイ出力に SSO 機能フラグが表示され、TCP 接続で SSO プロパティがエラーになった理由が示されます。
- **show tcp ha connections** ：接続 ID から TCP のマッピング データを表示します。

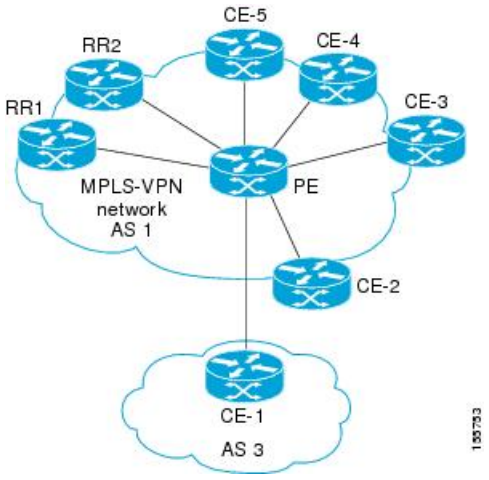
ステートフルスイッチオーバー（SSO）による無停止ルーティング（NSR）に対する BGP サポート機能の設定例

L2VPN VPLS を使用した BGP NSR with SSO の設定例

下の図に、BGP NSR with SSO ネットワーク トポロジの例を示します。その後の設定例では、トポロジ内の 3 つのルータである RR1 ルータ、PE ルータ、および CE-1 ルータの設定を示します。

（注） これらの設定例では、MPLS VPN に必要な一部の設定が省略されています。これらの例の目的は、BGP NSR with SSO の設定を示すことであるためです。

図 *81 : BGP NSR with SSO* のトポロジ例



RR1 の設定

次の例では、上の図の RR1 の BGP 設定を示します。RR1 は、NSF 認識ルート リフレクタとして設定されます。RP スイッチオーバー時に、PE ルータは NSF を使用して、RR1 との内部ピアリング セッションの BGP 状態を維持します。

```
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.2.2.2 remote-as 1
 neighbor 10.2.2.2 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.2.2.2 activate
 neighbor 10.2.2.2 send-community both
 neighbor 10.2.2.2 route-reflector-client
 exit-address-family
 !
```

PE の設定

次の例では、上の図の PE ルータの BGP NSR with SSO 設定を示します。PE ルータは、NSF 認識と BGP NSR with SSO 機能の両方をサポートするように設定されます。RP スイッチオーバー時に、PE ルータは BGP NSR with SSO を使用して、CE-1 ルータ（このトポロジでは NSF 認識ではない CE ルータ）との eBGP ピアリング セッションの BGP 状態を維持し、NSF を使用して RR1 との iBGP セッションの BGP 状態を維持します。また、PE ルータは MPLS VPN ネットワーク内に NSF 認識の CE ルータが他にあるかどうかを検出し、ある場合は、それらの CE ルータとのグレースフル リスタートを実行します。

```
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community both
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.3.3.3 remote-as 3
 neighbor 10.3.3.3 ha-mode sso
 neighbor 10.3.3.3 activate
 neighbor 10.3.3.3 as-override
 no auto-summary
 no synchronization
```

```
 exit-address-family
!
```

CE-1 の設定

次の例では、上の図の CE-1 の BGP 設定を示します。CE-1 ルータは、PE ルータの外部ピアとして設定されます。CE-1 ルータは、NSF 対応または NSF 認識として設定されません。ただし、PE ルータでの BGP NSR 機能のメリットを受けるために CE-1 ルータが NSF 対応や NSF 認識である必要や、BGP NSR をサポートするためにアップグレードする必要はありません。

```
!
router bgp 3
 neighbor 10.2.2.2 remote-as 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 IOS Master Commands List, All Releases』
BGP コマンド	『Cisco IOS BGP Command Reference』
MTR コマンド	『Cisco IOS Multitopology Routing Command Reference』
マルチトポロジ ルーティングの設定	『Multitopology Routing Configuration Guide』
iBGP ピアの BGP NSR サポート	『BGP Configuration Guide』
MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート	『BGP Configuration Guide』
BGP-IPV6 NSR	『BGP Configuration Guide』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

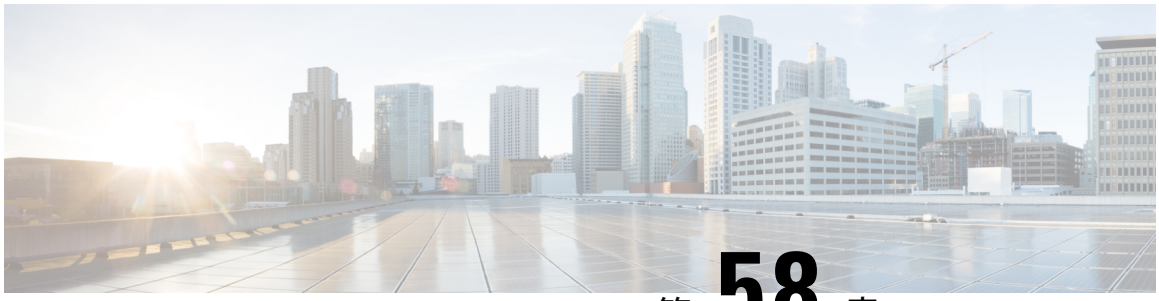
NSR with SSO に対する BGP サポートの機能情報

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 *76 : NSR with SSO* に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
NSR with SSO に対する BGP サポート	12.2(28)SB 15.0(1)S	ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能により、プロバイダー エッジ（PE）ルータはカスタマー エッジ（CE）ルータとともにボーダー ゲートウェイ プロトコル（BGP）の状態を維持でき、ルート プロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的なインサービス ソフトウェア アップグレード（ISSU）中に、継続的なパケットの転送を確実に行えるようになります。CE ルータは、PE ルータの BGP NSR 機能の恩恵を受けるためにノンストップ フォワーディング（NSF）対応または NSF 認識である必要はありません。PE ルータだけをアップグレードし、BGP NSR をサポートする必要があります。CE ルータのアップグレードは必要ありません。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。 次のコマンドが導入または変更されました。 • **debug ip bgp sso** • **debug ip tcp ha** • **neighbor ha-mode sso** • **show ip bgp vpnv4** • **show ip bgp vpnv4 all sso summary** • **show tcp** • **show tcp ha connections**
BGP—NSR 機能拡張	Cisco IOS Release XE 3.13S	BGP NSR およびグレースフル リスタートに優先する NSR に対するグローバル サポートが有効になりました。 オプションのキーワード **prefer** が **bgp ha-mode sso** コマンドに追加されました。



第 58 章

L2VPN VPLS を使用したステートフルスイッチオーバー（SSO）によるノンストップルーティング（NSR）に対する BGP サポート

L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能により、プロバイダー エッジ（PE）ルータはカスタマー エッジ（CE）ルータとともにボーダー ゲートウェイ プロトコル（BGP）の状態を維持でき、ルート プロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的なインサービス ソフトウェア アップグレード（ISSU）中に、継続的なパケットの転送を確実に行えるようになります。CE ルータは、PE ルータの BGP NSR 機能の恩恵を受けるためにノンストップ フォワーディング（NSF）対応または NSF 認識である必要はありません。PE ルータだけをアップグレードし、BGP NSR をサポートする必要があります。CE ルータのアップグレードは必要ありません。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。

- NSR with SSO に対する BGP サポートの前提条件 （1014 ページ）
- ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能に関する情報 （1014 ページ）
- ステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の設定方法 （1016 ページ）
- L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポートの設定例 （1025 ページ）
- その他の参考資料 （1027 ページ）
- L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の機能情報 （1028 ページ）

NSR with SSO に対する BGP サポートの前提条件

- BGP を実行するようにネットワークを設定する必要があります。
- マルチプロトコル レイヤ スイッチング（MPLS）レイヤ 3 VPN を設定する必要があります。
- NSF および SSO の概念や作業について十分に理解している必要があります。

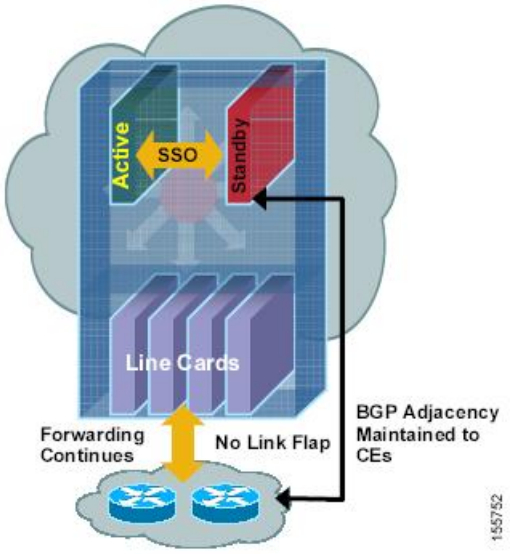
ステートフルスイッチオーバー（SSO）によるノンストップルーティング（NSR）に対する BGP サポート機能に関する情報

BGP NSR with SSO の概要

Cisco IOS Release 12.2(28)SB で BGP NSR with SSO が導入される以前は、BGP NSF に参加している隣接デバイスが NSF 対応であるか、または（BGP グレースフル リスタート メカニズムをサポートするようにデバイスを設定して）NSF 認識として設定する必要がありました。そのため、BGP NSF ではすべての隣接デバイスを BGP グレースフル リスタートをサポートする Cisco IOS ソフトウェア バージョンへアップグレードする必要がありました。ただし、多くの MPLS VPN 展開では、BGP グレースフル リスタートをサポートしておらず、プロバイダー（P）ルータと同じタイム フレームで BGP グレースフル リスタートがサポートされるソフトウェア バージョンにアップグレードできない CE ルータとの外部 BGP（eBGP）ピアリング セッションに PE ルータが関与していることがあります。

BGP NSR with SSO では、ハイ アベイラビリティ（HA）ソリューションをサービス プロバイダーに提供して、BGP グレースフル リスタートをサポートしない CE ルータとの eBGP ピアリング関係に PE ルータが関与できるようにします。BGP NSR は SSO と連携して、アクティブ RP とスタンバイ RP との間で BGP 状態情報を同期化します。SSO により、スイッチオーバー後にユーザがネットワークを使用できない時間が最小限になります。BGP NSR with SSO 機能を設定した場合、RP のスイッチオーバー時に、PE ルータが BGP NSR with SSO を使用して、NSF 認識でない CE との eBGP ピアリング セッションに関する BGP 状態を維持します（下の図を参照）。また、BGP NSR with SSO 機能では、NSF 認識ピアを動的に検出し、CE ルータでのグレースフル リスタートを実行します。NSF 認識ピアとの eBGP ピアリング セッションと、サービス プロバイダー コアの BGP ルート リフレクタ（RR）との内部 BGP（iBGP）セッションでは、PE が NSF を使用して BGP 状態を維持します。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。

図 *82 : RP* スイッチオーバー時の *BGP NSR with SSO* 操作



BGP NSR with SSO は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレート コンフィギュレーションでサポートされます。BGP ピアおよび BGP ピア グループ コンフィギュレーションで BGP NSR with SSO サポートを設定するには、IPv4 VRF アドレス ファミリ BGP ピア セッションのアドレス ファミリ コンフィギュレーション モードで **neighbor ha-mode sso** コマンドを使用します。ピア セッション テンプレートで Cisco BGP NSR with SSO のサポートを含めるには、セッション テンプレート コンフィギュレーション モードで **ha-mode sso** コマンドを使用します。

BGP NSR with SSO の利点

- サービスの中断を最小限に抑える：ステートフル スイッチオーバー（SSO）によるボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）により、ルート プロセッサ（RP）スイッチオーバー時（スケジュール済みイベントまたはスケジュールされていないイベント）にお客様のトラフィックに与える影響が少なくなり、エッジでの高可用性（HA）の展開および利点が拡張されます。
- エッジにおける高可用性ノンストップ フォワーディング（NSF）および SSO 展開を拡大する：BGP NSR with SSO では、NSR 機能を使用してプロバイダー エッジをアップグレードすることにより、段階的な展開が可能です。これにより、お客様側のエッジデバイスは自動的に同期され、お客様側にあるシスコ製または他社製のカスタマー エッジ デバイスでの調整や NSF 認識が不要になります。BGP NSR 機能では、NSF 認識ピアを動的に検出して、そのような CE デバイスとのグレースフル リスタートを実行します。
- 透過的ルート収束を提供する：BGP NSR with SSO では、アクティブ RP とスタンバイ RP の両方で BGP 状態を維持することにより、ルート フラップを取り除き、パケット転送を継続して RP フェールオーバー時のパケット損失を最小限に抑えます。

ステートフルスイッチオーバー（SSO）によるノンストップルーティング（NSR）に対するBGPサポート機能の設定方法

BGP NSR with SSO をサポートする PE デバイスの設定

プロバイダー エッジ（PE）デバイスがカスタマー エッジ（CE）デバイスとの BGP 状態を維持し、ルートプロセッサ（RP）スイッチオーバー時または計画されたISSU時にパケット転送を継続できるようにするには、次の作業を実行します。ステートフルスイッチオーバー（SSO）によるボーダーゲートウェイプロトコル（BGP）ノンストップルーティング（NSR）により、BGPグレースフルリスタートをサポートするためのCEデバイスのアップグレードを必要とせずに、サービス プロバイダーはNSRのさらなる利点とともにノンストップ フォワーディング（NSF）の利点を提供できます。

BGP NSR with SSO は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレート コンフィギュレーションでサポートされます。BGP NSR with SSO のサポートをピア、ピア グループ、セッション テンプレートのどのコンフィギュレーションで設定するかに応じて、PE デバイスでこの項の次のいずれかの作業を実行します。

前提条件

- これらの作業は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレートの概念に精通していることを前提にしています。詳細については、「基本BGPネットワークの設定」モジュールを参照してください。
- アクティブ RP およびスタンバイ RP が SSO モードになっている必要があります。SSO モードの設定については、『*High Availability Configuration Guide*』の「Configuring Stateful Switchover」モジュールを参照してください。
- PEデバイスでグレースフルリスタートが有効になっている必要があります。プロバイダーコアでBGP NSFに参加するすべてのBGPピアでグレースフルリスタートをイネーブルにすることをお勧めします。グレースフル リスタートの設定の詳細については、「BGP の拡張機能の設定」モジュールを参照してください。
- CE デバイスは、ルート リフレッシュ機能をサポートしていなければなりません。詳細については、「基本 BGP ネットワークの設定」モジュールを参照してください。

BGP NSR with SSO をサポートするピアの設定

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*]
5. **address-family ipv4 vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **ha-mode sso**
8. **neighbor** *ip-address* **activate**
9. **end**
10. **show ip bgp vpnv4 all sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart`	ボーダー ゲートウェイ プロトコル（BGP）グレースフル リスタート機能と BGP ノンストップ フォワーディング（NSF）認識を有効にします。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。 • このコマンドは、再起動デバイスとそのすべてのピア（NSF 対応と NSF 認識）で使用してください。
ステップ 5	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf test`	IPv4 VRF アドレス ファミリ セッションでアドレス ファミリ コンフィギュレーション モードを開始します。 • **vrf** キーワードおよび *vrf-name* 引数は、*IPv4 VRF* インスタンス情報が交換されることを示します。

	コマンドまたはアクション	目的
		（注） この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするようにネイバーを設定します。
ステップ 8	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor testgroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカル ルータと交換できるようにします。 （注） デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、ユニキャスト アドレス プレフィックスだけを交換します。
ステップ 9	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 10	**show ip bgp vpnv4 all sso summary** 例： `Device# show ip bgp vpnv4 all sso summary`	（任意）SSO モードである BGP ネイバーの番号を表示します。

BGP NSR with SSO をサポートするピア グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds*] [**stalepath-time** *seconds*]

5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **peer-group** *peer-group-name*
8. **neighbor** *peer-group-name* **ha-mode sso**
9. **address-family l2vpn vpls**
10. **neighbor** *peer-group-name* **activate**
11. **end**
12. **show ip bgp l2vpn vpls all sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] 例： `Device(config-router)# bgp graceful-restart`	ボーダー ゲートウェイ プロトコル（BGP）グレースフル リスタート機能と BGP ノンストップ フォワーディング（NSF）認識を有効にします。 • BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。 • このコマンドは、再起動デバイスとそのすべてのピア（NSF 対応と NSF 認識）で使用してください。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router-af)# neighbor testgroup peer-group`	BGP ピア グループを作成します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 7	**neighbor** *ip-address* **peer-group** *peer-group-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 peer-group testgroup`	BGP ネイバーの IP アドレスを BGP ピア グループに割り当てます。
ステップ 8	**neighbor** *peer-group-name* **ha-mode sso** 例： `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするように BGP ピア グループを設定します。
ステップ 9	**address-family l2vpn vpls** 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN VPLS ピアリングのアクティブ化を指定します。
ステップ 10	**neighbor** *peer-group-name* **activate** 例： `Device(config-router-af)# neighbor testgroup activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。
ステップ 11	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了し、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	**show ip bgp l2vpn vpls all sso summary** 例： `Device# show ip bgp l2vpn vpls all sso summary`	（任意）SSO モードである BGP ネイバーの番号を表示します。

BGP NSR with SSO をサポートするピア セッション テンプレートの設定

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **ha-mode sso**
6. **exit-peer-session**
7. **end**
8. **show ip bgp template peer-session** [*session-template-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
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 101`	ルータ コンフィギュレーション モードを開始して、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを作成します。
ステップ 4	**template peer-session** *session-template-name* 例： `Device(config-router)# template peer-session CORE1`	セッション テンプレート コンフィギュレーション モードを開始して、ピア セッション テンプレートを作成します。
ステップ 5	**ha-mode sso** 例： `Device(config-router-stmp)# ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートするようにネイバーを設定します。
ステップ 6	**exit-peer-session** 例： `Device(config-router-stmp)# exit-peer-session`	セッション テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
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。

	コマンドまたはアクション	目的
ステップ 8	**show ip bgp template peer-session** [*session-template-name*] 例： `Device# show ip bgp template peer-session`	（任意）ローカル設定のピア セッション テンプレートを表示します。 • *session-template-name* 引数を使用して、ピア ポリシー テンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

次の作業

ピア セッション テンプレートの作成後、ピア セッション テンプレートのコンフィギュレーションは、**inherit peer-session** コマンド、または **neighbor inherit peer-session** コマンドを使って、別のピア セッション テンプレートに継承させる、または適用することができます。

ピア セッション テンプレートの設定の詳細については、『*Cisco IOS IP Routing: BGP Configuration Guide*』の「基本 BGP ネットワークの設定」の章を参照してください。

NSR with SSO の BGP サポートの確認

手順の概要

1. **enable**
2. **show ip bgpl2vpnvpls all sso summary**
3. **show ip bgpl2vpnvpls all neighbors**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。

例：

```
Device> enable
```

ステップ 2 **show ip bgpl2vpnvpls all sso summary**

このコマンドは、ステートフルスイッチオーバー（SSO）モードであるボーダーゲートウェイプロトコル（BGP）ネイバーの番号を表示するために使用します。

次に、**show ip bgp l2vpnvpls all sso summary** コマンドの出力例を示します。

例：

```
Device# show ip bgp l2vpn vpls all sso summary
   Stateful switchover support enabled for 40 neighbors
```

ステップ 3　show ip bgpl2vpnvpls all neighbors

このコマンドは、BGP テーブルの VPN アドレス情報を表示します。

次に、**show ip bgp l2vpnvpls all neighbors** コマンドの出力例を示します。[Stateful switchover support] フィールドは、SSO が有効か無効かを示します。[SSO Last Disable Reason] フィールドは、SSO 機能が失われた最後の BGP セッションに関する情報を表示します。

例：

```
Device# show ip bgp l2vpn vpls all neighbors 10.3.3.3
BGP neighbor is 10.3.3.3,  vrf vrf1,  remote AS 3, external link
  Inherits from template 10vrf-session for session parameters
   BGP version 4, remote router ID 10.1.105.12
   BGP state = Established, up for 04:21:39
   Last read 00:00:05, last write 00:00:09, hold time is 30, keepalive interval is 10 seconds
   Configured hold time is 30, keepalive interval is 10 seconds
   Minimum holdtime from neighbor is 0 seconds
   Neighbor capabilities:
     Route refresh: advertised and received(new)
     Address family IPv4 Unicast: advertised and received
     Stateful switchover support enabled
   Message statistics:
     InQ depth is 0
     OutQ depth is 0
                         Sent       Rcvd
     Opens:                 1          1
     Notifications:         0          0
     Updates:               1          4
     Keepalives:         1534       1532
     Route Refresh:         0          0
     Total:              1536       1537
   Default minimum time between advertisement runs is 30 seconds
  For address family: L2VPN VPLS
   BGP table version 25161, neighbor version 25161/0
   Output queue size : 0
   Index 7, Offset 0, Mask 0x80
   7 update-group member
   Inherits from template 10vrf-policy
   Overrides the neighbor AS with my AS before sending updates
   Outbound path policy configured
   Route map for outgoing advertisements is Deny-CE-prefixes
                               Sent       Rcvd
   Prefix activity:            ----       ----
     Prefixes Current:           10         50 (Consumes 3400 bytes)
     Prefixes Total:             10         50
     Implicit Withdraw:           0          0
     Explicit Withdraw:           0          0
     Used as bestpath:          n/a          0
     Used as multipath:         n/a          0
                                 Outbound    Inbound
   Local Policy Denied Prefixes:    --------    -------
     route-map:                          150          0
     AS_PATH loop:                       n/a        760
     Total:                              150        760
   Number of NLRIs in the update sent: max 10, min 10
   Address tracking is enabled, the RIB does have a route to 10.3.3.3
   Address tracking requires at least a /24 route to the peer
   Connections established 1; dropped 0
   Last reset never
   Transport(tcp) path-mtu-discovery is enabled
   TCP session must be opened passively
Connection state is ESTAB, I/O status: 1, unread input bytes: 0 Connection is ECN Disabled Local
```

```
host: 10.0.21.1, Local port: 179 Foreign host: 10.0.21.3, Foreign port: 51205 Connection tableid
(VRF): 1
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1625488):
Timer          Starts    Wakeups            Next
Retrans          1746        210             0x0
TimeWait            0          0             0x0
AckHold          1535       1525             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 2241977291  snduna: 2242006573  sndnxt: 2242006573     sndwnd:  13097
irs:  821359845  rcvnxt:  821391670  rcvwnd:      14883  delrcvwnd:   1501
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms Status Flags: passive open, retransmission timeout,
 gen tcbs
   0x1000
Option Flags: VRF id set, always push, md5
Datagrams (max data segment is 4330 bytes):
Rcvd: 3165 (out of order: 0), with data: 1535, total data bytes: 31824
Sent: 3162 (retransmit: 210 fastretransmit: 0),with data: 1537, total data
bytes: 29300
SSO Last Disable Reason: Application Disable (Active)
```

トラブルシューティングのヒント

BGP NSR with SSO をトラブルシューティングするには、必要に応じて特権 EXEC モードで次のコマンドを使用します。

- **debug ip bgp sso** ：BGP 関連の SSO イベント、またはアクティブ RP とスタンバイ RP の間の BGP に関連するインタラクションのデバッグ情報を表示します。このコマンドは、RP スイッチオーバー時または計画された ISSU 時に PE ルータの BGP セッションを監視またはトラブルシューティングを行う際に役立ちます。
- **debug ip tcp ha** ：TCP HA イベント、またはアクティブ RP とスタンバイ RP の間の TCP スタック インタラクションのデバッグ情報を表示します。このコマンドは、SSO 認識 TCP 接続のトラブルシューティングを行う際に役立ちます。
- **show tcp** ：TCP 接続の状態を表示します。ディスプレイ出力に SSO 機能フラグが表示され、TCP 接続で SSO プロパティがエラーになった理由が示されます。
- **show tcp ha connections** ：接続 ID から TCP のマッピング データを表示します。

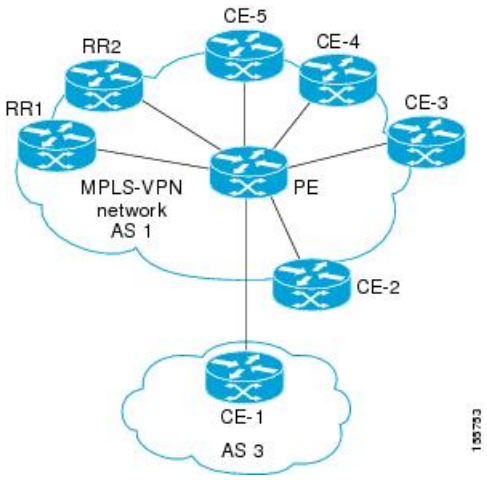
L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポートの設定例

例：L2VPN VPLS を使用した BGP NSR with SSO の設定

下の図に、L2VPN VPLS テクノロジーを使用したステートフル スイッチオーバー（SSO）によるボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）ネットワーク トポロジの例を示します。その後の設定例では、トポロジ内の 2 つのデバイスである RR1 デバイスおよびプロバイダー エッジ（PE）デバイスの設定を示します。

（注） これらの設定例では、マルチプロトコル ラベル スイッチング（MPLS）VPN に必要な一部の設定が省略されています。これらの例の目的は、BGP NSR with SSO の設定を示すことであるためです。

図 *83 : BGP NSR with SSO* のトポロジ例



RR1 の設定

次の例では、上の図の RR1 の BGP 設定を示します。RR1 は、ノンストップ フォワーディング（NSF）認識ルート リフレクタ（RR）として設定されます。ルート リフレクタ（RR）スイッチオーバー時に、PE デバイスは NSF を使用して、RR1 との内部ピアリング セッションの BGP 状態を維持します。

```
!
router bgp 1
 no synchronization
```

```
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.2.2.2 remote-as 1
 neighbor 10.2.2.2 update-source Loopback0
 no auto-summary
 !
 address-family l2vpn vpls
 neighbor 10.2.2.2 activate
 neighbor 10.2.2.2 send-community both
 neighbor 10.2.2.2 route-reflector-client
 exit-address-family
 !
```

PE の設定

次の例では、上の図の PE デバイスの BGP NSR with SSO 設定を示します。PE デバイスは、NSF 認識と BGP NSR with SSO 機能の両方をサポートするように設定されます。RP スイッチオーバー時に、PE デバイスは BGP NSR with SSO を使用して外部 BGP（eBGP）ピアリング セッションの BGP 状態を維持し、NSF を使用して RR1 との内部 BGP（iBGP）セッションの BGP 状態を維持します。

```
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback0
 neighbor 10.3.3.3 remote-as 3
 neighbor 10.3.3.3 ha-mode sso
 neighbor 10.3.3.3 activate
 neighbor 10.3.3.3 as-override
 no auto-summary
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community both
 exit-address-family
 !
 no auto-summary
 no synchronization
 exit-address-family
!
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
BGP コマンド	『Cisco IOS BGP Command Reference』
MTR コマンド	『Cisco IOS Multitopology Routing Command Reference』
マルチトポロジ ルーティングの設定	『Multitopology Routing Configuration Guide』
iBGP ピアの BGP NSR サポート	『BGP Configuration Guide』
MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート	『BGP Configuration Guide』
BGP-IPV6 NSR	『BGP Configuration Guide』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

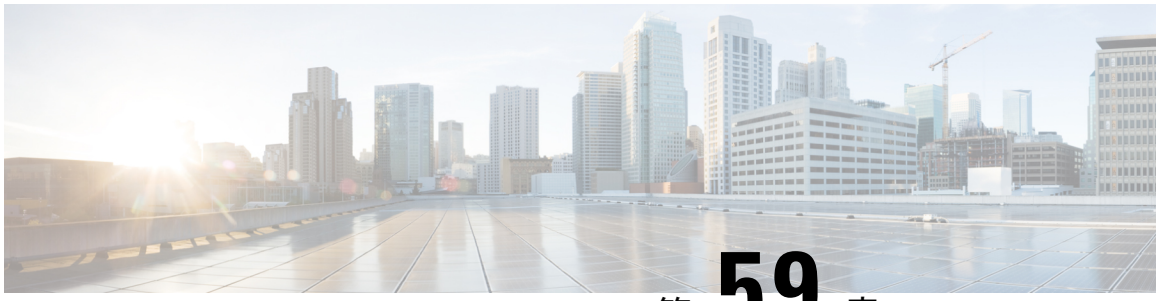
L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート機能の機能情報

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 *77*：ステートフル スイッチオーバー（*SSO*）による無停止ルーティング（*NSR*）に対する *BGP* サポート機能の機能情報

機能名	リリース	機能情報
L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップ ルーティング（NSR）に対する BGP サポート	Cisco IOS XE Fuji 16.7.1	L2VPN VPLS を使用したステートフル スイッチオーバー（SSO）によるノンストップルーティング（NSR）に対する BGP サポート機能により、プロバイダー エッジ（PE）ルータはカスタマーエッジ（CE）ルータとともにボーダー ゲートウェイ プロトコル（BGP）の状態を維持でき、ルート プロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的なインサービス ソフトウェア アップグレード（ISSU）中に、継続的なパケットの転送を確実に行えるようになります。CE ルータは、PE ルータの BGP NSR 機能の恩恵を受けるためにノンストップ フォワーディング（NSF）対応または NSF 認識である必要はありません。PE ルータだけをアップグレードし、BGP NSR をサポートする必要があります。CE ルータのアップグレードは必要ありません。さらに、BGP NSR with SSO により、BGP グレースフル リスタートをサポートするための CE ルータのアップグレードを必要とせずに、サービス プロバイダーは NSR のさらなる利点とともに NSF の利点を提供できます。 次のコマンドが変更されました。 • **debug ip bgp sso** • **show ip bgp l2vpn**



第 59 章

BGP NSR 自動検知

BGP NSR 自動検知機能は、ルート プロセッサ（RP）のフェールオーバー時に不要なチャーンを削減するために実装されたデフォルトの動作です。この機能が導入される前は、アクティブ RP がダウンすると、ボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）の提供を引き継いだ新しいアクティブ RP が、NSR を使用して設定されたすべてのピアに対して、ルートリフレッシュ リクエストを送信していました。しかし、新しいアクティブ RP は、スタンバイ RP として機能している間にすべての着信アップデートをすでに受信しています。ルートリフレッシュ リクエストの送信により、スイッチオーバー時に不要な BGP チャーンが発生していました。この機能は、デフォルトで、このようなルートリフレッシュ リクエストの送信を防止します。また、この機能は、ルートリフレッシュ機能がないピアに対しても NSR サポートを提供します。ルートリフレッシュ リクエストの送信を以前の動作に戻す必要がある場合は、新しいコマンドを使用して戻すことができます。

- 機能情報の確認 （1029 ページ）
- BGP NSR 自動検知に関する情報 （1030 ページ）
- BGP NSR 自動検知機能を無効にする方法 （1030 ページ）
- BGP NSR 自動検知の設定例 （1032 ページ）
- その他の参考資料 （1032 ページ）
- BGP NSR 自動検知の機能情報 （1033 ページ）

機能情報の確認

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

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

BGP NSR 自動検知に関する情報

BGP NSR 自動検知の利点

BGP NSR 自動検知機能には、次の利点があります。

- この機能は、ルート プロセッサ（RP）のフェールオーバー時に不要なチャーンを削減するデフォルトの動作です。この機能が導入される前は、アクティブ RP がダウンすると、BGP ノンストップ ルーティング（NSR）の提供を引き継いだ新しいアクティブ RP が、NSR を使用して設定されたすべてのピアに対して、ルートリフレッシュ リクエストを送信していました。しかし、新しいアクティブ RP は、スタンバイ RP として機能している間にすべての着信アップデートをすでに受信しています。ルート リフレッシュ リクエストの送信により、スイッチオーバー時に不要な BGP チャーンが発生していました。この機能は、デフォルトで、このようなルートリフレッシュリクエストの送信を防止します。
- また、この機能は、ルートリフレッシュ機能がないピアに対しても NSR サポートを提供します。この機能が導入される前は、ルートリフレッシュ機能がないピアでは NSR はサポートされていませんでした。
- この機能を設定する必要はありません。これは、この機能が実装されているリリースでのデフォルトの動作です。
- RP がダウンしたときは新しいアクティブ RP がルートリフレッシュ リクエストを送信するという以前の動作に戻す必要がある場合は、**bgp sso route-refresh-enable** コマンドを使用できます。

自動検知のない NSR に戻した場合の結果

場合により、BGP NSR 自動検知機能のデフォルト動作が必要ないことも考えられます。RP がダウンしたときは新しいアクティブ RP がルートリフレッシュ リクエストを送信するという以前の動作に戻す必要がある場合は、**bgp sso route-refresh-enable** コマンドを使用できます。この操作により、受信した OPEN メッセージでルートリフレッシュ機能を交換しなかったピアでは、NSR サポートが無効になります。

BGP NSR 自動検知機能を無効にする方法

BGP NSR 自動検知機能の無効化

BGP NSR 自動検知機能は、デフォルトで有効になっています。この作業は、この機能を無効にする必要がある場合にのみ実行してください。たとえば、スイッチオーバーの時点でアドバタイズされていたルートが、何らかの理由により、スタンバイ RP（新しいアクティブ RP）で処理されなかった場合などがあります。そのような場合は、ピアがアドバタイズしたすべての

ルートを要求するルートリフレッシュを送信すると役に立つことがあります。この作業の実行後は、フェールオーバーが発生すると、新しいアクティブ RP が、NSR を使用して設定されたピアに対して、ルートリフレッシュ リクエストを送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp sso route-refresh-enable**
5. **end**
6. **show ip bgp vpnv4 all neighbor** [*ip-address*]
7. **show ip bgp vpnv4 all sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp** *as-number* 例： `Router(config)# router bgp 6500`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。 • 4 バイト AS の設定については、『*IP Routing: BGP Command Reference*』の **bgp asnotation dot** コマンドに関する説明を参照してください。
ステップ 4	**bgp sso route-refresh-enable** 例： `Router(config-router)# bgp sso route-refresh-enable`	BGP NSR 自動検知機能を無効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp vpnv4 all neighbor** [*ip-address*] 例： `Router# show ip bgp vpnv4 all neighbor 10.0.0.2`	BGP ピアの情報を表示します。
ステップ 7	**show ip bgp vpnv4 all sso summary** 例： `Router# show ip bgp vpnv4 all sso summary`	（任意）ステートフル スイッチオーバー（SSO）による BGP ノンストップ ルーティング（NSR）をサポートする BGP ピアの数を表示します。

BGP NSR 自動検知の設定例

例：BGP NSR 自動検知機能の無効化

```
router bgp 65600
 bgp sso route-refresh-enable
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 NSR 自動検知の機能情報

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 *78 : BGP NSR* 自動検知の機能情報

機能名	リリース	機能情報
BGP NSR 自動検知	15.2(2)S Cisco IOS XE Release 3.6S	BGP NSR 自動検知機能は、RP のフェールオーバー時に不要なチャーンを削減するためにデフォルトで実装されています。また、この機能は、ルートリフレッシュのサポートがないピアに対しても NSR サポートを提供します。 **bgp sso route-refresh-enable** コマンドが導入されました。

第 60 章

iBGP ピアの BGP NSR サポート

BGP NSR は、アクティブ RP からスタンバイ RP へのスイッチオーバー時に BGP ノンストップ ルーティング（NSR）およびノンストップ フォワーディング（NSF）を提供します。iBGP ピアの BGP NSR サポート機能は、IPv4 ユニキャストまたは IPv4+ラベル アドレス ファミリで設定された iBGP ピアに対して NSR サポートを提供します。

- 機能情報の確認 （1035 ページ）
- iBGP ピアの BGP NSR サポートの制約事項 （1035 ページ）
- iBGP ピアの BGP NSR サポートに関する情報 （1036 ページ）
- iBGP ピアの BGP NSR サポートの設定方法 （1036 ページ）
- iBGP ピアの BGP NSR サポートの設定例 （1040 ページ）
- その他の参考資料 （1041 ページ）
- iBGP ピアの BGP NSR サポートの機能情報 （1041 ページ）

機能情報の確認

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

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

iBGP ピアの BGP NSR サポートの制約事項

この機能は、IPv4 ユニキャストまたは IPv4+ラベル アドレス ファミリで設定された iBGP ピアに適用されます。

iBGP ピアの BGP NSR サポートに関する情報

iBGP ピアの BGP NSR サポートの利点

ノンストップ ルーティングは、アクティブ RP からスタンバイ RP へのスイッチオーバー時にパケットがドロップされる可能性を低減するため、iBGP ピアで役立ちます。スイッチオーバーは何らかの理由によりアクティブ RP で障害が発生した場合に行われ、スタンバイ RP がアクティブ RP の機能を制御することになります。

iBGP ピアの BGP NSR サポートの設定方法

IPv4 アドレス ファミリでの iBGP ピアの NSR 対応化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address* **activate**
7. **neighbor** *ip-address* **ha-mode sso**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 4000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv4** [**unicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 ユニキャスト アドレス ファミリを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 5	**neighbor** *ip-address* **remote-as** *as-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 4000`	ネイバーの自律システムを指定します。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	指定したピアをアクティブにします。
ステップ 7	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP NSR をサポートするように BGP ネイバーを設定します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

VPNv4 アドレス ファミリでの iBGP ピアの NSR 対応化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *as-number*
5. **neighbor** *ip-address* **ha-mode sso**
6. **address-family vpnv4** [**unicast**]

7. **neighbor** *ip-address* **activate**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 4000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *as-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 4000`	ネイバーの自律システムを指定します。
ステップ 5	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP NSR をサポートするように BGP ネイバーを設定します。
ステップ 6	**address-family vpnv4** [**unicast**] 例： `Device(config-router)# address-family VPNv4 unicast`	VPNv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	指定したピアをアクティブにします。
ステップ 8	**end** 例：	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-router-af)# end`	

ルータ レベルでの iBGP ピアの NSR 対応化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *as-number*
5. **neighbor** *ip-address* **activate**
6. **neighbor** *ip-address* **ha-mode sso**
7. **end**
8. **show ip bgp sso summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 4000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *as-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 4000`	ネイバーの自律システムを指定します。
ステップ 5	**neighbor** *ip-address* **activate** 例： `Device(config-router)# neighbor 192.168.1.1 activate`	指定したネイバーをアクティブにします。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router)# neighbor 192.168.1.1 ha-mode sso`	指定したピアについて、そのピアがアクティブになっているすべての NSR 対応アドレス ファミリで NSR 対応となるように設定します。
ステップ 7	**end** 例： `Device(config-router)# end`	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	**show ip bgp sso summary** 例： `Device# show ip bgp sso summary`	（任意）ステートフル スイッチオーバー（SSO）に関する情報およびピアで NSR が有効になっているか無効になっているかを表示します。

iBGP ピアの BGP NSR サポートの設定例

例：iBGP ピアを NSR 対応にするための設定

アドレス ファミリ レベルで iBGP ピアを NSR 対応にするための設定

```
router bgp 4000
 address-family ipv4 unicast
 neighbor 192.168.1.1 remote-as 4000
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 ha-mode sso
```

ルータ レベルで iBGP ピアを NSR 対応にするための設定

```
router bgp 4000
 neighbor 192.168.1.1 remote-as 4000
 neighbor 192.168.1.1 activate
 neighbor 192.168.1.1 ha-mode sso
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BFD コマンド	『Cisco IOS IP Routing: Protocol Independent Command Reference』
別のルーティング プロトコルに対する BFD サポートの設定	『IP Routing: BFD Configuration Guide』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

iBGP ピアの BGP NSR 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 *79 : iBGP* ピアの *BGP NSR* サポートの機能情報

機能名	リリース	機能情報
iBGP ピアの BGP NSR サポート		BGP NSR は、アクティブ RP からスタンバイ RP へのスイッチオーバー時に BGP ノンストップ ルーティングおよびノンストップ フォワーディングを提供します。 次のコマンドが変更されました。**neighbor ha-mode sso**、**show ip bgp vpnv4 all sso summary**

第 61 章

BGP グレースフル シャットダウン

BGP グレースフル シャットダウン機能は、メンテナンスのためにシャットダウンされるリンク上でのトラフィックの損失を低減または排除します。ルータは、常に、コンバージェンスプロセス中に有効なルートを確保できます。この機能は、主に、プロバイダー エッジ（PE）、PE-PE、PE-ルート リフレクタ（RR）、PE-カスタマー エッジ（CE）、CE 間のリンクでのメンテナンスに使用します。

- 機能情報の確認 （1043 ページ）
- BGP グレースフル シャットダウンに関する情報 （1044 ページ）
- BGP グレースフル シャットダウンの設定方法 （1045 ページ）
- BGP グレースフル シャットダウンの設定例 （1051 ページ）
- その他の参考資料 （1053 ページ）
- BGP グレースフル シャットダウンの機能情報 （1054 ページ）

機能情報の確認

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

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

BGP グレースフル シャットダウンに関する情報

BGP グレースフル シャットダウンの目的と利点

計画的なメンテナンス作業によって BGP でルーティングの変更が生じる場合があります。自律システム境界ルータ（ASBR）間の eBGP および iBGP ピアリング セッションのシャットダウン後、BGP デバイスは BGP コンバージェンス中に一時的に到達不能になります。BGP セッションのグレースフルシャットダウンを行う目的は、セッションの計画的なシャットダウンとそれに続く再確立時におけるトラフィックの損失を最小限に抑えることです。

BGP グレースフル シャットダウン機能は、メンテナンスのためにシャットダウンされるピアリンク上で最初に転送された着信または発信トラフィック フローの損失を低減または排除します。この機能は、主に、PE-CE、PE-RR、PE-PE リンク用です。シャットダウンされるセッション上で受信したパスのローカル プリファレンスを低くすると、影響を受けるパスは BGP 決定プロセスでの優先度が下がりますが、コンバージェンス中にそれらのパスを引き続き使用できるようになるうえに、影響を受けるデバイスに代替パスが伝播されます。したがって、デバイスは、常に、コンバージェンス プロセス中に有効なルートを確保できます。

また、この機能により、ベンダーは、メンテナンス時にルータの再設定を必要としないグレースフル シャットダウン メカニズムを提供できます。BGP グレースフル シャットダウン機能の利点は、損失パケットの数が減り、デバイスの再構成にかかる時間が短くなることです。

GSHUT コミュニティ

GSHUT コミュニティは、BGP グレースフル シャットダウン機能とともに使用されるウェルノウン（well-known）コミュニティです。GSHUT コミュニティ属性は **neighbor shutdown graceful** コマンドで指定したネイバーに適用されるため、設定した秒数でリンクのグレースフル シャットダウンが行われます。GSHUT コミュニティは、常に、GSHUT イニシエータによって送信されます。

GSHUT コミュニティはコミュニティ リストで指定します。このコミュニティ リストが、ルート マップで参照され、ポリシー ルーティング決定を行う際に使用されます。

また、GSHUT コミュニティを **show ip bgp community** コマンドで使用して、GSHUT ルートへの出力を制限することもできます。

BGP GSHUT 拡張機能

BGP グレースフル シャットダウン（GSHUT）拡張機能は、すべての BGP セッションにおける、すべてのネイバーまたは Virtual Routing and Forwarding（VRF）ネイバーのみのグレースフル シャットダウンを可能にします。デバイスで BGP GSHUT 拡張機能を有効にするには、**bgp graceful-shutdown all** コマンドで **community** キーワードまたは **local-preference** キーワードを設定する必要があります。すべての BGP セッションにおいて、すべてのネイバーで、または

すべての VRF ネイバーのみでグレースフル シャットダウンをアクティブにするには、**activate** キーワードを使用します。

BGP グレースフル シャットダウンの設定方法

BGP リンクのグレースフル シャットダウン

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ipv4-address* | *ipv6-address*} **remote-as** *number*
5. **neighbor** {*ipv4-address* | *ipv6-address* | *peer-group-name*} **shutdown graceful** *seconds* {**community** *value* [**local-preference** *value*] | **local-preference** *value*}
6. **end**
7. **show ip bgp community gshut**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 5000`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ipv4-address* | *ipv6-address*} **remote-as** *number* 例： `Device(config-router)# neighbor 2001:db8:3::1 remote-as 5500`	ネイバーが属する自律システム（AS）を設定します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ipv4-address* | *ipv6-address* | *peer-group-name*} **shutdown graceful** *seconds* {**community** *value* [**local-preference** *value*] | **local-preference** *value*} 例： `Device(config-router)# neighbor 2001:db8:3::1 shutdown graceful 600 community 1200 local-preference 300`	次のことを行うようにデバイスを設定します。指定したピアへのリンクを指定した秒数でグレースフルシャットダウンします。GSHUT（グレースフルシャットダウン）コミュニティを使用してルートをアドバタイズします。別のコミュニティを使用してルートをアドバタイズするか、ルートのローカルプリファレンス値を指定します（またはその両方を行います）。 • 必ず、iBGP ピアが収束して代替パスをベストパスとして選択するための十分な時間を指定するようにします。 • **neighbor shutdown** コマンドで **graceful** キーワードを使用する場合は、2つの属性（コミュニティまたはローカルプリファレンス）のうち少なくとも 1 つを設定する必要があります。両方の属性を設定することもできます。 • **neighbor shutdown** コマンドで **graceful** キーワードを使用すると、デフォルトでは、GSHUT コミュニティでルートがアドバタイズされます。また、ポリシー ルーティングのために別のコミュニティを 1 つ設定することもできます。 • この特定の例では、ネイバーへのルートは、600 秒でシャットダウンするように設定されており、GSHUT コミュニティおよびコミュニティ 1200 でアドバタイズされ、ローカル プリファレンスが 300 に設定されます。 • アドバタイズされた情報を受信したデバイスは、ルートのコミュニティ値を確認し、必要に応じコミュニティ値を使用してルーティングポリシーを適用します。コミュニティに基づくルートのフィルタ処理は、 **ip community-list** コマンドおよびルート マップを使用して行います。 • グレースフル シャットダウン時、**neighbor shutdown** コマンドの不揮発性生成（NVGEN）は行われません。タイマーが期限切れになると、SHUTDOWN の不揮発性生成（NVGEN）が行われます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-router)# end`	EXEC モードに戻ります。
ステップ 7	**show ip bgp community gshut** 例： `Device# show ip bgp community gshut`	（任意）ウェルノウン GSHUT コミュニティを使用してアドバタイズされるルートに関する情報を表示します。

GSHUT コミュニティに基づく BGP ルートのフィルタ処理

BGP グレースフル シャットダウン機能を有効にしたデバイスへの BGP ピアでこの作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ipv4-address* | *ipv6-address*} **remote-as** *number*
5. **neighbor** {*ipv4-address* | *ipv6-address*} **activate**
6. **neighbor** {*ipv4-address* | *ipv6-address*} **send-community**
7. **exit**
8. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
9. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
10. **exit**
11. **ip community-list** {*standard* | **standard** *list-name*} {**deny** | **permit**} **gshut**
12. **router bgp** *autonomous-system-number*
13. **neighbor** *address* **route-map** *map-name* **in**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 2000`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ipv4-address* | *ipv6-address*} **remote-as** *number* 例： `Device(config-router)# neighbor 2001:db8:4::1 remote-as 1000`	ネイバーが属する自律システム（AS）を設定します。
ステップ 5	**neighbor** {*ipv4-address* | *ipv6-address*} **activate** 例： `Device(config-router)# neighbor 2001:db8:4::1 activate`	ネイバーをアクティブにします。
ステップ 6	**neighbor** {*ipv4-address* | *ipv6-address*} **send-community** 例： `Device(config-router)# neighbor 2001:db8:4::1 send-community`	ネイバーとの BGP コミュニティ交換を可能にします。
ステップ 7	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 8	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map RM_GSHUT deny 10`	ポリシー ルーティング用にルートを許可または拒否するようにルート マップを設定します。
ステップ 9	**match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]} 例： `Device(config-route-map)# match community GSHUT`	ip community-list GSHUT に一致するルートがポリシー ルーティングされるように設定します。
ステップ 10	**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。

	コマンドまたはアクション	目的
ステップ 11	**ip community-list** {*standard* | **standard** *list-name*} {**deny** | **permit**} **gshut** 例： `Device(config)# ip community-list standard GSHUT permit gshut`	コミュニティ リストを設定し、そのコミュニティ リストに対してGSHUTコミュニティを持つルートを許可または拒否します。 • 同じステートメントで他のコミュニティを指定した場合は、論理AND演算が行われ、そのステートメント内のすべてのコミュニティがルートのコミュニティと一致していない限り、ステートメントは処理されません。
ステップ 12	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 2000`	BGP ルーティング プロセスを設定します。
ステップ 13	**neighbor** *address* **route-map** *map-name* **in** 例： `Device(config)# neighbor 2001:db8:4::1 route-map RM_GSHUT in`	指定したネイバーからの着信ルートにルート マップを適用します。 • この例では、RM_GSHUTという名前のルートマップは、GSHUTコミュニティを持つ、指定されたネイバーからのルートを拒否します。

BGP GSHUT 拡張機能の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-shutdown all** {**neighbors** | **vrfs**} *shutdown-time* {**community** *community-value* [**local-preference** *local-pref-value*] | **local-preference** *local-pref-value* [**community** *community-value*]}
5. **bgp graceful-shutdown all** {**neighbors** | **vrfs**} **activate**
6. **end**
7. **show ip bgp**
8. **show running-config**

手順の詳細

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

	コマンドまたはアクション	目的
	`Device> enable`	
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 65000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**bgp graceful-shutdown all** {**neighbors** | **vrfs**} *shutdown-time* {**community** *community-value* [**local-preference** *local-pref-value*] | **local-preference** *local-pref-value* [**community** *community-value*]} 例： `Device(config-router)# bgp graceful-shutdown all neighbors 180 local-preference 20 community 10`	デバイスで BGP GSHUT 拡張機能を有効にします。
ステップ 5	**bgp graceful-shutdown all** {**neighbors** | **vrfs**} **activate** 例： `Device(config-router)# bgp graceful-shutdown all neighbors activate`	BGP セッションのすべてのネイバーまたは VRF ネイバーのみでグレースフル シャットダウンをアクティブにします。
ステップ 6	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** 例： `Device# show ip bgp neighbors 10.2.2.2 | include shutdown`	BGP ルーティング テーブル内のエントリを表示します。
ステップ 8	**show running-config** 例： `Device# show running-config | session router bgp`	デバイスの実行コンフィギュレーションを表示します。

BGP グレースフル シャットダウンの設定例

例：BGP リンクのグレースフル シャットダウン

ローカル プリファレンスも設定するグレースフル シャットダウン

この例では、指定したネイバーへのリンクを 600 秒でグレースフル シャットダウンし、GSHUT コミュニティをルートに追加して、ルートのローカル プリファレンスを 500 に設定します。

```
router bgp 1000
 neighbor 2001:db8:5::1 remote-as 2000
 neighbor 2001:db8:5::1 shutdown graceful 600 local-preference 500
 neighbor 2001:db8:5::1 send-community
 exit
```

追加のコミュニティも設定するグレースフル シャットダウン

この例では、指定したネイバーへのリンクを 600 秒でグレースフル シャットダウンし、GSHUT コミュニティおよび番号付きコミュニティをルートに追加します。

```
router bgp 1000
 neighbor 2001:db8:5::1 remote-as 2000
 neighbor 2001:db8:5::1 shutdown graceful 600 community 1400
 neighbor 2001:db8:5::1 send-community
 exit
```

追加のコミュニティとローカルプリファレンスを設定するグレースフルシャットダウン

この例では、指定したネイバーへのリンクを 600 秒でグレースフル シャットダウンし、GSHUTコミュニティおよび番号付きコミュニティをルートに追加して、ルートのローカル プリファレンスを 500 に設定します。

```
router bgp 1000
 neighbor 2001:db8:5::1 remote-as 2000
 neighbor 2001:db8:5::1 shutdown graceful 600 community 1400 local-preference 500
 neighbor 2001:db8:5::1 send-community
 exit
```

例：GSHUT コミュニティに基づく BGP ルートのフィルタ処理

BGP ルートのグレースフル シャットダウンに加えて、GSHUT コミュニティのもう 1 つの使用方法は、このコミュニティでルートをフィルタ処理して BGP ルーティング テーブルに挿入しないようにコミュニティ リストを設定することです。

この例では、コミュニティ リストを使用し、GSHUT コミュニティに基づいて着信 BGP ルートをフィルタ処理する方法を示します。この例では、RM_GSHUT という名前のルート マップは、GSHUT という名前の標準コミュニティ リストに基づいてルートを拒否します。コミュニティ リストには、GSHUT コミュニティを持つルートが含まれています。ルート マップは、2001:db8:4::1 のネイバーからの着信ルートに適用されます。

```
router bgp 2000
 neighbor 2001:db8:4::1 remote-as 1000
 neighbor 2001:db8:4::1 activate
 neighbor 2001:db8:4::1 send-community
 exit
route-map RM_GSHUT deny 10
 match community GSHUT
 exit
ip community-list standard GSHUT permit gshut
router bgp 2000
 neighbor 2001:db8:4::1 route-map RM_GSHUT in
```

例：BGP GSHUT 拡張機能

次の例は、すべてのネイバーで BGP GSHUT 拡張機能を有効化およびアクティブ化する方法を示しています。この例では、指定した期間の 180 秒以内にグレースフル シャットダウンが行われるようにネイバーを設定しています。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-shutdown all neighbors 180 local-preference 20
community 10
Device(config-router)# bgp graceful-shutdown all neighbors activate
Device(config-router)# end
```

次に、各ネイバーのグレースフル シャットダウン時間を表示する **show ip bgp** コマンドの出力例を示します。この例では、IP アドレス 10.2.2.2 と 172.16.2.1 を使用して設定された 2 つの IPv4 ネイバーがあり、v1 というタグが付いた 1 つの VRF ネイバーが IP アドレス 192.168.1.1 を使用して設定されています。

```
Device# show ip bgp neighbors 10.2.2.2 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:47 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

```
Device# show ip bgp neighbors 172.16.2.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:38 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10

Device# show ip bgp vpnv4 vrf v1 neighbors 192.168.1.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:01:45 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

次に、ルータ コンフィギュレーション モードで BGP セッションに関連付けられた情報を表示する **show running-config** コマンドの出力例を示します。

```
Device# show running-config | session router bgp

router bgp 65000
bgp log-neighbor-changes
bgp graceful-shutdown all neighbors 180 local-preference 20 community 10
network 10.1.1.0 mask 255.255.255.0
neighbor 10.2.2.2 remote-as 40
neighbor 10.2.2.2 shutdown
neighbor 172.16.2.1 remote-as 10
neighbor 172.16.2.1 shutdown
!
address-family vpnv4
neighbor 172.16.2.1 activate
neighbor 172.16.2.1 send-community both
exit-address-family
!
address-family ipv4 vrf v1
neighbor 192.168.1.1 remote-as 30
neighbor 192.168.1.1 shutdown
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 send-community both
exit-address-family
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 6198	*BGP* セッションのグレースフル シャットダウンの要件

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 グレースフル シャットダウンの機能情報

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 *80 : BGP* グレースフル シャットダウンの機能情報

機能名	リリース	機能情報
BGP グレースフル シャットダウン		BGP グレースフル シャットダウン機能は、メンテナンスのためにシャットダウンされるリンク上でのトラフィックの損失を低減または排除します。ルータは、常に、コンバージェンス プロセス中に有効なルートを確保できます。 次のコマンドが変更されました。**ip community-list**、**neighbor shutdown**、**show ip bgp community**、**show ip bgp vpnv4**
BGP GSHUT 拡張機能		BGP グレースフル シャットダウン（GSHUT）拡張機能は、すべての BGP セッションにおける、すべてのネイバーまたは Virtual Routing and Forwarding（VRF）ネイバーのみのグレースフル シャットダウンを可能にします。 **bgp graceful-shutdown all** コマンドが導入されました。

第 62 章

BGP — mVPN BGP sAFI 129 - IPv4

BGP—mVPN BGP sAFI 129 IPv4 機能は、サービス プロバイダーのコア IPv4 ネットワークでマルチキャスト ルーティングをサポートする機能を提供します。この機能は、BGP ベースの MVPN をサポートするために必要です。BGP MVPN により、サービス プロバイダーは、サービス プロバイダー ネットワークで MVPN マルチキャスト データ トラフィックを転送するためのさまざまなカプセル化方式（Generic Routing Encapsulation（GRE）、マルチキャスト ラベル配布プロトコル（MLDP）、入力複製）を使用できるようになります。

- 機能情報の確認 （1057 ページ）
- BGP--mVPN BGP sAFI 129 - IPv4 に関する情報 （1058 ページ）
- BGP -- mVPN BGP sAFI 129 - IPv4 の設定方法 （1058 ページ）
- BGP--mVPN BGPsAFI 129 - IPv4 の設定例 （1062 ページ）
- その他の参考資料 （1065 ページ）
- BGP - mVPN BGP sAFI 129 - IPv4 の機能情報 （1065 ページ）

機能情報の確認

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

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

BGP--mVPN BGP sAFI 129 - IPv4 に関する情報

BGP — mVPN BGP sAFI 129 - IPv4 の概要

Cisco BGP の Address Family Identifier（AFI; アドレス ファミリ識別子）モデルは、マルチプロトコルBGPと一緒に導入され、モジュラ式かつスケーラブルで、複数のAFIおよびSubsequent Address Family Identifier（SAFI; 後続アドレス ファミリ識別子）コンフィギュレーションをサポートするように設計されています。SAFI は、ルートおよび宛先への接続方法を表すために使用されるネットワーク層到達可能性情報（NLRI）のタイプに関する追加情報を提供します。

SAFI 129 は、サービス プロバイダーのコア IPv4 ネットワークでマルチキャスト ルーティングをサポートする機能を提供します。この機能は、BGP ベースの MVPN をサポートするために必要です。SAFI 129 の追加により、マルチキャストで、ユニキャスト トポロジに依存しないこともあるアップストリームマルチキャストホップを選択できるようになります。カスタマーエッジ（CE）ルータから学習したマルチキャスト ルートまたはリモート プロバイダー エッジ（PE）ルータから学習したマルチキャスト VPN ルートは、マルチキャスト ルーティング情報ベース（RIB）にインストールされますが、以前はユニキャスト RIB 内のユニキャスト ルートがマルチキャスト RIB に複製されていました。

address-family ipv4 コマンドは、VPN ルーティングおよび転送（VRF）インスタンスの IP バージョン 4（IPv4）マルチキャスト アドレス プレフィックスをサポートするように更新され、**address-family vpnv4** コマンドは、VPN バージョン 4（VPNv4）マルチキャスト アドレス プレフィックスをサポートするように更新されました。

BGP -- mVPN BGP sAFI 129 - IPv4 の設定方法

BGP — mVPN BGP sAFI 129 - IPv4 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf1*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **address-family ipv4**
8. **mdt default** *group-address*
9. **exit**
10. **router bgp** *autonomous-system-number*
11. **address-family vpnv4 multicast**
12. **neighbor** *peer-group-name* **send-community extended**

13. **neighbor** *peer-group-name* **route-reflector-client**
14. **exit-address-family**
15. **address-family ipv4 vrf** *vrf-name*
16. **no synchronization**
17. **exit-address-family**
18. **address-family ipv4 multicast vrf** *vrf-name*
19. **no synchronization**
20. **exit-address-family**
21. **end**
22. **show running-config | b router bgp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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** *vrf1* 例： `Device(config)# vrf definition vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 1:1`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 1:1`	VRF インスタンス用にルート ターゲット エクスポート拡張コミュニティを作成します。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 1:1`	VRF インスタンス用にルート ターゲット インポート拡張コミュニティを作成します。

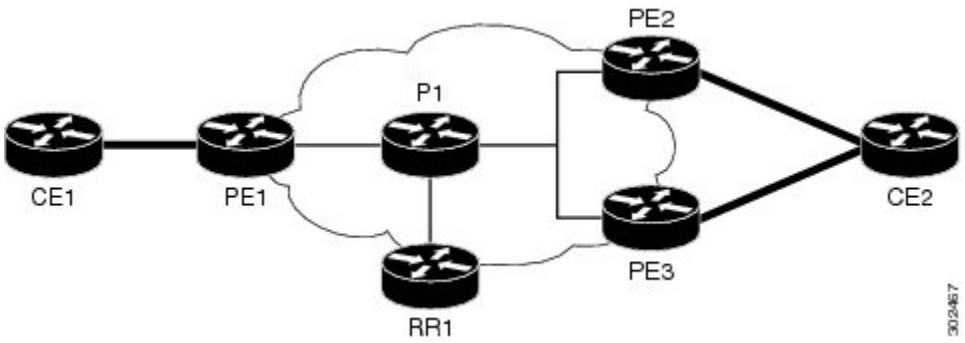
	コマンドまたはアクション	目的
ステップ 7	**address-family ipv4** 例： `Device(config-router)# address-family ipv4`	IPv4 アドレス プレフィックスを使用するルーティング セッションを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**mdt default** *group-address* 例： `Device(config-vrf)# mdt default 239.0.0.1`	VRF インスタンスに対してデフォルトのマルチキャスト配信ツリー（MDT）を設定します。
ステップ 9	**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 10	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 50000`	BGP ルーティング プロセスを設定して、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 11	**address-family vpnv4 multicast** 例： `Device(config-router)# address-family vpnv4 multicast`	VPN バージョン 4 マルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 12	**neighbor** *peer-group-name* **send-community extended** 例： `Device(config-router-af)# neighbor client1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 13	**neighbor** *peer-group-name* **route-reflector-client** 例： `Device(config-router-af)# neighbor client1 route-reflector-client`	（任意）ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 14	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 15	**address-family ipv4 vrf** *vrf-name* 例：	ルータをアドレス ファミリ コンフィギュレーション モードにし、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。

	コマンドまたはアクション	目的
	`Device(config-router)# address-family ipv4 vrf vrf1`	
ステップ 16	**no synchronization** 例： `Device(config-router-af)# no synchronization`	シスコ ソフトウェアが内部ゲートウェイ プロトコル（IGP）システムを待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 17	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 18	**address-family ipv4 multicast vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 multicast vrf vrf1`	VRF インスタンスに対して IPv4 マルチキャスト アドレスプレフィックスを使用するルーティングセッションを設定し、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 19	**no synchronization** 例： `Device(config-router-af)# no synchronization`	シスコ ソフトウェアが IGP システムを待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 20	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 21	**end** 例： `Device(config)# 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 22	**show running-config | b router bgp** 例： `Device# show running-config | b router bgp`	（任意）指定したデバイスの実行コンフィギュレーションを表示します。

BGP--mVPN BGPsAFI 129 - IPv4 の設定例

例：BGP - mVPN BGP sAFI 129 - IPv4 の設定

この例では、下の図に示すトポロジを使用します。



次の例では、ルート リフレクタ（RR）で BGP SAFI 129 を設定します。

```
!
ip multicast-routing
!
!<<< Define BGP update-source loopback0
!<<< on RR as 192.0.2.10
interface loopback0
 ip pim sparse-dense-mode
 ip address 192.0.2.10 255.255.255.255
!
.
.
.
router bgp 65000
 no synchronization
 neighbor 192.0.2.1 remote-as 65000
 neighbor 192.0.2.1 update-source loopback0
 neighbor 192.0.2.2 remote-as 65000
 neighbor 192.0.2.2 update-source loopback0
 neighbor 192.0.2.3 remote-as 65000
 neighbor 192.0.2.3 update-source loopback0
 !
 .
 .
 address-family vpnv4 unicast
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 send-community extended
  neighbor 192.0.2.1 route-reflector-client
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community extended
  neighbor 192.0.2.2 route-reflector-client
  neighbor 192.0.2.3 activate
  neighbor 192.0.2.3 send-community extended
  neighbor 192.0.2.3 route-reflector-client
  exit-address-family
 !
 address-family vpnv4 multicast
```

```
  !<<< want route from CE1 with nexthop
  !<<< through PE3 in multicast routing table
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 send-community extended
  neighbor 192.0.2.1 route-reflector-client
  neighbor 192.0.2.3 activate
  neighbor 192.0.2.3 send-community extended
  neighbor 192.0.2.3 route-reflector-client
 exit-address-family
!
.
.
```

次の例では、PE1 ルータで BGP SAFI 129 を設定します（PE2 および PE3 は同様の設定になります）。

```
Hostname PE1
!
vrf definition vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
  mdt default 239.0.0.1
 exit-address-family
!
ip multicast-routing
ip multicast-routing vrf vrf1
!
.
.
.
!<<< Define BGP update-source on Loopback0
!<<< on PE1
inteface loopback0
 ip pim sparse-dense-mode
 ip address 192.0.2.1 255.255.255.255
!
.
.
.
!<<< Define vrf vrf1 interface on PE1 to CE1
interface ethernet0/0
 vrf forwarding vrf1
 ip pim sparse-dense-mode
 ip address 192.0.2.1 255.255.255.0
!
.
.
,
router bgp 65000
 !<<<< PE peer neighbor with RR
 neighbor 192.0.2.10 remote-as 65000
 neighbor 192.0.2.10 update-source loopback0
 no synchronization
 .
 .
 .
 address-family vpnv4
  neighbor 192.0.2.10 activate
  neighbor 192.0.2.10 send-community extended
```

```
 exit-address-family
 !
 !<<< Define vpnv4 safi129 with neighbor
 !<<< to RR
 address-family vpnv4 multicast
  neighbor 192.0.2.10 activate
  neighbor 192.0.2.10 send-community extended
 exit-address-family
 !
 .
 .
 .
 !<<< Define unicast address-family vrf vrf1.
 !<<< PE-CE is eBGP in this case.
 !<<< If PE-CE is not eBGP, please use
 !<<< redistribute cli, instead of
 !<<< neighbor cli below.
 address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
  neighbor 192.0.2.5 remote-as 65011
 exit-address-family
 !
 !<<< Define multicast address-family vrf vrf1
 !<<< (safi2. PE-CE is eBGP in this case.
 !<<< If PE-CE is not eBGP, please use
 !<<< redistribute cli, instead of
 !<<< neighbor cli below.
 address-family ipv4 multicast vrf vrf1
  no synchronization
  redistribute connected
  neighbor 192.0.2.5 remote-as 65011
 exit-address-family
 !
```

次の例では、CE1 ルータで BGP SAFI 129 を設定します（この場合、PE-CE ルーティングは eBGP です。CE2 は同様の設定になります）。

```
interface ethernet0/0
 ip address 192.0.2.5 255.255.255.0
 ip pim sparse-dense-mode
!
.
.
.
router bgp 65011
 bgp router-id 192.0.2.5
 bgp log-neighbor-changes
 !
 address-family ipv4
  redistribute connected
  neighbor 192.0.2.1 remote-as 65000
 exit-address-family
 !
 address-family ipv4 multicast
  redistribute connected
  neighbor 192.0.2.1 remote-as 65000
 exit-address-family
!
```

その他の参考資料

関連資料

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

標準および RFC

標準/RFC	タイトル
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 - mVPN BGP sAFI 129 - IPv4 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 *81 : BGP - mVPN BGP sAFI 129 - IPv4* の機能情報

機能名	リリース	機能情報
BGP - mVPN BGP sAFI 129 - IPv4	15.2(2)S 15.2(4)S Cisco IOS XE Release 3.6S	BGP - mVPN BGP sAFI 129 IPv4 機能は、サービス プロバイダーのコア IPv4 ネットワークでマルチキャスト ルーティングをサポートする機能を提供します。この機能は、BGP ベースの MVPN をサポートするために必要です。BGP MVPN により、サービス プロバイダーは、サービス プロバイダー ネットワークで MVPN マルチキャスト データ トラフィックを転送するためのさまざまなカプセル化方式（Generic Routing Encapsulation（GRE）、マルチキャスト ラベル配布プロトコル（MLDP）、入力複製）を使用できるようになります。Cisco IOS Release 15.2(4)S では、Cisco 7200 シリーズ ルータのサポートが追加されました。 次のコマンドが変更されました。**address-family ipv4**、**address-family vpnv4**

第 63 章

BGP-MVPN SAFI 129 IPv6

Subsequent Address Family Identifier（SAFI; 後続アドレス ファミリ識別子）129 は、VPN マルチキャスト SAFI とも呼ばれ、サービス プロバイダーのコア IPv6 ネットワークでマルチキャスト ルーティングをサポートする機能を提供します。

ボーダー ゲートウェイ プロトコル（BGP）マルチキャスト バーチャル プライベート ネットワーク（MVPN）により、サービス プロバイダーは、サービス プロバイダー ネットワークで MVPN マルチキャスト データ トラフィックを転送するためのさまざまなカプセル化方式（Generic Routing Encapsulation（GRE）、マルチキャスト ラベル配布プロトコル（MLDP）、入力複製）を使用できるようになります。

BGP-MVPN SAFI 129 IPv6 機能は、BGP ベースの MVPN をサポートするために必要です。

- 機能情報の確認 （1067 ページ）
- BGP-MVPN SAFI 129 IPv6 の前提条件 （1068 ページ）
- BGP-MVPN SAFI 129 IPv6 に関する情報 （1068 ページ）
- BGP-MVPN SAFI 129 IPv6 の設定方法 （1069 ページ）
- BGP-MVPN SAFI 129 IPv6 の設定例 （1071 ページ）
- その他の参考資料 （1074 ページ）
- BGP-MVPN SAFI 129 IPv6 の機能情報 （1075 ページ）

機能情報の確認

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

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

BGP-MVPN SAFI 129 IPv6 の前提条件

- SAFI 129 IPv6 関連のアドレス ファミリを設定する前に、**ipv6 unicast-routing** コマンドをデバイスで設定する必要があります。
- BGP でマルチキャスト IPv6 VRF アドレス ファミリを作成するには、まず、VRF 自体で IPv6 をアクティブにする必要があります。

（注） VRF には個別のマルチキャスト設定はありません。VRF で **address-family ipv6** コマンドを設定すると、ユニキャスト トポロジとマルチキャスト トポロジの両方が有効になります。

- プレフィックスをルーティング情報ベース（RIB）にインストールする場合は、VRF インターフェイスで **pim** コマンドを設定する必要があります。

BGP-MVPN SAFI 129 IPv6 に関する情報

BGP-MVPN SAFI 129 IPv6 の概要

MVPN では、既存の VPN インフラストラクチャを利用して、マルチキャスト トラフィックがプロバイダー空間を通過できるようにします。VPN ルートから取得される情報は、コア内でトンネルをセットアップするために必要なコンポーネントの 1 つです。現在、マルチキャスト トラフィックはユニキャスト VPNv6 テーブルからこの情報を取得するため、必然的にマルチキャスト トラフィックはユニキャスト トポロジに依存することになります。

マルチキャスト トラフィックとユニキャスト トラフィックが個別のトポロジに適しているシナリオでは、マルチキャスト VPN のみに使用される特別なルートのセットをカスタマー エッジ（CE）ルータからアドバタイズすることもできます。CE ルータから学習したマルチキャスト ルートは、SAFI 129 を介してリモート プロバイダー エッジ（PE）ルータに伝播できます。ユニキャスト RIB から複製されたルートを使用するのではなく、CE ルータから学習したマルチキャスト ルートまたはリモート PE ルータから学習したマルチキャスト VPN ルートを、マルチキャスト RIB に直接インストールできるようになりました。ユニキャストとマルチキャストで別々のルートおよびエントリを維持することで、コア内のサービスごとに異なるトポロジを作成できます。

BGP-MVPN SAFI 129 IPv6 の設定方法

BGP-MVPN SAFI 129 IPv6 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf1*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **address-family ipv6**
8. **mdt default** *group-address*
9. **exit**
10. **exit**
11. **router bgp** *autonomous-system-number*
12. **address-family vpnv6 multicast**
13. **neighbor** *peer-group-name* **send-community extended**
14. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* **%**} **activate**
15. **address-family ipv6 multicast vrf** *vrf-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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** *vrf1* 例： `Device(config)# vrf definition vrf1`	VRFインスタンスを定義し、VRFコンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例：	VRFインスタンスのルート識別子（RD）を指定します。

	コマンドまたはアクション	目的
	`Device(config-vrf)# rd 1:1`	
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 1:1`	VRF インスタンス用にルート ターゲット エクスポート拡張コミュニティを作成します。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 1:1`	VRF インスタンス用にルート ターゲット インポート拡張コミュニティを作成します。
ステップ 7	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	IPv6 アドレス プレフィックスを使用するルーティング セッションを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**mdt default** *group-address* 例： `Device(config-vrf-af)# mdt default 239.0.0.1`	VRF インスタンスに対してデフォルトのマルチキャスト配信ツリー（MDT）を設定します。
ステップ 9	**exit** 例： `Device(config-vrf-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 10	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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 11	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 50000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 12	**address-family vpnv6 multicast** 例： `Device(config-router)# address-family vpnv6 multicast`	VPN バージョン 6 マルチキャスト アドレス プレフィックスを使用するルーティング セッションを設定し、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 13	**neighbor** *peer-group-name* **send-community extended** 例：	コミュニティ属性が BGP ネイバーに送信されるように指定します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# neighbor client1 send-community extended`	
ステップ 14	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* **%**} **activate** 例： `Router(config-router-af)# neighbor 2001:DB8:0:CC00::1 % activate`	ネイバーが、指定したファミリ タイプのプレフィックスをネイバーおよびローカル ルータと交換できるようにします。
ステップ 15	**address-family ipv6 multicast vrf** *vrf-name* 例： `Device(config-router-af)# address-family ipv6 multicast vrf vrf1`	VRF インスタンスに対して IPv6 マルチキャスト アドレスプレフィックスを使用するルーティングセッションを設定します。
ステップ 16	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP-MVPN SAFI 129 IPv6 の設定例

例：BGP-MVPN SAFI 129 IPv6 の設定

下の例は、PE ルータの設定を示しています。

```
hostname PE1
!
!
vrf definition blue
 rd 55:1111
 route-target export 55:1111
 route-target import 55:1111
 !
 address-family ipv6
  mdt default 232.1.1.1
  mdt data 232.1.200.0 0.0.0.0
 exit-address-family
!
!ip multicast-routing
ip multicast-routing vrf blue
ip cef
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 multicast-routing vrf blue
ipv6 cef
```

```
!
!interface Loopback0
 ip address 205.1.0.1 255.255.255.255
 ip pim sparse-dense-mode
 ipv6 address FE80::205:1:1 link-local
 ipv6 address 205::1:1:1/64
 ipv6 enable
!
interface Ethernet0/0
 ! interface connect to the core vpn
 bandwidth 1000
 ip address 30.3.0.1 255.255.255.0
 ip pim sparse-dense-mode
 delay 100
 ipv6 address FE80::70:1:1 link-local
 ipv6 address 70::1:1:1/64
 ipv6 enable
 mpls ip
!
interface Ethernet1/1
 ! interface connect to CE (vrf interface)
 bandwidth 1000
 vrf forwarding blue
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-dense-mode
 delay 100
 ipv6 address FE80::20:1:1 link-local
 ipv6 address 20::1:1:1/64
 ipv6 enable
!
router ospf 200
 redistribute connected subnets
 redistribute bgp 55 metric 10
 passive-interface Loopback0
 network 30.3.0.0 0.0.255.255 area 1
!
router bgp 55
 bgp log-neighbor-changes
 no bgp default route-target filter
 ! neighbor to another PE in core
 neighbor 205.3.0.3 remote-as 55
 neighbor 205.3.0.3 update-source Loopback0
 !
 address-family ipv4 mdt
  ! neighbor to another PE in core
  neighbor 205.3.0.3 activate
  neighbor 205.3.0.3 send-community extended
 exit-address-family
 !
 address-family vpnv6
  ! neighbor to another PE in core
  neighbor 205.3.0.3 activate
  neighbor 205.3.0.3 send-community extended
 exit-address-family
 !
 address-family vpnv6 multicast
  ! neighbor to another PE in core
  ! this address-family is added to enable
  ! safi129 between two PEs
  neighbor 205.3.0.3 activate
  neighbor 205.3.0.3 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf blue
```

```
  ! neighbor to CE1 in vrf
  redistribute connected
  redistribute static
  neighbor FE80::20:1:6%Ethernet1/1 remote-as 56
  neighbor FE80::20:1:6%Ethernet1/1 activate
 exit-address-family
 !
 address-family ipv6 multicast vrf blue
  !  neighbor to CE1 in vrf
  ! this address-family is added to enable
  ! safi2 on PE-CE
  redistribute connected
  redistribute static
  neighbor FE80::20:1:6%Ethernet1/1 remote-as 56
  neighbor FE80::20:1:6%Ethernet1/1 activate
 exit-address-family
!
ipv6 pim vrf blue rp-address 201::1:1:7 blue_bidir_acl bidir
ipv6 pim vrf blue rp-address 202::1:1:6 blue_sparse_acl
!
ipv6 access-list black_bidir_acl
 permit ipv6 any FF06::/64
!
ipv6 access-list black_sparse_acl
 permit ipv6 any FF04::/64
!
ipv6 access-list blue_bidir_acl
 permit ipv6 any FF05::/64
!
ipv6 access-list blue_sparse_acl
 permit ipv6 any FF03::/64
!
end
```

下の例は、CE ルータの設定を示しています。

```
hostname CE1
!
ip multicast-routing
ip cef
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 multicast rpf use-bgp
ipv6 cef
!
interface Ethernet1/1
 bandwidth 1000
 ip address 10.1.0.6 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 delay 100
 ipv6 address FE80::20:1:6 link-local
 ipv6 address 20::1:1:6/64
 ipv6 enable
 no keepalive
!
router bgp 56
 bgp log-neighbor-changes
 neighbor FE80::20:1:1%Ethernet1/1 remote-as 55
 !
 address-family ipv6
  redistribute connected
```

```
  redistribute static
  neighbor FE80::20:1:1%Ethernet1/1 activate
 exit-address-family
 !
 address-family ipv6 multicast
  redistribute connected
  redistribute static
  neighbor FE80::20:1:1%Ethernet1/1 activate
 exit-address-family
!
ipv6 pim rp-address 201::1:1:7 blue_bidir_acl bidir
ipv6 pim rp-address 202::1:1:6 blue_sparse_acl
!
ipv6 access-list blue_bidir_acl
 permit ipv6 any FF05::/64
!
ipv6 access-list blue_sparse_acl
 permit ipv6 any FF03::/64
!
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*』
BGP 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、使用上のガイドライン、および例	『*Cisco IOS IP Routing: BGP Command Reference*』

標準および RFC

標準/RFC	タイトル
MDT SAFI	『*Subsequent Address Family Identifiers (SAFI) Parameters*』
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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-MVPN SAFI 129 IPv6 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 *82 : BGP—MVPN SAFI 129 IPv6* の機能情報

機能名	リリース	機能情報
BGP—MVPN SAFI 129 IPv6	15.2(4)S Cisco IOS XE Release 3.7S 15.3(1)T	SAFI 129 は、VPN マルチキャスト SAFI とも呼ばれ、サービス プロバイダーのコア IPv6 ネットワークでマルチキャスト ルーティングをサポートする機能を提供します。 次のコマンドが導入または変更されました。**address-family ipv6**、**address-family vpnv6**、**show bgp vpnv6 multicast**

第 64 章

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モード

BFD—BGP マルチホップ クライアント サポート機能により、ボーダー ゲートウェイ プロトコル（BGP）でマルチホップ Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）サポートを使用できるようになります。BFD の障害検出時間はほとんどのネットワーク トポロジで内部ゲートウェイ プロトコル（IGP）コンバージェンス時間よりも速くなるため、BGP コンバージェンスが改善されます。

BFD—BGP cBIT 機能は、BFD 障害がコントロール プレーンに依存しているかいないかを BGP で判別できるようにします。これにより、BGP で BFD ダウン イベントをより柔軟に処理できます。

- 機能情報の確認 （1077 ページ）
- BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの制約事項 （1078 ページ）
- BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードに関する情報 （1078 ページ）
- BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定方法 （1080 ページ）
- BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定例 （1082 ページ）
- その他の参考資料 （1084 ページ）
- BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モードの機能情報 （1084 ページ）

機能情報の確認

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

い。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの制約事項

- BGP IPv4 および BGP IPv6 ピアリング セッションについてのみ、アドレス ファミリ IPv4 および IPv6 ユニキャストの BGP でマルチホップ BFD サポートを使用できます。
- IPv6 リンク ローカル アドレスを使用するマルチホップ BGP セッションでは、BFD マルチホップ サポートは使用できません。
- 現在、BFD ハードウェア オフロードはマルチホップ BFD セッションでサポートされていないため、C-bit はマルチホップ セッションに対しては設定されません。
- IPv6 Virtual Routing and Forwarding（VRF）のマルチホップ BFD はサポートされていません。
- BGP セッションがシングルホップからマルチホップに変わったときに、BFD の BGP セッション属性は動的に変化しないため、マルチホップ BFD セッションを再度開始するには、既存の BGP セッションをクリアする必要があります。

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードに関する情報

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モード

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。BGP 用の BFD を実装する主な利点は、再コンバージェンス時間が非常に短いことです。シングルホップまたはマルチホップの内部 BGP（iBGP）セッ

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モード

ションと外部 BGP（eBGP）セッションでは、BGP でマルチホップ BFD サポートを使用すると、ほとんどのネットワーク トポロジで BFD の障害検出時間が IGP コンバージェンス時間よりも速くなるため、BGP コンバージェンスを改善できます。BGP には、RFC5882『*Generic Application of Bidirectional Forwarding Detection (BFD)*』に記載されているように、マルチホップ BFD のサポートが必要です。

BGP は、デフォルトでは、BFD ダウン イベントが発生し、それについて BFD から通知を受けると、該当のピアから受信したルートを消去します。BFD がコントロール プレーンに依存しているかいないかは、BFD の cBit によって判別されます。BFD をサポートする高速フォールオーバー機能でピアが有効化されている、BGP などのクライアントは、この BFD cBit サポートを使用して、BGP セッションに対する BFD 高速フォールオーバー サポートとともに BGP グレースフル リスタートが有効化されている場合にノンストップ フォワーディング（NSF）を行うためのより確定的なメカニズムを提供します。

BGP でリモート接続検出用の高速フォールオーバー機能のために BFD を使用している場合は、BFD でそれらの障害の一部を検出できます。BFD がコントロール プレーンに依存していない場合、BFD セッション障害が発生すると、（リンク制御障害により）データをそれ以上は転送できなくなるため、トラフィック ブラックホールを避けるために BGP グレースフル リスタートの手順を中止する必要があります。一方、BFD がコントロール プレーンに依存している場合は、コントロール プレーンで発生している他のイベントから BFD 障害を分離することはできません。コントロール プレーンがクラッシュすると、スイッチオーバーが発生し、BFD が再起動します。クライアント（BGP など）では、グレースフル リスタートの実行によるいかなる中止も避けることをお勧めします。

下の表に、BGP による BFD ダウン イベントの処理について示します。

表 *83 : BGP* による *BFD* ダウン イベントの処理

BFD ダウン イベント	障害—コントロール プレーンは独立しているか?	**NSF** に関する **BGP** のアクション（**GR** および **BFD** が有効な場合）
BGP コントロール プレーン障害検出が有効	対応	ルートを消去
BGP コントロール プレーン障害検出が有効	非対応	NSF を続行し、ルーティング情報ベース（RIB）内の失効ルートを保持
BGP コントロール プレーン障害検出が無効（デフォルトの動作）	対応	ルートを消去
BGP コントロール プレーン障害検出が無効（デフォルトの動作）	非対応	ルートを消去

BGP セッションの確立は、高速フォールオーバー検出を除いて、BFD の状態変化とは独立して動作するため、ネクストホップがアクセス不能となり、ベスト パスの再計算が行われます。

これは、neighbor fail-over bfd が設定されている場合でも、BFD 状態がダウンまたはダンプニング済みであるときに BGP セッションを確立できることを意味します。

XE 3.17S リリースから、BFD がダウン状態の場合には BGP セッションの確立を許可しない新しいオプションのキーワード strict-mode が導入されています。BFD がダンプニング済みまたはダウン状態の場合は、ルーティング プロトコルの状態またはセッションをアップ状態にすることはできません。

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定方法

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定

始める前に

（注） 再コンバージェンス中にダウン イベントが誤って識別されて、マルチホップ BGP セッションがフラップしないように、マルチホップ BFD の最小検出時間はネットワークでの IGP コンバージェンス時間よりも長くする必要があります。

（注） BFD ストリクト モードを機能させるには、隣接する両方のデバイスで BFD を設定してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **update-source** *interface-type interface-number*
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **ebgp-multihop** *ttl*
8. **neighbor** *ip-address* **fall-over bfd** [**multi-hop**] [**check-control-plane-failure**] [**strict-mode**]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 50000`	ボーダーゲートウェイ プロトコル（BGP）ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.2 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 5	**neighbor** *ip-address* **update-source** *interface-type interface-number* 例： `Device(config-router)# neighbor 10.0.0.2 update-source GigabitEthernet 0/0/0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。
ステップ 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.0.0.2 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 7	**neighbor** *ip-address* **ebgp-multihop** *ttl* 例： `Device(config-router)# neighbor 10.0.0.2 ebgp-multihop 4`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 8	**neighbor** *ip-address* **fall-over bfd** [**multi-hop**] [**check-control-plane-failure**] [**strict-mode**] 例：	• BGP で隣接関係の変化について指定したネイバーのピアリングセッションをモニタし、ピアリングセッションを非アクティブ化できるようにします。

	コマンドまたはアクション	目的
	`Device(config-router)# neighbor 10.0.0.2 fall-over bfd multi-hop check-control-plane-failure strict-mode`	• BFD cBit サポートについてコントロールプレーンの独立性を有効にして BGP BFD を設定します。
ステップ 9	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BFD - BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの設定例

例：BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モードの設定

```
R1 e0/0 ---------------e0/0 R2

Router 1 configuration

hostname R1
!
bfd map ipv4 2.2.2.2/32 1.1.1.1/32 mh1
!
bfd-template multi-hop mh1
interval min-tx 50 min-rx 50 multiplier 3
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
ip ospf 1 area 0
!
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0
ip ospf 1 area 0
!
router ospf 1
!
router bgp 1
neighbor 2.2.2.2 remote-as 1
neighbor 2.2.2.2 update-source Loopback1
neighbor 2.2.2.2 fall-over bfd multi-hop check-control-plane-failure strict-mode
!
address-family ipv4
neighbor 2.2.2.2 activate
exit-address-family
!

Router 2 configuration:
```

```
hostname R2
!
bfd map ipv4 1.1.1.1/32 2.2.2.2/32 mh1
bfd-template multi-hop mh1
interval min-tx 50 min-rx 50 multiplier 3
!
interface Loopback1
ip address 2.2.2.2 255.255.255.255
ip ospf 1 area 0
!
interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
ip ospf 1 area 0
!
router ospf 1
!
router bgp 1
neighbor 1.1.1.1 remote-as 1
neighbor 1.1.1.1 update-source Loopback1
neighbor 1.1.1.1 fall-over bfd multi-hop check-control-plane-failure strict-mode
!
address-family ipv4
neighbor 1.1.1.1 activate
exit-address-family
!
```

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4 および IPv6）、ストリクト モードの確認

次の例は、ネイバー、ピアグループで BFD が有効になっているかどうかを確認する方法を示しています。

```
R801-ASBR#sh ip bgp neighbor 11.1.0.2 BGP neighbor is 11.1.0.2, remote AS 65000,
 external link Fall over configured for session BFD is configured. BFD peer is
 Up. Using BFD to detect fast fallover (single-hop) in strict-mode. BGP version
 4, remote router ID 10.10.10.10 BGP state = Established, up for 00:04:12 Last
 read 00:00:49, last write 00:00:24, hold time is 180, keepalive interval is
60 seconds …
```

BFD がアップ状態で実行中の場合は、次のように表示されます。

```
Fall over configured for session BFD is configured. BFD peer is Up. Using BFD
 to detect fast fallover (single-hop) in strict-mode (will be verified). …
```

BFD がアップ状態でなく実行されていない場合は、次のように表示されます。

```
Fall over configured for session BFD is configured. BFD peer is Down. Using
BFD to detect fast fallover (single-hop) in strict-mode.
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モードの機能情報

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 *84 : BFD—BGP* マルチホップ クライアント サポート、*cBit*（*IPv4/IPv6*）、ストリクト モードの機能情報

機能名	リリース	機能情報
BFD—BGP マルチホップ クライアント サポートおよび cBit（IPv4/IPv6）	15.2(4)S Cisco IOS XE Release 3.6S Cisco IOS XE リリース 3.7S	BFD—BGP マルチホップ クライアント サポート機能により、ボーダー ゲートウェイ プロトコル（BGP）でマルチホップ Bidirectional Forwarding Detection（BFD）サポートを使用できるようになります。BFD の障害検出時間はほとんどのネットワーク トポロジで内部ゲートウェイ プロトコル（IGP）コンバージェンス時間よりも速くなるため、BGP コンバージェンスが改善されます。 BFD—BGP cBIT 機能は、BFD 障害がコントロール プレーンに依存しているかいないかを BGP で判別できるようにします。これにより、BGP で BFD ダウン イベントをより柔軟に処理できます。 Cisco IOS XE Release 3.7S では、Cisco ASR 903 ルータのサポートが追加されました。 次のコマンドが変更されました。**neighbor fall-over**、**show ip bgp neighbors**
BFD—BGP マルチホップ クライアント サポート、cBit（IPv4/IPv6）、ストリクト モード	Cisco IOS XE リリース 3.17S	Cisco IOS XE Release 3.17S では、次のコマンドが変更されました。 **neighbor** *ip-address* **fall-over bfd** [**multi-hop**|**single-hop**] [**check-control-plane-failure**] [**strict-mode**]

第 65 章

BGP属性フィルタと拡張属性エラーの処理

BGP 属性フィルタ機能を使用すると、特定のパス属性を含むアップデートを取り消す（「treat-as-withdraw」）ことができます。アップデートに含まれるプレフィックスは、ルーティングテーブルから削除されます。また、この機能では、着信アップデートから特定のパス属性を削除することもできます。どちらの動作でも、セキュリティ対策が向上します。BGP拡張属性エラー処理機能は、形式が誤っているアップデートのエラーによるピアセッションのフラッピングを防止して、リソースを節約します。

- 機能情報の確認 （1087 ページ）
- BGP 属性フィルタリングに関する情報 （1088 ページ）
- BGP パス属性をフィルタ処理する方法 （1089 ページ）
- BGP 属性フィルタの設定例 （1092 ページ）
- その他の参考資料 （1093 ページ）
- BGP 属性フィルタと拡張属性エラー処理の機能情報 （1094 ページ）

機能情報の確認

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

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

BGP 属性フィルタリングに関する情報

BGP 属性フィルタと拡張属性エラーの処理

BGP 属性フィルタ機能は、セキュリティ対策を向上させる次の 2 つの方法を提供します。

- この機能では、指定したネイバーから受け取ったアップデートに、指定した属性タイプが含まれている場合に、そのアップデートを取り消すことができます。アップデートを取り消すと、そのアップデート内のプレフィックスは BGP ルーティング テーブルから削除されます（ルーティング テーブル内に存在する場合）。
- また、この機能では、アップデートから指定したパス属性をドロップすることもできます。その場合、残りのアップデートは通常どおりに処理されます。

BGP 拡張属性エラー処理機能は、形式が誤っているアップデートに起因するピア セッションのフラッピングを防止します。形式が誤っているアップデートは取り消され、BGPセッションがリセットされることはありません。この機能はデフォルトで有効になっていますが、無効にすることができます。

機能は、次の順序で実装されます。

1. ユーザ指定のパス属性を含むアップデートを受信すると、そのアップデートは取り消されます（NLRI を正常に解析できる場合のみ）。BGP ルーティング テーブルに既存のプレフィックスがある場合、そのプレフィックスは削除されます。この機能は **neighbor path-attribute treat-as-withdraw** コマンドによって設定します。
2. 受信したアップデートからユーザ指定のパス属性が破棄され、残りのアップデートは正常に処理されます。この機能は **neighbor path-attribute discard** コマンドによって設定します。
3. 形式が誤っているアップデートを受信すると、そのアップデートは取り消されます。この機能はデフォルトで有効になっています。**no bgp enhanced-error** コマンドを設定すると、無効にすることができます。

treat-as-withdraw を属性に指定する場合の詳細

属性タイプ 1、2、3、4、8、14、15、16 は、パス属性 treat-as-withdraw に対して設定できません。

属性タイプ 5（localpref）、タイプ 9（Originator）、タイプ 10（Cluster-id）は、eBGP ネイバーでのみ treat-as-withdraw に対して設定できます。

取り消しとして処理（treat-as-withdraw）されるようにパス属性を設定すると、ルーティング テーブルを最新の状態に維持するために着信ルート リフレッシュがトリガーされます。

discard を属性に指定する場合の詳細

属性タイプ 1、2、3、4、8、14、15、16 は、パス属性 discard に対して設定できません。

属性タイプ 5（localpref）、タイプ 9（Originator）、タイプ 10（Cluster-id）は、eBGP ネイバーでのみ discard に対して設定できます。

破棄（discard）されるようにパス属性を設定すると、ルーティング テーブルを最新の状態に維持するために着信ルート リフレッシュがトリガーされます。

拡張属性エラー処理の詳細

形式が誤っているアップデートを受信すると、BGP パス属性の処理によるピア セッションのフラッピングを防止するために、そのアップデートは取り消されます（treat-as-withdraw）。この機能は、eBGP ピアと iBGP ピアに適用されます。この機能はデフォルトで有効になっていますが、無効にすることができます。

BGP 拡張属性エラー処理機能を有効または無効にすると、BGP では、アップデートの形式を整えると同時に属性リストの先頭に MP_REACH 属性（属性 14）を配置します。MP_REACH 属性が属性リストの先頭にあると、拡張属性エラー処理がより簡単に機能します。

BGP パス属性をフィルタ処理する方法

指定したパス属性を含む BGP アップデートの取り消し

（注） この作業を実行すると、ルーティング テーブルを最新の状態に維持するために着信ルート リフレッシュがトリガーされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address*} **path-attribute treat-as-withdraw** {*attribute-value* | **range** *start-value end-value*} **in**
5. 手順 4 を繰り返して、範囲に含まれない他の属性を設定するか、別のネイバーを設定します。
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*} **path-attribute treat-as-withdraw** {*attribute-value* | **range** *start-value end-value*} **in** 例： `Device(config-router)# neighbor 2001:DB8:1::1 path-attribute treat-as-withdraw 100 in`	指定したパス属性またはパス属性の範囲を含む着信アップデート メッセージをすべて取り消します。 • 取り消されるアップデート内のプレフィックスは、BGP ルーティング テーブルから削除されます。 • 特定の属性値と属性値の範囲は、互いに独立しています。
ステップ 5	手順 4 を繰り返して、範囲に含まれない他の属性を設定するか、別のネイバーを設定します。	
ステップ 6	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

アップデート メッセージからの特定パス属性の破棄

（注） この作業を実行すると、ルーティング テーブルを最新の状態に維持するために着信ルート リフレッシュがトリガーされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address*} **path-attribute discard** {*attribute-value* | **range** *start-value end-value*} **in**
5. 手順 4 を繰り返して、範囲に含まれない他の属性を設定するか、別のネイバーを設定します。
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 6500`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*} **path-attribute discard** {*attribute-value* | **range** *start-value end-value*} **in** 例： `Device(config-router)# neighbor 2001:DB8:1::1 path-attribute discard 128 in`	指定したネイバーからのアップデート メッセージから指定したパス属性を削除します。
ステップ 5	手順 4 を繰り返して、範囲に含まれない他の属性を設定するか、別のネイバーを設定します。 例：	
ステップ 6	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

取り消されたパス属性または破棄されたパス属性の表示

取り消されたパス属性、破棄されたパス属性、または不明なパス属性に関する情報を表示するには、これらの手順のいずれかを任意の順序で実行します。**show ip bgp** コマンドは、**show ip bgp ipv4 multicast**、**show ip bgp ipv6 unicast** など、BGP がサポートする任意のアドレス ファミリで使用できます。

手順の概要

1. **enable**
2. **show ip bgp neighbor** [*ip-address* | *ipv6-address*]

3. **show ip bgp path-attribute unknown**
4. **show ip bgp path-attribute discard**
5. **show ip bgp vpnv4 all** *prefix*
6. **show ip bgp neighbors** *prefix*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp neighbor** [*ip-address* | *ipv6-address*] 例： `Device# show ip bgp neighbor 2001:DB8:1::1`	（任意）ネイバーに対して設定された discard および treat-as-withdraw 属性値、そのような属性が破棄または取り消されたアップデートの数、および形式が誤っているために取り消されたアップデートの数を表示します。
ステップ 3	**show ip bgp path-attribute unknown** 例： `Device# show ip bgp path-attribute unknown`	（任意）不明な属性を持つすべてのプレフィックスを表示します。
ステップ 4	**show ip bgp path-attribute discard** 例： `Device# show ip bgp path-attribute discard`	（任意）属性が破棄されたすべてのプレフィックスを表示します。
ステップ 5	**show ip bgp vpnv4 all** *prefix* 例： `Device# show ip bgp vpnv4 all 192.168.1.0`	（任意）プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。
ステップ 6	**show ip bgp neighbors** *prefix* 例： `Device# show ip bgp neighbors 192.168.1.0`	（任意）プレフィックスに関連付けられている設定済みの discard および treat-as-withdraw 属性を表示します。

BGP 属性フィルタの設定例

例：パス属性に基づくアップデートの取り消し

次の例では、指定したネイバーからのアップデート メッセージに不要なパス属性 100 または 128 が含まれている場合は取り消すようにデバイスを設定する方法を示します。

```
router bgp 65600
 neighbor 2001:DB8:1::2 path-attribute treat-as-withdraw 100 in
 neighbor 2001:DB8:1::2 path-attribute treat-as-withdraw 128 in
```

次の例では、指定したネイバーからのアップデート メッセージに 21 ～ 255 の範囲内の不要なパス属性が含まれている場合は取り消すようにデバイスを設定する方法を示します。

```
router bgp 65600
 neighbor 2001:DB8:1::2 path-attribute treat-as-withdraw 21 255 in
```

例：アップデートからのパス属性の破棄

次の例では、指定したネイバーからの着信アップデート メッセージからパス属性 100 および 128 を破棄するようにデバイスを設定する方法を示します。アップデート メッセージの残りの部分は、通常どおりに処理されます。

```
router bgp 65600
 neighbor 2001:DB8:1::1 path-attribute discard 100 in
 neighbor 2001:DB8:1::1 path-attribute discard 128 in
```

次の例では、指定したネイバーからの着信アップデート メッセージから 17 ～ 255 の範囲内のパス属性を破棄するようにデバイスを設定する方法を示します。アップデート メッセージの残りの部分は、通常どおりに処理されます。

```
router bgp 65600
 neighbor 2001:DB8:1::1 path-attribute discard 17 255 in
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
draft-ietf-idr-error-handling	外部ネイバーからの BGP アップデートに関するエラー処理の修正

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 属性フィルタと拡張属性エラー処理の機能情報

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 *85 : BGP* 属性フィルタと拡張属性エラー処理の機能情報

機能名	リリース	機能情報
BGP 属性フィルタと拡張属性エラーの処理		BGP 属性フィルタを使用すると、特定のパス属性を含むアップデートを取り消す（「treat-as-withdraw」）ことができます。アップデートに含まれるプレフィックスは、ルーティング テーブルから削除されます。また、この機能では、着信アップデートから特定のパス属性を削除することもできます。どちらの動作でも、セキュリティ対策が向上します。BGP 拡張属性エラー処理機能は、形式が誤っているアップデートのエラーによるピア セッションのフラッピングを防止して、リソースを節約します。 次のコマンドが導入されました。**bgp enhanced-error**、**neighbor path-attribute discard**、**neighbor path-attribute treat-as-withdraw**、**show ip bgp path-attribute discard**、 **show ip bgp path-attribute unknown** 次のコマンドが変更されました。**show ip bgp**、**show ip bgp neighbor**、**show ip bgp vpnv4 all**

第 66 章

BGP の追加パス

BGP 追加パスは、暗黙的に以前のパスから新しいパスに代わることなく、同じピア セッションを介して同じプレフィックスのマルチパスをアドバタイズする機能を備えています。この動作により、パス ダイバーシティが向上し、Multi-Exit Discriminator（MED）の変動が減少します。

- 機能情報の確認 （1097 ページ）
- BGP 追加パスについて （1098 ページ）
- BGP 追加パスの設定方法 （1102 ページ）
- BGP 追加パスの設定例 （1113 ページ）
- その他の参考資料 （1115 ページ）
- BGP 追加パスの機能情報 （1116 ページ）

機能情報の確認

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

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

BGP 追加パスについて

追加パスで解決できる問題

BGP ルータおよびルート リフレクタ（RR）は、セッションにおけるベスト パスにのみ伝播します。プレフィックス アドバタイズメントで、以前アナウンスされたプレフィックスを置き換えます（この動作は暗黙の取り消しとして知られています）。暗黙の取り消しはスケーリングには適していますが、パス ダイバーシティに影響があります。

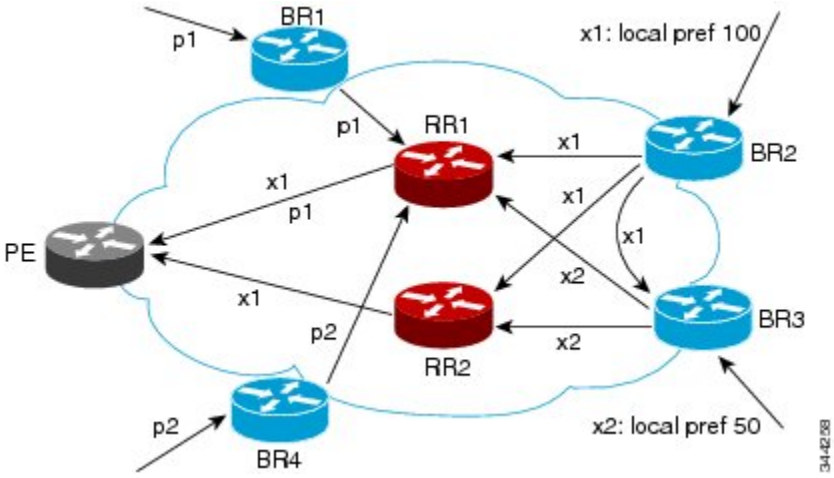
パスの隠蔽は BGP マルチパスの効率的な使用や、スムーズな定期メンテナンスを妨げ、MED の変動や最適でないホットポテト ルーティングが発生する可能性があります。ネクスト ホップが失敗した場合も、ネットワークは BGP コントロール プレーンのコンバージェンスによりトラフィックが復旧するのを待たなければならないので、パスの隠蔽は迅速かつローカルの復旧の妨げになります。BGP 追加パス機能では、パス ダイバーシティを一般的な方法で提供します。Best External または Best Internal 機能は、限られた場合にのみパス ダイバーシティを提供します。

BGP 追加パス機能は、同じプレフィックスのマルチパスに対して、新しいパスで以前のパスを暗黙的に置き換えることなく、アドバタイズする手段を提供します。したがって、パスを隠蔽しないでパス ダイバーシティが実現されます。

パスの隠蔽の例

ここでは、パスの隠蔽が発生する過程の詳細を説明します。次の図では、BR1 および BR4 から RR1 にアドバタイズされるプレフィックス p を持つパス p1 および p2 があります。RR1 は 2 つのうちベスト パスを選択し、PE に p1 のみアドバタイズします。

図 *84 : RR* で追加パスを非表示にする



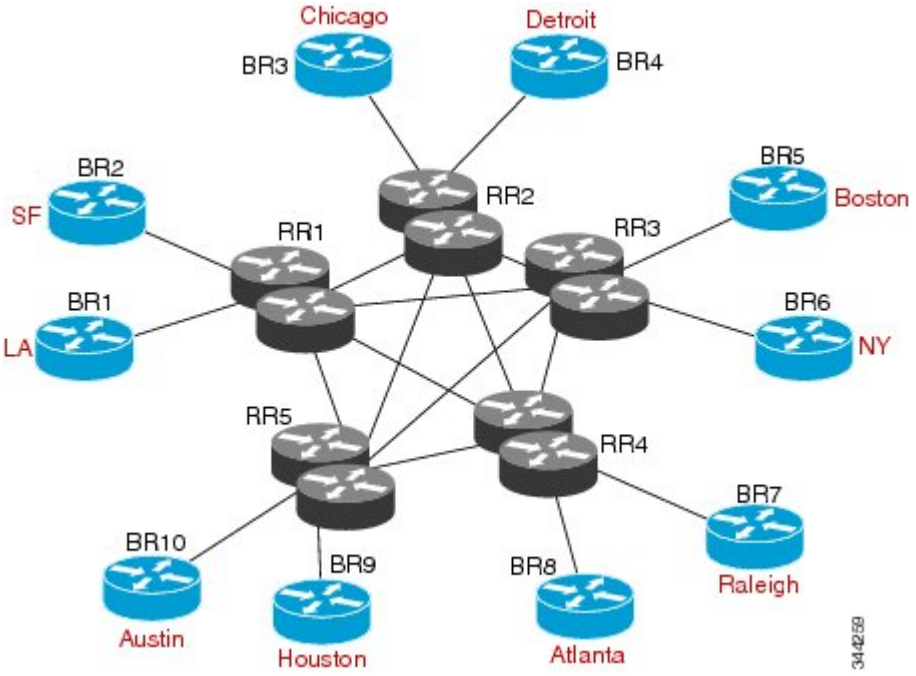
また上の図では、BR2 から（パス x2 がある）BR3 にローカル プリファレンス 100 でアドバタイズされる、プレフィックス x を持つパス x1 が表示されています。BR3 にはパス x2 もありますが、ルーティング ポリシーにより、x2 ではなく RR の x1（表示されていません）をアドバ

タイズし、x2 のアドバタイズは抑制されます。ユーザは BR3 で最良外部のアドバタイズメントを有効にして RR に x2 をアドバタイズできますが、この場合も RR はベスト パスのみをアドバタイズします。

最適ではないのホット ポテト ルーティングの例

内部転送コストを最小化するために、中継する ISP は（内部ゲートウェイ プロトコル（IGP）コストに基づいて）最も近い出口ポイントにパケットを転送しようとします。この動作は、ホット ポテト ルーティングと呼ばれます。次の図の分散 RR クラスタ モデルでは、ロサンゼルスから発信されるトラフィックがメキシコに進む必要があることを想定しています。すべてのリンクで、IGP コストは同じです。メキシコへの出口ポイントは 2 つあり、1 つがオースティンに向かい、もう 1 つがアトランタに向かう場合、ロサンゼルスからは、アトランタよりオースティンに向かう方が IGP コストが低いため、オースティンに向けてトラフィックを送信します。RR3 がある（および RR1、RR2、RR4 および RR5 がない）場所に中央 RR が存在する集中型 RR モデルでは、RR3 から見てメキシコへの最も近い出口ポイントはアトランタとなります。ロサンゼルスからアトランタに向けてトラフィックが送信され、それによって最適ではないホットポテト ルーティングが生じます。これは望ましいことではありません。

図 *85* : 分散 *RR* クラスタ

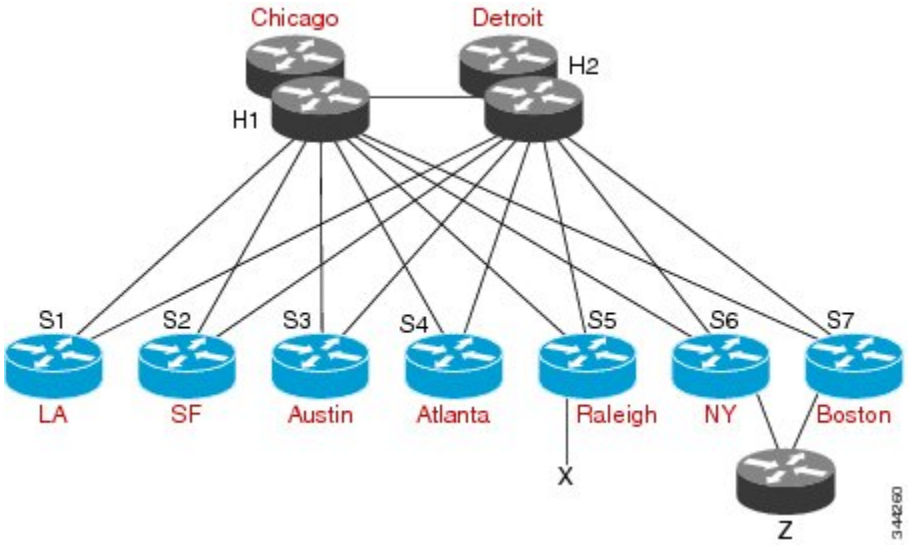


DMVPN シナリオ

Dynamic Multipoint Virtual Private Network（DMVPN; ダイナミック マルチポイント仮想プライベート ネットワーク）の展開では、BGP はスケーリングのために使用されます。下の図では、Z は、スポーク S6（NY）とスポーク S7（ボストン）に接続されています。ハブへの S7 リンクは、ハブへの S6 リンクよりも IGP コストが低くなっています。S5 を S7 に、S6 を S7 に接続する物理的なリンクがあり（図には非表示）、IGP コストはハブへのリンクよりも低くなっています。スポーク S6 とスポーク S7 は、ハブ H1（シカゴ）とハブ H2（デトロイト）にアップデートを送信します。その後、RR ハブは、IGP コストがより低いことに基づいてベスト パ

スを選択します。これは、S7 であることもあります。このシナリオでは、S6（NY）をネクスト ホップとして選択する方が望ましい可能性もありますが、スポーク S5（ローリー）は、Z について S7 をネクスト ホップとする 2 つのアップデートを RR から受信します。

図 *86 : DMVPN* 展開



BGP 追加パスの利点

BGP ルータおよびルート リフレクタ（RR）は、セッションにおけるベスト パスにのみ伝播します。プレフィックス アドバタイズメントで、以前アナウンスされたプレフィックスを置き換えます（この動作は暗黙の取り消しとして知られています）。

この動作は、スケーリングには適していますが、パス ダイバーシティを妨げる可能性があります（これによって脆弱になるまたは完全に無くなるおそれがあります）。同様にこの動作は、BGP マルチパスの効率的な使用や、スムーズな定期メンテナンスを妨げ、MED の変動や最適でないホットポテト ルーティングが発生する可能性があります。ネクスト ホップが失敗した場合も、ネットワークは BGP コントロール プレーンのコンバージェンスによりトラフィックが復旧するのを待たなければならないので、迅速かつローカルの復旧の妨げになります。

BGP 追加パス機能は、暗黙的に以前のパスに代わる新しいパスなしで、同じプレフィックスのマルチパスをアドバタイズする BGP の拡張機能です。これにより、パス ダイバーシティが向上し、MED の変動が減少します。

BGP 追加パスの機能

BGP 追加パス機能は、NLRI で各パスにパス ID を追加することによって実現します。パス ID は VPN のルート識別子（RD）のようなものです。ただし、パス ID はすべてのアドレス ファミリに適用できます。パス ID はピアリング セッション内で一意で、各ネットワークに生成されます。ルート アナウンスが暗黙的に以前のパスを取り消すことを防ぐために、パス ID が使用されます。追加パス機能は、ベスト パスに加えその他のパスのアドバタイズメントが可能で

す。追加パスは、暗黙的に以前のパスから新しいパスに代わることなく、同じプレフィックスのマルチパスをアドバタイズする機能を備えています。

BGP 追加パス機能を使用する場合は、次の 3 つの一般的な手順を実行する必要があります。

1. デバイスが追加パスを送信、受信、または送受信するかどうかを指定します。これは、アドレス ファミリ レベルまたはネイバー レベルで行い、それぞれ **bgp additional-paths** {**send** [**receive**] | **receive**} コマンドまたは **neighbor additional-paths** {**send** [**receive**] | **receive**} コマンドで制御します。セッションの確立中に、2 つの BGP ネイバーが追加パス機能（送信または受信のどちら（あるいは両方）を実行できるか）についてネゴシエートします。

2. 選択基準を指定して、アドバタイズする候補パスのセットを選択します（**bgp additional-paths select** コマンドを使用）。

3. 示された候補パスから追加パスのセットをネイバーに対してアドバタイズします（**neighbor advertise additional-paths** コマンドを使用）。

追加パスを送受信するには、追加パス機能をネゴシエートする必要があります。ネゴシエートされない場合、選択基準によりベストパス以上のパスが指定され、ネイバーが指定されたパスをアドバタイズするように設定されていても、ネゴシエートできないために選択パスは利用されず、ベストパスのみ送信されます。

追加パスの送受信を BGP に設定すると、デバイスのピアに対して追加パス機能のネゴシエーションが開始されます。この機能についてネゴシエートしたネイバーは、（他のアップデート グループ ポリシーが許可する場合）アップデート グループに追加され、この機能についてネゴシエートされていないピアとは別のアップデート グループに分類されます。したがって、追加パス機能によってネイバーのアップデート グループ メンバーシップが再計算されます。

追加パスの選択

3 つのパス選択（パス マーキング）ポリシーがあり、相互に排他的ではありません。これらは、 **bgp additional-paths select** コマンドを使用して、アドレス ファミリごとに指定します。その内容は次のとおりです。

- **best 2** または **best 3**（**best 2** は、ベストパスおよび 2 番目に適したパスを意味します。2 番目に適したパスは、ベストパス計算アルゴリズムからベストパスを除外することで計算されます。同様に、**best 3** は、ベストパス、2 番目に適したパス、および 3 番目に適したパスを意味します。3 番目に適したパスは、ベストパス計算アルゴリズムからベストパスと 2 番目に適したパスを除外することで計算されます）。
- **group-best** （ベストパス計算時にプレフィックスのグループベスト パス（group-best）を計算します。詳細は下記を参照してください）
- **all** （固有のネクスト ホップを持つすべてのパスが選択対象となります）

group-best 選択の定義

group-best キーワードは、次のコマンドの一部です。

- **advertise additional-paths**
- **bgp additional-paths select**

- **match additional-paths advertise-set**
- **neighbor advertise additional-paths**

group-best は、同じ AS のパスからのベストパスであるパスのセットです。たとえば、AS 100、200、300 という 3 つの自律システムがあるとします。p101、p102、p103 は、AS 100 からのパスで、p201、p202、p203 は AS200 からのパスで、p301、p302、p303 は AS300 からのパスです。各 AS からのパスに対して BGP ベストパスアルゴリズムを実行すると、アルゴリズムは、各 AS からの各パス セットから 1 つのベストパスを選択します。p101 が AS100 からのベストパスで、p201 が AS200 からのベストパスで、p301 が AS300 からのベストパスであると仮定すると、**group-best** は、p101、p201、p301 のセットになります。

選択したパスの一部をアドバタイズ

パスのセットを選択する際に、別のパスのセットをアドバタイズしたい場合は注意してください。アドバタイズするパスのセットが、選択されたパスのサブセットではない場合、意図したパスがアドバタイズされません。

次の例では、選択される追加パスが group-best および all 選択となるように設定します。ただし、ネイバーにアドバタイズされるように設定するパスは、最適な 3 つのパス（best 3）です。選択およびアドバタイズのポリシーは同じではないため、次のメッセージが表示されます。このような場合は、ベストパスのみがアドバタイズされます。

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4
Device(config-router-af)# bgp additional-paths send receive
Device(config-router-af)# bgp additional-paths select group-best all
Device(config-router-af)# neighbor 192.168.2.2 advertise additional-paths best 3
 % BGP: AF level 'bgp additional-paths select' more restrictive than advertising policy.
 This is a reminder that AF level additional-path select commands are needed.
```

BGP 追加パスの設定方法

アドレス ファミリごとの追加パスの設定

追加パスの候補となるパスを選択する場合は、手順 6、7、8 を任意に組み合わせて実行できますが、これらの手順のうち少なくとも 1 つは実行する必要があります。

ネイバーごとに追加パスを無効にする場合は、「ネイバーごとの追加パスの無効化」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**unicast** | **multicast**]
5. **bgp additional-paths** {**send** [**receive**] | **receive**}

6. **bgp additional-paths select group-best**
7. **bgp additional-paths select best** *number*
8. **bgp additional-paths select all**
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name* } **advertise additional-paths** [**best** *number*] [**group-best**] [**all**]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**unicast**	**multicast**] 例： `Device(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始します。 • サポートされているアドレス ファミリは、IPv4 ユニキャスト、IPv4 マルチキャスト、IPv4 ユニキャスト+ラベル、IPv6 ユニキャスト、IPv6 マルチキャスト、IPv6 マルチキャスト+ラベルです。
ステップ 5	**bgp additional-paths** {**send** [**receive**]	**receive**} 例： `Device(config-router-af)# bgp additional-paths send receive`	ネイバーとのネゴシエーションが完了した後に、BGP 追加パスの送信のみ、受信のみ、または送受信を行えるようにします。 • この例では、追加パスを送受信できるようにしています。

	コマンドまたはアクション	目的
ステップ 6	**bgp additional-paths select group-best** 例： `Device(config-router-af)# bgp additional-paths select group-best`	（任意）ベストパス計算時にプレフィックスのグループベスト パスを計算します。
ステップ 7	**bgp additional-paths select best** *number* 例： `Device(config-router-af)# bgp additional-paths select best 3`	（任意）ベストパスのアドバタイズを含む、指定した数のベスト パスを計算します。 • *number* の値には 2 または 3 を指定できます。
ステップ 8	**bgp additional-paths select all** 例： `Device(config-router-af)# bgp additional-paths select all`	（任意）固有のネクスト ホップを持つすべてのパスが選択対象となることを指定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name* } **advertise additional-paths** [**best** *number*] [**group-best**] [**all**] 例： `Device(config-router-af)# neighbor 192.168.0.1 advertise additional-paths best 3 group-best all`	ネイバーにアドバタイズされる追加のパスを制御する選択方法を指定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権EXECモードに戻ります。

ネイバーごとの追加パスの設定

追加パスの候補となるパスを選択する場合は、手順6、7、8を任意に組み合わせて実行できますが、これらの手順のうち少なくとも 1 つは実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**unicast** | **multicast**]
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **additional-paths** {**send** [**receive**] | **receive**}
6. **bgp additional-paths select group-best**
7. **bgp additional-paths select best** *number*
8. **bgp additional-paths select all**
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **advertise additional-paths** [**best** *number*] [**group-best**] [**all**]

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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv4 unicast`	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。 • サポートされているアドレス ファミリは、IPv4 ユニキャスト、IPv4 マルチキャスト、IPv4 ユニキャスト+ラベル、IPv6 ユニキャスト、IPv6 マルチキャスト、IPv6 マルチキャスト+ラベルです。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **additional-paths** {**send** [**receive**] | **receive**} 例： `Device(config-router-af)# neighbor 192.168.1.2 additional-paths send receive`	ネゴシエーションが完了した後にネイバーが追加パスを送信または受信できるようにします。 • この例では、ネイバーが追加パスを送受信できるようにしています。 • このコマンドはアドレス ファミリのレベルで設定されたすべての送受信機能をオーバーライドすることに注意してください。
ステップ 6	**bgp additional-paths select group-best** 例：	（任意）ベストパス計算時にプレフィックスのグループベスト パスを計算します。

	コマンドまたはアクション	目的
	`Device(config-router-af)# bgp additional-paths select group-best`	
ステップ 7	**bgp additional-paths select best** *number* 例： `Device(config-router-af)# bgp additional-paths select best 3`	（任意）ベストパスの選択を含む、指定した数のベスト パスを計算します。 • *number* の値には 2 または 3 を指定できます。
ステップ 8	**bgp additional-paths select all** 例： `Device(config-router-af)# bgp additional-paths select all`	（任意）固有のネクスト ホップを持つすべてのパスが選択対象となることを指定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **advertise additional-paths** [**best** *number*] [**group-best**] [**all**] 例： `Device(config-router-af)# neighbor 192.168.1.2 advertise additional-paths best 3 group-best all`	ネイバーにアドバタイズされる追加パスを制御する選択方法を指定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権EXECモードに戻ります。

ピア ポリシー テンプレートを使用した追加パスの設定

この設定作業例では、追加パスを送受信する機能および選択基準をアドレス ファミリに設定してから、テンプレートを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 unicast**
5. **bgp additional-paths** {**send** [**receive**] | **receive**}
6. **bgp additional-paths select** [**best** *number*] [**group-best**] [**all**]
7. **template peer-policy** *policy-template-name*
8. **additional-paths** {**send** [**receive**] | **receive**}
9. **advertise additional-paths** [**best** *number*] [**group-best**] [**all**]
10. **exit**
11. **address-family ipv4 unicast**
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
13. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*

14. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4 unicast** 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを設定します。
ステップ 5	**bgp additional-paths** {**send** [**receive**] | **receive**} 例： `Device(config-router)# bgp additional-paths send receive`	該当のアドレス ファミリのピアに対して、BGP 追加パスの送信のみ、受信のみ、または送受信を行えるようにします。
ステップ 6	**bgp additional-paths select** [**best** *number*] [**group-best**] [**all**] 例： `Device(config-router)# bgp additional-paths select best 3 group-best all`	ベストパスに加えて、アドバタイズの候補となる BGP 追加パスが計算されるようにします。
ステップ 7	**template peer-policy** *policy-template-name* 例： `Device(config-router)# template peer-policy rr-client-pt1`	ポリシー テンプレート コンフィギュレーション モードを開始し、ピア ポリシー テンプレートを作成します。

	コマンドまたはアクション	目的
ステップ 8	**additional-paths** {**send** [**receive**] | **receive**} 例： `Device(config-router-ptmp)# additional-paths send receive`	ピア ポリシー テンプレートの対象となるピアに対して、BGP 追加パスの送信のみ、受信のみ、または送受信を行えるようにします。
ステップ 9	**advertise additional-paths** [**best** *number*] [**group-best**] [**all**] 例： `Device(config-router-ptmp)# advertise additional-paths best 3 group-best all`	ピア ポリシー テンプレートの対象となるピアにアドバタイズされる追加パスを制御する選択方法を指定します。
ステップ 10	**exit** 例： `Device(config-router-ptmp)# exit`	ポリシー テンプレート コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 11	**address-family ipv4 unicast** 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを設定します。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	エントリを BGP ネイバー テーブルに追加します。
ステップ 13	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* 例： `Device(config-router-af)# neighbor 192.168.1.1 inherit peer-policy rr-client-pt1`	ネイバーが設定を継承できるように、ピア ポリシー テンプレートをこのネイバーに送信します。
ステップ 14	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

追加パスのフィルタリングおよび設定操作

必要に応じて、アドバタイズされる候補である追加パスのタグを照合することで、アドバタイズされるパスをフィルタ処理するためにルート マップを使用できます（このタグは、**bgp additional-paths select** コマンドで設定されている advertise-set です）。**match additional-paths advertise-set** コマンドで設定されているマーキングと同じパス マーキング（タグ）を持つパスが、ルート マップ エントリと一致します（そして、許可または拒否されます）。

また、必要に応じて、ルートマップを通過したこれらのパスに対して実行するアクションを設定することもできます。この作業では、**set metric** コマンドを使用して、**match additional-paths advertise-set** コマンドでルート マップを使用する方法を示します。当然ながら、この作業で記載のない他の **set** コマンドも使用できます。

all でマークされたパス（固有のネクスト ホップを持つすべてのパス）にメトリックを設定するのは、以下の理由によります。ネイバー 2001:DB8::1037 が別のネイバーから同じルートを受信しているとします。ローカル デバイスから受信されたルートはメトリックが 565 で、メトリックが 700 の別のデバイスからのルートが存在する可能性があります。メトリックが 565 のルートは、メトリックが 700 のルートよりも優先されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match additional-paths advertise-set** [**best** *number*] [**best-range** *start-range end-range*] [**group-best**] [**all**]
5. **set metric** *metric-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 additional_path1 permit 10`	ルート マップを作成します。

	コマンドまたはアクション	目的
ステップ 4	**match additional-paths advertise-set** [**best** *number*] [**best-range** *start-range end-range*] [**group-best**] [**all**] 例： `Device(config-route-map)# match additional-paths advertise-set best 3`	指定したパス選択ポリシーを使用して、タグが付けられているすべてのパスを照合します。 • 選択方法を少なくとも 1 つは指定する必要があります。このコマンドでは、複数の選択方法を指定できます。 • **best** *number* の指定は **best-range** の指定と互換性がありません。 • **best 1** を指定した場合、ベストパスのみが一致します。 • **best-range 1 1** を指定した場合、ベストパスのみが一致します。 • **match additional-paths advertise-set** コマンドはルートマップごとに 1 つしか使用できません。後続の **match additional-paths advertise-set** コマンドは、前のコマンドを上書きします。
ステップ 5	**set metric** *metric-value* 例： `Device(config-route-map)# set metric 500`	一致基準を満たす追加パスのメトリックを設定します。 • 他の **set** コマンドを使用して、ルート マップを通過したパスに対してアクションを実行することもできます。この例では、**set metric** コマンドを使用しています。

次のタスク

ルート マップを作成した後、**neighbor route-map out** コマンドでそのルート マップを参照します。つまり、ルートマップは、ネイバーにアドバタイズ（発信）されるパスに適用されます。次に、**neighbor advertise additional-paths** コマンドを使用して、追加パスをアドバタイズします。前後関係を含めてルート マップを確認する場合は、「例：BGP 追加パス」の項を参照してください。

追加パス情報の表示

BGP 追加パスに関する情報を表示するには、この作業の手順 2 または手順 3 を実行します。

手順の概要

1. **enable**
2. **show ip bgp neighbors** [*ip-address*]
3. **show ip bgp** [*network*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp neighbors** [*ip-address*] 例： `Device# show ip bgp neighbors 192.168.1.1`	追加パスを送受信するネイバーの機能を表示します。
ステップ 3	**show ip bgp** [*network*] 例： `Device# show ip bgp 192.168.0.0`	ネットワークの追加パス選択およびパス ID を表示します。

ネイバーごとの追加パスの無効化

（**neighbor additional-paths** コマンドを使用して）ネイバーごとに追加パスの送信または受信を設定している場合に、その機能を無効にするには、**no neighbor additional-paths** コマンドを使用します。

ただし、（**bgp additional-paths** コマンドを使用して）特定のアドレス ファミリについて追加パスの送信または受信を設定している場合に、ネイバーでその機能を無効にするには、**neighbor additional-paths disable** コマンドを使用します。追加パスの無効化は、機能がテンプレートから継承された場合にも適用されます。

ネイバーの追加パス機能を無効にするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **bgp additional-paths** {**send** [**receive**] | **receive**}
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **additional-paths disable**
7. **end**

手順の詳細

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

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6 unicast`	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	**bgp additional-paths** {**send** [**receive**] | **receive**} 例： `Device(config-router-af)# bgp additional-paths send receive`	該当のアドレス ファミリのネイバーに対して BGP 追加パスを送信または受信できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **additional-paths disable** 例： `Device(config-router-af)# neighbor 2001:DB8::1 additional-paths disable`	指定したネイバーとの間における BGP 追加パスの送信または受信を無効にします。 • 追加パス機能は、アドレス ファミリ内の他のネイバーでは引き続き有効になります。
ステップ 7	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

BGP 追加パスの設定例

例：BGP 追加パスの送受信機能

この例では、R1 のアドレスは 192.168.1.1 です。そのネイバーは、アドレスが 192.168.1.2 である R2 です。R2 から R1 に additional-paths を含む更新が送信されます（すべてのパスがアドバタイズされます）。R2 が追加パスの送信のみ可能で追加パスを受信しないため、更新はアドバタイズされる標準の BGP ベストパスのみ R1 から R2 に送信されます。

R1

```
router bgp 1
 address-family ipv4 unicast
 bgp additional-paths select all
 neighbor 192.168.1.2 additional-paths send receive
 neighbor 192.168.1.2 advertise additional-paths all
```

R2

```
router bgp 2
 address-family ipv4 unicast
 bgp additional-paths select all
 neighbor 192.168.1.1 additional-paths send
 neighbor 192.168.1.1 advertise additional-paths all
```

例：BGP 追加パス

次の例では、すべてのアドレスファミリについて、ルートをローカルデバイスに送信している eBGP ネイバーが 1 つ以上あります（設定には示されていません）。これらのネイバーから学習した eBGP ルートは、下の設定に示されているネイバーにアドバタイズされ、パス属性が変更されます。この例の設定は、次のとおりです。

- add_path1 というルートマップでは、すべてのパスをネイバー 192.168.101.15 にアドバタイズするが、**best 2** でマークされているパスについては、ネイバーに送信する前にそのメトリックを 780 に設定するように指定しています。
- add_path2 というルートマップでは、**best 3** でマークされているパスについては、そのメトリックを 640 に設定してからネイバー 192.168.25 にアドバタイズするように指定しています。
- add_path3 というルートマップでは、**group-best** でマークされているパスについては、そのメトリックを 825 に設定してからネイバー 2001:DB8::1045 にアドバタイズするように指定しています。
- IPv6 マルチキャストアドレスファミリでは、すべてのパスがアドバタイズの候補となり、ネイバー 2001:DB8::1037 にアドバタイズされます。

```
router bgp 1
 neighbor 192.168.101.15 remote-as 1
 neighbor 192.168.101.25 remote-as 1
 neighbor 2001:DB8::1045 remote-as 1
 neighbor 2001:DB8::1037 remote-as 1
!
 address-family ipv4 unicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.15 activate
  neighbor 192.168.101.15 route-map add_path1 out
  neighbor 192.168.101.15 advertise additional-paths best 2
 exit-address-family
!
address-family ipv4 multicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.25 activate
  neighbor 192.168.101.25 route-map add_path2 out
  neighbor 192.168.101.25 advertise additional-paths best 3
 exit-address-family
!
 address-family ipv6 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1045 activate
  neighbor 2001:DB8::1045 route-map add_path3 out
  neighbor 2001:DB8::1045 advertise additional-paths all group-best
 exit-address-family
!
 address-family ipv6 multicast
  bgp additional-paths send receive
  bgp additional-paths select all
  neighbor 2001:DB8::1037 activate
  neighbor 2001:DB8::1037 route-map add_path4 out
  neighbor 2001:DB8::1037 advertise additional-paths all
 exit-address-family
!
route-map add_path1 permit 10
 match additional-paths advertise-set best 2
 set metric 780
route-map add_path1 permit 20
!
route-map add_path2 permit 10
 match additional-paths advertise-set best 3
 set metric 640
!
route-map add_path3 permit 10
 match additional-paths advertise-set group-best
 set metric 825
!
```

例：ネイバー機能によるアドレス ファミリ機能のオーバーライド

次の例では、ネイバーの受信専用機能が、アドレス ファミリの送受信機能をオーバーライドします。

```
router bgp 65000
```

```
 address-family ipv6 multicast
 bgp additional-paths send receive
 bgp additional-paths select group-best
 neighbor 2001:DB8::1037 activate
 neighbor 2001:DB8::1037 additional-paths receive
 neighbor 2001:DB8::1037 advertise additional-paths group-best
!
```

例：ピア ポリシー テンプレートを使用する BGP 追加パス

```
router bgp 45000
address-family ipv4 unicast
 bgp additional-paths send receive
 bgp additional-paths select all group-best best 3
 template peer-policy rr-client-pt1
  additional-paths send receive
  advertise additional-paths group-best best 3
  exit
 address-family ipv4 unicast
  neighbor 192.168.1.1 remote-as 45000
  neighbor 192.168.1.1 inherit peer-policy rr-client-pt1
  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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 4271	『*A Border Gateway Protocl (BGP-4)*』
RFC 4760	『*Multiprotocol Extensions for BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 追加パスの機能情報

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 *86 : BGP* 追加パスの機能情報

機能名	リリース	機能情報
BGP の追加パス		BGP 追加パスは、暗黙的に以前のパスから新しいパスに代わることなく、同じプレフィックスのマルチパスをアドバタイズする機能を備えています。 次のコマンドが導入されました。 • **additional-paths** • **advertise additional-paths** • **bgp additional-paths** • **bgp additional-paths select** • **match additional-paths advertise-set** • **neighbor additional-paths** • **neighbor advertise additional-paths** 次のコマンドが変更されました。 • **show ip bgp** • **show ip bgp neighbors**

第 67 章

BGP-複数のクラスタ ID

BGP—複数のクラスタ ID機能により、iBGP ネイバー（通常はルート リフレクタ）は複数のクラスタ ID（グローバル クラスタ ID と、クライアント（ネイバー）に割り当てられる追加クラスタ ID）を持つことができます。この機能が導入される前は、デバイスは単一のグローバル クラスタ ID を持つことができました。

ネットワーク管理者がネイバーごとのクラスタ ID を設定すると、次のようになります。

- CLUSTER_LIST に基づくループ防止メカニズムが、複数のクラスタ ID を考慮するように自動的に変更されます。
- クラスタ ID に基づいてクライアント間のルート リフレクションを無効にすることができます。

- 機能情報の確認 （1119 ページ）
- BGP-複数のクラスタ ID に関する情報 （1120 ページ）
- BGP-複数のクラスタ ID の使用方法 （1123 ページ）
- BGP-複数のクラスタ ID の設定例 （1129 ページ）
- その他の参考資料 （1130 ページ）
- BGP-複数のクラスタ ID の機能情報 （1131 ページ）

機能情報の確認

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

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

BGP-複数のクラスタ ID に関する情報

ルート リフレクタごとの複数クラスタ ID の利点

BGP—複数のクラスタ ID 機能により、ルート リフレクタ（RR）は複数のクラスタに属して複数のクラスタ ID を持つことができます。RR は、グローバル単位とネイバー単位で設定されたクラスタ ID を持つことができます。単一のクラスタ ID を 2 つ以上の iBGP ネイバーに割り当てることができます。この機能が導入される前は、RR では、 **bgp cluster-id** ルータ コンフィギュレーション コマンドで設定された単一のグローバル クラスタ ID を使用していました。

クラスタ ID を（**neighbor cluster-id** ルータ コンフィギュレーション コマンドで）ネイバーごとに設定すると、次の 2 つの変更が行われます。

- CLUSTER_LIST 属性に基づくループ防止メカニズムが、複数のクラスタ ID を考慮するように自動的に変更されます。
- ネットワーク管理者は、クラスタ ID に基づいてクライアント間のルート リフレクションを無効にすることができます。これにより、ネットワーク設計の変更が可能になります。

ループ防止メカニズムおよび CLUSTER_LIST 伝播ルールについては、「CLUSTER_LIST 属性の使用方法」の項を参照してください。クライアント間のリフレクションの無効化については、「クライアント間のルート リフレクションを無効にした場合の動作」の項を参照してください。

CLUSTER_LIST 属性の使用方法

CLUSTER_LIST 伝播ルールは、リリースによって異なり、デバイスが実行しているシスコ ソフトウェア リリースが BGP—複数のクラスタ ID 機能の実装前に生成されたか実装後に生成されたかによって決まります。CLUSTER_LIST に基づくループ防止についても同様です。

CLUSTER_LIST の動作については、以下で説明します。Classic は、複数クラスタ ID 機能の実装前にリリースされたソフトウェアの動作を指します。MCID は、複数クラスタ ID 機能の実装後にリリースされたソフトウェアの動作を指します。

CLUSTER_LIST 伝播ルール

- Classic：ルートを反映する前に、RR はグローバル クラスタ ID を CLUSTER_LIST に追加します。受信したルートに CLUSTER_LIST 属性がない場合、RR はそのグローバル クラスタ ID を持つ新しい CLUSTER_LIST 属性を作成します。
- MCID：ルートを反映する前に、RR はルートの送信元であるネイバーのクラスタ ID を CLUSTER_LIST に追加します。受信したルートに CLUSTER_LIST 属性がない場合、RR はそのクラスタ ID を持つ新しい CLUSTER_LIST 属性を作成します。この動作には、スピーカーのクライアントではないネイバーが含まれます。ルートの送信元である非クライアント ネイバーにクラスタ ID が関連付けられていない場合、RR はグローバル クラスタ ID を使用します。

CLUSTER_LIST に基づくループ防止

- Classic：ルートを受信すると、RR は、RR のグローバル クラスタ ID がルートの CLUSTER_LIST に含まれている場合にはそのルートを破棄します。
- MCID：ルートを受信すると、RR は、RR のグローバル クラスタ ID またはいずれかの iBGP ネイバーに割り当てられているクラスタ ID がルートの CLUSTER_LIST に含まれている場合にはそのルートを破棄します。

クライアント間のルート リフレクションを無効にした場合の動作

iBGP ネイバーごとの複数クラスタ ID の導入により、クラスタ ID に基づいてクライアント間のルート リフレクションを無効化できるようになりました。ルート リフレクションを無効にすると、ネットワーク設計の変更が可能になります。ルート リフレクションを無効にした後の一般的なシナリオ（別のシナリオもあり得る）では、クライアントが完全にメッシュ化されているため、クライアントから送信する必要があるアップデートは多くなり、クライアント間のリフレクションが無効になっているため、RR から送信する必要があるアップデートは少なくなります。

次に示すようなシナリオでは、ルート リフレクションの無効化が必要になる場合があります。RR には、セッションが確立されているクライアント（プロバイダー エッジ（PE）ルータ）が複数あるとします。1 つのクラスタに属する iBGP ネイバーには、同じクラスタ ID が割り当てられています。

同じクラスタに属する PE は完全にメッシュ化されているため（PE1 と PE2 はそれらの間でセッションを確立しており、PE3 と PE4 もそれらの間でセッションを確立しています）、それらの PE 間でルートを反映する必要はありません。つまり、PE1 からのルートは、PE3 および PE4 に転送する必要がありますが、PE2 に転送する必要はありません。

重要なポイントは、特定のクラスタ ID についてリフレクション状態がソフトウェアによって変更されると、BGP はアウトバウンド ソフト リフレッシュをすべてのクライアントに送信するということです。

クライアント間のルート リフレクションを無効にする方法とその結果はさまざまで、デバイスが実行しているシスコ ソフトウェアが複数クラスタ ID 機能の実装前に生成されたか実装後に生成されたかによって決まります。Classic は、複数クラスタ ID 機能の実装前にリリースされたソフトウェアの動作を指します。MCID は、複数クラスタ ID 機能の実装後にリリースされたソフトウェアの動作を指します。

- Classic：クライアントからルートを受信しても、RR は他のクライアントには反映しません。リフレクションのその他のシナリオ（クライアントから非クライアント、非クライアントからクライアント）は維持されます。クライアント間のルート リフレクションの無効化は、通常、すべてのクライアントが完全にメッシュ化されている場合（ルートは、そのメッシュを介してクライアント間でアドバタイズされるため、リフレクションの必要はありません）に行います。クライアント間のルート リフレクションを無効にするコマンドは、ルータ コンフィギュレーション モードで入力し（ **router bgp** コマンドの後）、すべてのアドレス ファミリにグローバルに適用されます。**no bgp client-to-client reflection**

- MCID：クライアントからルートを受信しても、RRは、クライアント間のリフレクションが無効になっているクラスタに両方のクライアントが属している場合には、もう一方のクライアントには反映しません。つまり、ルートリフレクションは、クラスタ内（指定されたクラスタ内）のみで無効になります。リフレクションのその他のケース（クライアントから非クライアント、非クライアントからクライアント、クラスタ間）は維持されます。この機能は、通常、特定のクラスタのすべてのクライアントがそれらの間（他のクラスタのクライアントは含まない）で完全にメッシュ化されている場合に設定されます。特定のクラスタでクライアント間のルート リフレクションを無効にするコマンドは、ルータ コンフィギュレーション モードで入力し、すべてのアドレス ファミリにグローバルに適用されます。

  no bgp client-to-client reflection intra-cluster cluster-id {any | *cluster-id1 cluster-id2...*}

  any キーワードは、どのクラスタでもクライアント間のリフレクションを無効にするために使用します。

  以前にリリースされたコマンドClassic（すべてのクライアント間のリフレクションを無効にする）も、この MCID 導入後のリリース タイムフレームでも使用できます。

  no bgp client-to-client reflection [all]

  （オプションの **all** キーワードは、コマンドの肯定形式にも否定形式にも影響を及ぼすことはなく、コンフィギュレーションファイルにも表示されません。このキーワードは、単にクラスタ間とクラスタ内の両方でクライアント間のリフレクションが有効または無効になっていることをネットワーク管理者に明示するために用意されています。）

  要約すると、複数クラスタ ID 機能の導入後は、3 つの設定レベルで、クライアント間のリフレクションを無効にすることができるということです。この無効化は、最も固有性の低いものから最も固有性の高いものまで、次の順序で実行されます。

  1. 最も低い固有性：**no bgp client-to-client reflection [all]** クラスタ内とクラスタ間のクライアント間リフレクションを無効にします。
  2. より高い固有性：**no bgp client-to-client reflection intra-cluster cluster-id any** あらゆるクラスタ ID についてクラスタ内のクライアント間リフレクションを無効にします。
  3. 最も高い固有性：**no bgp client-to-client reflection intra-cluster cluster-id** *cluster-id1 cluster-id2 ...* 指定したクラスタについてクラスタ内のクライアント間リフレクションを無効にします。

  BGPがアップデートをアドバタイズする際、各設定レベルが順に評価されます。いずれかの設定レベルでクライアント間のリフレクションが無効化されている場合は、より固有性の高いポリシーをさらに評価する必要はありません。

  上記の3つのコマンドの基本（肯定）形式と否定（**no**）形式の結果に注意してください。

  - 否定設定（**no** キーワードあり）は、より固有性の低いすべての設定を上書きします。
  - 肯定設定（**no** キーワードなし）は、より固有性の低い設定によって（デフォルトで）置き換えられます。

- どのレベルの設定も、否定形式の場合にのみコンフィギュレーションファイルに表示されます。

すべてのレベルは個別に設定でき、すべてのレベルは他のレベルの設定とは独立してコンフィギュレーション ファイルに表示されます。

否定設定を使用すると、より固有性の高い設定はすべて不要になります（より固有性の高い設定が肯定の場合は、否定設定の後には処理されず、より固有性の高い設定が否定の場合は、前の否定設定と機能的に同じであるため）。以下の各例で、この動作を示します。

例 1

no bgp client-to-client reflection

no bgp client-to-client reflection intra-cluster cluster-id any

クラスタ間とクラスタ内のリフレクションは無効になります（最初のコマンドに基づきます）。2 番目のコマンドは、クラスタ内のリフレクションを無効にしますが、クラスタ内のリフレクションは最初のコマンドですでに無効になっているため不要です。

例 2

no bgp client-to-client reflection intra-cluster cluster-id any

bgp client-to-client reflection intra-cluster cluster-id 1.1.1.1

最初のコマンドを使用してアップデートが評価されるため、クラスタ ID 1.1.1.1 ではクラスタ内のルートリフレクションは無効になります（2番目のコマンドが肯定の場合でも）。最初のコマンドが否定であり、いずれかの設定レベルでクライアント間のリフレクションが無効化されると、それ以上評価は実行されません。

この例で注目すべきもう 1 つの点は、2 番目のコマンドです。2 番目のコマンドは肯定形式であるため、デフォルトで最初のコマンドの動作（より固有性の低い設定）になります。したがって、この 2 番目のコマンドは不要です。

また、2番目のコマンドは、否定のコマンドではないため、コンフィギュレーションファイルには表示されません。

BGP-複数のクラスタ ID の使用方法

ネイバーごとのクラスタ ID の設定

ネイバーごとにクラスタ ID を設定するには、iBGP ピア（通常はルート リフレクタ）でこの作業を実行します。ネイバーごとにクラスタ ID を設定すると、CLUSTER_LIST に基づくループ防止メカニズムが複数のクラスタ ID を考慮するように自動的に変更されます。また、クラスタ ID に基づいてクライアント間のルート リフレクションを無効化できるようになります。別のコマンドを使用してルートリフレクションを無効にすることができるように、ネイバーにタグが付けられます（クライアント間のリフレクションの無効化については、このモジュールで後述する各作業を参照してください）。

（注） ネイバーのクラスタ ID を変更すると、BGP により、すべての iBGP ピアについてインバウンド ソフト リフレッシュとアウトバウンド ソフト リフレッシュが自動的に実行されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address*} **remote-as** *autonomous-system-number*
5. **neighbor** {*ip-address* | *ipv6-address*} **cluster-id** *cluster-id*
6. **end**
7. **show ip bgp cluster-ids**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*} **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.2 remote-as 65000`	エントリを BGP ルーティング テーブルに追加します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*} **cluster-id** *cluster-id* 例： `Device(config-router)# neighbor 192.168.1.2 cluster-id 0.0.0.1`	指定されたネイバーにクラスタ ID を割り当てます。 • クラスタ ID は、ドット付き 10 進法形式（192.168.7.4 など）または 10 進法形式（23 など）で、最大 4 バイトまで指定できます。 • 10 進法形式（23 など）で設定されたクラスタ ID は、コンフィギュレーション ファイルに表示される際にはドット付き 10 進法形式（0.0.0.23 など）に変更されます。 • ネイバーのクラスタ ID を変更すると、BGP により、すべての iBGP ピアについてインバウンド ソフト リフレッシュとアウトバウンド ソフト リフレッシュが自動的に実行されます。
ステップ 6	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp cluster-ids** 例： `Device# show ip bgp cluster-ids`	（任意）以下をリストします。 • グローバル クラスタ ID（設定の有無を問わない） • ネイバーに設定されているすべてのクラスタ ID • ネットワーク管理者がリフレクションを無効にしているすべてのクラスタ ID

クラスタ内とクラスタ間のクライアント間リフレクションの無効化

クラスタ内とクラスタ間の両方でクライアント間のリフレクションを無効にする場合は、ルートリフレクタで次の作業を実行します。これは、クライアント間のリフレクションを無効にする最も広範な（最も固有性の低い）方法です。アップデートをアドバタイズする前に、各設定レベルが、最も固有性の低いものから最も固有性の高いものまで順に評価されます。いずれかの設定レベルでクライアント間のリフレクションが無効化されている場合は、より固有性の高いポリシーをさらに評価する必要はありません。

（注） 特定のクラスタ ID についてリフレクション状態がソフトウェアによって変更されると、BGP はアウトバウンド ソフト リフレッシュをすべてのクライアントに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp client-to-client reflection** [**all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**no bgp client-to-client reflection** [**all**] 例： `Device(config-router)# no bgp client-to-client reflection all`	クラスタ内とクラスタ間のクライアント間リフレクションを無効にします。 • **all** キーワードは、単に **bgp client-to-client reflection** コマンドがクラスタ内とクラスタ間の両方のリフレクションに作用することを明示するために用意されています。**all** キーワードは、コマンドの肯定形式にも否定形式にも影響を及ぼすことはありません。

すべてのクラスタ ID のクラスタ内におけるクライアント間リフレクションの無効化

あらゆるクラスタ ID についてクラスタ内のクライアント間リフレクションを無効にするには、ルート リフレクタで次の作業を実行します。これは、クライアント間のリフレクションを無効

にするために使用できる3つのレベルのコマンドのうち、中間レベルに該当します。つまり、クラスタ内とクラスタ間のクライアント間リフレクションを無効にするよりも固有性は高く、特定のクラスタ ID についてクラスタ内のクライアント間リフレクションを無効にするよりも固有性は低くなります。

アップデートをアドバタイズする前に、各設定レベルが、最も固有性の低いものから最も固有性の高いものまで順に評価されます。いずれかの設定レベルでクライアント間のリフレクションが無効化されている場合は、より固有性の高いポリシーをさらに評価する必要はありません。

（注） 特定のクラスタ ID についてリフレクション状態がソフトウェアによって変更されると、BGP はアウトバウンド ソフト リフレッシュをすべてのクライアントに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp client-to-client reflection intra-cluster cluster-id any**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 4	**no bgp client-to-client reflection intra-cluster cluster-id any** 例： `Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id any`	あらゆるクラスタについてクラスタ内のクライアント間ルート リフレクションを無効にします。

指定したクラスタ ID のクラスタ内におけるクライアント間リフレクションの無効化

指定したクラスタ ID についてクラスタ内のクライアント間リフレクションを無効にするには、ルート リフレクタで次の作業を実行します。これは、クライアント間のリフレクションを無効にするために使用できる 3 つのレベルのコマンドのうち、最も固有性が高いレベルに該当します。アップデートをアドバタイズする前に、各設定レベルが、最も固有性の低いものから最も固有性の高いものまで順に評価されます。いずれかの設定レベルでクライアント間のリフレクションが無効化されている場合は、より固有性の高いポリシーをさらに評価する必要はありません。

（注） 特定のクラスタ ID についてリフレクション状態がソフトウェアによって変更されると、BGP はアウトバウンド ソフト リフレッシュをすべてのクライアントに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp client-to-client reflection intra-cluster cluster-id** *cluster-id1* [*cluster-id2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**no bgp client-to-client reflection intra-cluster cluster-id** *cluster-id1* [*cluster-id2...*] 例： `Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.1 0.0.0.3 105`	指定した各クラスタ内でクライアント間のルート リフレクションを無効にします。 • コンフィギュレーション ファイルでは、10 進法のクラスタ ID 番号はドット付き 10 進法形式で表示されるため、この例のコマンドは「no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.1 0.0.0.3 0.0.0.105」と表示されることに注意してください。

BGP-複数のクラスタ ID の設定例

例：ネイバーごとのクラスタ ID

次の例は、ルート リフレクタでの設定です。IPv6 アドレス 2001:DB8:1::1 のネイバー（クライアント）が、0.0.0.6 のクラスタ ID を持つように設定されています。

```
router bgp 6500
 neighbor 2001:DB8:1::1 cluster-id 0.0.0.6
```

例：クライアント間リフレクションの無効化

次の例では、すべてのクラスタ内とクラスタ間でクライアント間のリフレクションを無効にしています。

```
router bgp 65000
 no bgp client-to-client reflection all
```

次の例では、すべてのクラスタ IDについてクラスタ内のクライアント間リフレクションを無効にしています。

```
router bgp 65000
 no bgp client-to-client reflection intra-cluster cluster-id any
```

次の例では、指定したクラスタ ID（0.0.0.1、14、15、0.0.0.6）についてクラスタ内のクライアント間リフレクションを無効にしています。

```
router bgp 65000
 no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.1 14 15 0.0.0.6
```

neighbor cluster-id コマンドで 10 進法形式（23 など）で指定したクラスタ ID は、コンフィギュレーション ファイルではドット付き 10 進法形式（0.0.0.23 など）で表示されることに注意してください。10 進法形式はコンフィギュレーション ファイルには表示されません。実行コンフィギュレーションは次のようになります。

```
router bgp 65000
no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.1
no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.6
no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.14
no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.15
```

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』
BGP コマンド	『Cisco IOS IP Routing: BGP 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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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-複数のクラスタ ID の機能情報

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

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

表 *87 : BGP*—複数のクラスタ *ID* の機能情報

機能名	リリース	機能情報
BGP：複数のクラスタ ID		

機能名	リリース	機能情報
		BGP—複数のクラスタ ID 機能により、iBGP ネイバー（通常はルート リフレクタ）は複数のクラスタ ID（グローバル クラスタ ID と、クライアント（ネイバー）に割り当てられる追加クラスタ ID）を持つことができます。この機能が導入される前は、デバイスは単一のグローバル クラスタ ID を持つことができました。 ネットワーク管理者がネイバーごとのクラスタ ID を設定すると、次のようになります。 • CLUSTER_LIST に基づくループ防止メカニズムが、複数のクラスタ ID を考慮するように自動的に変更されます。 • クラスタ ID に基づいてクライアント間のルート リフレクションを無効にすることができます。 次のコマンドが導入されました。 • **bgp client-to-client reflection intra-cluster** • **neighbor cluster-id** • **show ip bgp cluster-ids** 次のコマンドが変更されました。 • **bgp client-to-client reflection** • **show ip bgp neighbors** • **show ip bgp template peer-session** • **show ip bgp update-group**

第 68 章

BGP-VPN 識別子属性

BGP—VPN識別子属性機能により、ネットワーク管理者は、宛先自律システム内の自律システム境界ルータ（ASBR）から送信元ルートターゲット（RT）をプライベートに保つことができます。出力 ASBR の RT が VPN 識別子にマッピングされ、VPN 識別子が eBGP を介して伝送されて、入力 ASBR の RT にマッピングされます。

- 機能情報の確認 （1135 ページ）
- BGP-VPN 識別子属性に関する情報 （1136 ページ）
- BGP-VPN 識別子属性の設定方法 （1138 ページ）
- BGP-VPN 識別子属性の設定例 （1144 ページ）
- その他の参考資料 （1145 ページ）
- BGP-VPN 識別子属性の機能情報 （1146 ページ）

機能情報の確認

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

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

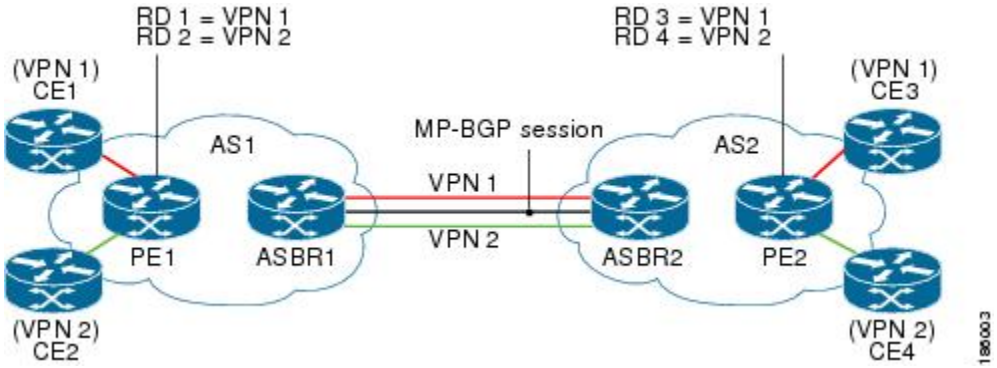
BGP-VPN 識別子属性に関する情報

VPN 識別子属性の役割と利点

route-target（RT）拡張コミュニティ属性は、ルートの VPN メンバーシップを識別します。RT 属性は、エクスポート側（出力）プロバイダー エッジ ルータ（PE）でルートに配置され、iBGP クラウド全体およびすべての自律システムに転送されます。このようなルートをインポートする必要があるリモート PE の Virtual Routing and Forwarding（VRF）インスタンスでは、対応する RT がその VRF のインポート RT として設定されている必要があります。

下の図には、異なる VPN に属するカスタマー エッジ（CE）ルータを含む 2 つの自律システムが示されています。各 PE は、どのルート識別子（RD）がどの VPN に対応するかを追跡して、各 VPN に属するトラフィックを制御します。

図 *88*：自律システム間で *ASBR* が *RT* を変換するシナリオ



上の図に示されているような Inter-AS オプション B のシナリオでは、これらのルートは、MP-eBGP セッションを介して自律システム境界ルータ 1（ASBR1）から AS 境界を越えて ASBR2 に伝送され、ルートの各 RT は拡張コミュニティ属性として ASBR2 によって受信されます。

ASBR2 では、CE3 および CE4 に対する PE2 上の各 VPN メンバーシップの CE 接続で RT をインポートできるように、AS1 によって生成された RT を AS2 で認識できる RT に変換するための複雑な RT マッピング スキームを維持する必要があります。

ネットワーク管理者によっては、AS1 の送信元 RT を AS2 内のデバイスからは認識できないようにすることを必要とする場合があります。それには、各 VPN に属するルートを特定の属性によって区別する必要があります。これにより、ASBR2 にルートを送信する前に ASBR1 の発信側で RT を削除できるようになり、ASBR2 でその属性を AS2 の認識可能な RT にマッピングできるようになります。VPN 識別子（VD）拡張コミュニティ属性はこの目的に役立ちます。

BGP—VPN 識別子属性機能の利点は、送信元 RT を宛先自律システムのデバイスからプライベートに保てることです。

VPN 識別子属性の仕組み

ネットワーク管理者は、VPN 識別子拡張コミュニティ属性への RT の変換を実行するように出力 ASBR を設定し、RT への VPN 識別子の変換を実行するように入力 ASBR を設定します。より具体的には、この変換は次のように実現されます。

出力 ASBR 側

- 発信ルート マップで、ルートの RT 値に基づいてどの VPN ルートがマッピング対象となるかを判別する **match excommunity** 句を指定します。
- **set extcommunity vpn-distinguisher** コマンドで、RT を置き換える VPN 識別子を設定します。
- RT を削除するように、同じ RT セットを参照する **set extcomm-list delete** コマンドを設定します。その後、隣接する入力 ASBR にルートが送信されます。

入力 ARBR 側

- 着信ルート マップで、ルートの VPN 識別子に基づいてどの VPN ルートがマッピング対象となるかを判別する **match excommunity vpn-distinguisher** コマンドを指定します。
- **set extcommunity rt** コマンドで、VPN 識別子を置き換える RT を指定します。
- この句に一致するルートでは、VPN 識別子は設定した RT に置き換えられます。

VPN 識別子に関連するその他の動作

出力 ASBR で、**set extcommunity vpn-distinguisher** コマンドが設定されていないルート マップ句に VPN ルートが一致した場合、VPN ルートにタグ付けされている RT は保持されます。

VPN 識別子は AS 境界を越えて移動しますが、iBGP クラウド内では伝送されません。つまり、入力 ASBR は eBGP ピアから VPN 識別子を受信できますが、VPN 識別子は対応する RT にマッピングされた後に着信側で破棄されます。

入力 ASBR で、VPN 識別子を伝送する VPN ルートが、着信ルート マップの **set extcommunity rt** コマンドが設定されていないルート マップ句と一致した場合、その属性は、破棄されることも、iBGP クラウド内で伝播されることもありません。ルートの VPN 識別子は保持されるため、ネットワーク管理者は、VPN ルートで伝送する必要がある RT に VPN 識別子を変換するための適切な着信ポリシーを設定できます。ルートが eBGP ピアに送信される場合、VPN 識別子はそのまま伝送されます。ネットワーク管理者は、eBGP ピアに送信されるルートから VPN 識別子を削除するようにルートマップ エントリを設定できます。

発信ルート マップで **set extcommunity vpn-distinguisher** コマンドを設定すると、または着信ルート マップで **match excommunity** コマンドを設定すると、送受信されるルートを更新するために、それぞれ発信または着信ルート リフレッシュ リクエストが生成されます。

BGP-VPN 識別子属性の設定方法

RT を VPN 識別子属性に置き換える

ルート ターゲット（RT）を VPN 識別子拡張コミュニティ属性に置き換えるには、出力 ASBR でこの作業を実行します。必ず、入力 ASBR で VPN 識別子をルート ターゲットに置き換えてください。この作業については、「VPN 識別子属性を RT に置き換える」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *value*
4. **exit**
5. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
6. **match extcommunity** *extended-community-list-name*
7. **set extcomm-list** *extcommunity-name* **delete**
8. **set extcommunity vpn-distinguisher** *id*
9. **exit**
10. **route-map** *map-name* {**permit** | **deny**} [*sequence-number*]
11. **exit**
12. **router bgp** *as-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **address-family vpnv4**
15. **neighbor** *ip-address* **activate**
16. **neighbor** *ip-address* **route-map** *map-name* **out**
17. **exit-address-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *value* 例： `Device(config)# ip extcommunity-list 4 permit rt 101:100`	IP 拡張コミュニティ リストを設定して、指定した RT を持つルートが拡張コミュニティ リストに含まれるように、バーチャル プライベート ネットワーク（VPN）ルート フィルタリングを設定します。 • この例では、RT 101:100 を持つルートを拡張コミュニティ リスト 4 に対して許可しています。
ステップ 4	**exit** 例： `Device(config-extcomm-list)# exit`	コンフィギュレーション モードを終了し、次に高い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	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map vpn-id-map1 permit 10`	後続の **match** コマンドで一致と認められたルートを許可または拒否するルートマップを設定します。 • この例では、後続の **match** コマンドで一致と認められたルートを許可します。
ステップ 6	**match extcommunity** *extended-community-list-name* 例： `Device(config-route-map)# match extcommunity 4`	指定したコミュニティ リストを照合します。 • この例では、拡張コミュニティ リスト 4（手順 3 で設定）に一致するルートが後続の **set** コマンドの対象となります。
ステップ 7	**set extcomm-list** *extcommunity-name* **delete** 例： `Device(config-route-map)# set extcomm-list 4 delete`	指定した拡張コミュニティ リスト内のルートから RT を削除します。 • この例では、拡張コミュニティ リスト 4 内のルートから RT が削除されます。
ステップ 8	**set extcommunity vpn-distinguisher** *id* 例： `Device(config-route-map)# set extcommunity vpn-distinguisher 111:100`	ルート マップで許可されているルートに対して、指定した VPN 識別子を設定します。 • この例では、拡張コミュニティ 4 に一致するルートに VPN 識別子 111:100 を設定します。
ステップ 9	**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、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 10	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] 例：	（任意）ルートを許可するルート マップ エントリを設定します。

	コマンドまたはアクション	目的
	`Device(config)# route-map vpn-id-map1 permit 20`	• この例では、RT から VPN 識別子へのマッピングの対象とならない他のルートを許可するルート マップ エントリを設定します。この手順を実行しない場合、他のすべてのルートは暗黙の deny の対象となります。
ステップ 11	**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、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 12	**router bgp** *as-number* 例： `Device(config)# router bgp 2000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.101.1 remote-as 2000`	自律システムに属するネイバーを指定します。
ステップ 14	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.101.1 activate`	指定したネイバーをアクティブにします。
ステップ 16	**neighbor** *ip-address* **route-map** *map-name* **out** 例： `Device(config-router-af)# neighbor 192.168.101.1 route-map vpn-id-map1 out`	指定した発信ルート マップを、指定したネイバーに適用します。
ステップ 17	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

VPN 識別子属性を RT に置き換える

VPN 識別子拡張コミュニティ属性をルート ターゲット（RT）属性に置き換えるには、入力 ASBR でこの作業を実行します。この作業では、RT を VPN 識別子に置き換えるように出力 ASBR を設定済みであることを前提としています。この作業については、「RT を VPN 識別子属性に置き換える」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** *expanded-list* {**permit** | **deny**} **vpn-distinguisher** *id*
4. **exit**
5. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
6. **match extcommunity** *extended-community-list-name*
7. **set extcomm-list** *extcommunity-name* **delete**
8. **set extcommunity rt** *value* **additive**
9. **exit**
10. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
11. **exit**
12. **router bgp** *as-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **address-family vpnv4**
15. **neighbor** *ip-address* **activate**
16. **neighbor** *ip-address* **route-map** *map-name* **in**
17. **exit-address-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 extcommunity-list** *expanded-list* {**permit**	**deny**} **vpn-distinguisher** *id* 例： `Device(config)# ip extcommunity-list 51 permit vpn-distinguisher 111:100`	IP 拡張コミュニティ リストを設定して、指定した VPN 識別子を持つルートが拡張コミュニティ リストに含まれるように、バーチャルプライベートネットワーク（VPN）ルート フィルタリングを設定します。

	コマンドまたはアクション	目的
		• この例では、VPN 識別子 111:110 を持つルートを拡張コミュニティ リスト 51 に対して許可しています。
ステップ 4	**exit** 例： `Device(config-extcomm-list)# exit`	コンフィギュレーション モードを終了し、次に高い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	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map vpn-id-rewrite-map1 permit 10`	後続の **match** コマンドで一致と認められたルートを許可または拒否するルートマップを設定します。 • この例では、後続の **match** コマンドで一致と認められたルートを許可します。
ステップ 6	**match extcommunity** *extended-community-list-name* 例： `Device(config-route-map)# match extcommunity 51`	指定したコミュニティ リストを照合します。 • この例では、拡張コミュニティ リスト 51（手順 3 で設定）に一致するルートが後続の **set** コマンドの対象となります。
ステップ 7	**set extcomm-list** *extcommunity-name* **delete** 例： `Device(config-route-map)# set extcomm-list 51 delete`	指定した拡張コミュニティ リスト内のルートから VPN 識別子を削除します。 • この例では、拡張コミュニティ リスト 51 内のルートから VPN 識別子が削除されます。
ステップ 8	**set extcommunity rt** *value* **additive** 例： `Device(config-route-map)# set extcommunity rt 101:1 additive`	ルート マップで許可されているルートに、指定した RT を設定します。 • この例では、拡張コミュニティ 51 に一致するルートに RT 101:1 を設定します。**additive** キーワードを指定すると、RT を置き換えずに RT が RT リストに追加されます。
ステップ 9	**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、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 10	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map vpn-id-rewrite-map1 permit 20`	（任意）ルートを許可するルート マップ エントリを設定します。 • この例では、VPN 識別子から RT へのマッピングの対象とならない他のルートを許可するルート マップ エントリを設定します。この手

	コマンドまたはアクション	目的
		順を実行しない場合、他のすべてのルートは暗黙の deny の対象となります。
ステップ 11	**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、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 12	**router bgp** *as-number* 例： `Device(config)# router bgp 3000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.0.81 remote-as 3000`	自律システムに属するネイバーを指定します。
ステップ 14	**address-family vpnv4** 例： `Device(config-router-af)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.0.81 activate`	指定したネイバーをアクティブにします。
ステップ 16	**neighbor** *ip-address* **route-map** *map-name* **in** 例： `Device(config-router-af)# neighbor 192.168.0.81 route-map vpn-id-rewrite-map1 in`	指定した発信ルート マップを、指定したネイバーに適用します。
ステップ 17	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

BGP-VPN 識別子属性の設定例

例：RT から VPN 識別子への変換と VPN 識別子 から RT への変換

次の例は、ルート ターゲット（RT）を VPN 識別子に置き換えるための出力 ASBR の設定、および VPN 識別子をルート ターゲットに置き換えるための入力 ASBR の設定を示しています。

出力 ASBR では、VPN ルートをフィルタ処理して RT 101:100 のルートのみを許可するように、IP 拡張コミュニティ リスト 1 を設定します。vpn-id-map1 という名前のルートマップで、IP 拡張コミュニティ リスト 1 によって許可されているルートに一致するすべてのルートが 2 つの **set** コマンドの対象となるように指定します。1 つ目の **set** コマンドは、ルートから RT を削除します。2 つ目の **set** コマンドは、VPN 識別子属性を 111:100 に設定します。

route-map vpn-id-map1 permit 20 コマンドは、RT から VPN 識別子へのマッピングに含まれない他のルートが、破棄されないようルート マップを通過できるようにします。このコマンドを使用しないと、暗黙の deny によってこれらのルートは破棄されます。

最後に、自律システム 2000 で、VPNv4 アドレス ファミリについて、ルート マップ vpn-id-map1 を 192.168.101.1 のネイバーに送出されるルートに適用します。

出力 ASBR

```
ip extcommunity-list 1 permit rt 101:100
!
route-map vpn-id-map1 permit 10
 match extcommunity 1
 set extcomm-list 1 delete
 set extcommunity vpn-distinguisher 111:100
!
route-map vpn-id-map1 permit 20
!
router bgp 2000
 neighbor 192.168.101.1 remote-as 2000
 address-family vpnv4
  neighbor 192.168.101.1 activate
  neighbor 192.168.101.1 route-map vpn-id-map1 out
  exit-address-family
!
```

入力 ASBR では、IP 拡張コミュニティ リスト 51 で、VPN 識別子が 111:100 であるルートを許可します。vpn-id-rewrite-map1 という名前のルート マップで、IP 拡張コミュニティ リスト 51 によって許可されているルートに一致するすべてのルートが 2 つの **set** コマンドの対象となるように指定します。1 つ目の **set** コマンドは、ルートから VPN

識別子を削除します。2 つ目の **set** コマンドは RT を 101:1 に設定し、RT を置き換えずにその RT を RT リストに追加します。

route-map vpn-id-rewrite-map1 permit 20 コマンドは、VPN 識別子から RT へのマッピングに含まれない他のルートが、破棄されないようルート マップを通過できるようにします。このコマンドを使用しないと、暗黙の deny によってこれらのルートは破棄されます。

最後に、自律システム 3000 で、VPNv4 アドレス ファミリについて、vpn-id-rewrite-map1 という名前のルート マップを 192.168.0.81 のネイバーを宛先とする着信ルートに適用します。

入力 ASBR

```
ip extcommunity-list 51 permit vpn-distinguisher 111:100
!
route-map vpn-id-rewrite-map1 permit 10
 match extcommunity 51
 set extcomm-list 51 delete
 set extcommunity rt 101:1 additive
!
route-map vpn-id-rewrite-map1 permit 20
!
router bgp 3000
 neighbor 192.168.0.81 remote-as 3000
 address-family vpnv4
  neighbor 192.168.0.81 activate
  neighbor 192.168.0.81 route-map vpn-id-rewrite-map1 in
  exit-address-family
!
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP 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	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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-VPN 識別子属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレ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 *88 : BGP—VPN* 識別子属性の機能情報

機能名	リリース	機能情報
BGP—VPN 識別子属性		BGP—VPN 識別子属性機能により、ネットワーク管理者は、宛先自律システム内の ASBR から送信元 RT をプライベートに保つことができます。出力 ASBR の RT が VPN 識別子にマッピングされ、VPN 識別子が eBGP を介して伝送されて、入力 ASBR の RT にマッピングされます。 次のコマンドが導入されました。 • **set extcommunity vpn-distinguisher** 次のコマンドが変更されました。 • **show ip bgp vpnv4**

第 69 章

BGP-RT および VPN 識別子属性の書き換えワイルドカード

BGP—RT および VPN 識別子属性の書き換えワイルドカード機能は、マッピングの際にルートターゲット（RT）コミュニティ属性または VPN 識別子コミュニティ属性の範囲を設定できるようにします。出力 ASBR における 1 つ以上の RT を入力 ASBR における別の RT にマッピングすることが必要となる場合があります。VPN 識別子属性機能により、管理者は、eBGP を介して伝送される VPN 識別子に RT をマッピングし、次に入力 ASBR で RT にマッピングすることができます。このマッピングは、拡張コミュニティ属性の RT 範囲または VPN 識別子範囲を指定するルートマップを設定することによって実現されます。個々の RT ではなく範囲を指定することにより、時間が節約され、設定が簡素化されます。また、VPN 識別子範囲では、route-map 句ごとに複数の VPN 識別子属性を使用できるため、この機能が導入される前に適用されていた制約がなくなります。

- 機能情報の確認 （1149 ページ）
- BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する制約事項 （1150 ページ）
- BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する情報 （1150 ページ）
- 範囲を使用してRT を RT にマッピングする方法 （1151 ページ）
- BGP-RT および VPN 識別子属性の書き換えワイルドカードの設定例 （1157 ページ）
- BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する追加情報 （1159 ページ）
- BGP—RT および VPN 識別子属性の書き換えワイルドカードに関する機能情報 （1159 ページ）

機能情報の確認

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

リースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する制約事項

- 範囲（**set extcommunity rt** コマンドまたは **set extcommunity vpn-distinguisher** コマンドで指定）には、最大 450 個の拡張コミュニティを含めることができます。
- VPN 識別子範囲は、iBGP ピアにはリレーされません。

BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する情報

RT および VPN 識別子属性のマッピング範囲の利点

出力 ASBR における 1 つ以上のルート ターゲット（RT）を入力 ASBR における別の RT に書き換える（マッピングする）ことが必要となる場合があります。1 つの使用例は、出力 ASBR の RT を入力 ASBR からプライベートに保つことです。

この書き換えは、着信ルート マップを使用し、route-map 句で着信 RT とプレフィックスを照合して、一致する RT をネイバー AS で認識できる別の RT にマッピングすることによって実現されます。このような書き換えの設定は、着信ルート マップで、数百もの RT を個別に指定（**set extcommunity rt** *value1 value2 value3 ...* のように設定）しなければならない場合もあるため、複雑になることがあります。プレフィックスに対応する RT が連続している場合は、RT の範囲を指定することで設定を簡素化できます。つまり、RT マッピング範囲の利点は、時間の節約と設定の簡素化です。

同様に、VPN 識別子属性への RT のマッピング（およびその逆）も、RT または VPN 識別子の範囲を指定することで簡素化できます。BGP—VPN 識別子属性機能により、ネットワーク管理者は、宛先 AS 内の ASBR から送信元 RT をプライベートに保つことができます。出力 ASBR の RT が VPN 識別子にマッピングされ、VPN 識別子が eBGP を介して伝送されて、入力 ASBR の RT にマッピングされます。

RT および VPN 識別子属性のマッピング範囲機能は、マッピングの際にルート ターゲット（RT）または VPN 識別子の範囲を指定できるようにします。

もう 1 つの利点は、VPN 識別子の設定で得られます。この機能が導入される前は、route-map 句ごとに使用できる **set extcommunity vpn-distinguisher** 値は 1 つだけでした。マッピング範囲の導入により、VPN 識別子の範囲をルートに設定できます。

範囲を使用してRT を RT にマッピングする方法

RT を RT 範囲に置き換える

ルート ターゲット（RT）を RT 範囲に置き換えるには、出力 ASBR でこの作業を実行します。必ず、入力 ASBR で RT の範囲を RT に置き換えてください。この作業については、「RT 範囲を RT に置き換える」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *value*
4. **exit**
5. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
6. **match extcommunity** *extended-community-list-name*
7. **set extcomm-list** *extcommunity-name* **delete**
8. **set extcommunity rt range** *start-value end-value*
9. **exit**
10. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
11. **exit**
12. **router bgp** *as-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **address-family vpnv4**
15. **neighbor** *ip-address* **activate**
16. **neighbor** *ip-address* **route-map** *map-tag* **out**
17. **exit-address-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**ip extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *value* 例： `Device(config)# ip extcommunity-list 22 permit rt 101:100`	IP 拡張コミュニティ リストを設定して、指定した RT を持つルートが拡張コミュニティ リストに含まれるように、バーチャル プライベート ネットワーク（VPN）ルート フィルタリングを設定します。 • この例では、RT 101:100 を持つルートを拡張コミュニティ リスト 22 に対して許可しています。
ステップ 4	**exit** 例： `Device(config-extcomm-list)# exit`	コンフィギュレーション モードを終了し、次に高い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	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map rt-mapping permit 10`	後続の **match** コマンドで一致と認められたルートを許可または拒否するルートマップを設定します。 • この例では、後続の **match** コマンドで一致と認められたルートを許可します。
ステップ 6	**match extcommunity** *extended-community-list-name* 例： `Device(config-route-map)# match extcommunity 22`	指定したコミュニティ リストを照合します。 • この例では、拡張コミュニティ リスト 22（手順 3 で設定）に一致するルートが後続の **set** コマンドの対象となります。
ステップ 7	**set extcomm-list** *extcommunity-name* **delete** 例： `Device(config-route-map)# set extcomm-list 22 delete`	指定した拡張コミュニティ リスト内のルートから RT を削除します。 • この例では、拡張コミュニティ リスト 22 内のルートから RT が削除されます。
ステップ 8	**set extcommunity rt range** *start-value end-value* 例： `Device(config-route-map)# set extcommunity rt range 500:1 500:9`	ルート マップで許可されているルートに対して、拡張コミュニティ属性の指定した RT 範囲（境界値を含む）を設定します。 • この例では、拡張コミュニティ 22 に一致するルートに対して、500:1、500:2、500:3、500:4、500:5、500:6、500:7、500:8、500:9 の RT 拡張コミュニティ属性値を設定しています。

	コマンドまたはアクション	目的
ステップ 9	**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、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 10	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map rt-mapping permit 20`	（任意）ルートを許可するルート マップ エントリを設定します。 • この例では、RT から RT 範囲へのマッピングの対象とならない他のルートを許可するルート マップ エントリを設定します。この手順を実行しない場合、他のすべてのルートは暗黙の deny の対象となります。
ステップ 11	**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、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 12	**router bgp** *as-number* 例： `Device(config)# router bgp 3000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.103.1 remote-as 3000`	自律システムに属するネイバーを指定します。
ステップ 14	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.103.1 activate`	指定したネイバーをアクティブにします。
ステップ 16	**neighbor** *ip-address* **route-map** *map-tag* **out** 例： `Device(config-router-af)# neighbor 192.168.103.1 route-map rt-mapping out`	指定した発信ルート マップを、指定したネイバーに適用します。

	コマンドまたはアクション	目的
ステップ 17	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

RT 範囲を RT に置き換える

属性の RT 範囲を RT 属性に置き換えるには、入力 ASBR でこの作業を実行します。この作業では、RT を RT 範囲に置き換えるように出力 ASBR を設定済みであることを前提としています。この作業については、「RT を RT 範囲に置き換える」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *reg-exp*
4. **exit**
5. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
6. **match extcommunity** *extended-community-list-name*
7. **set extcomm-list** *extcommunity-name* **delete**
8. **set extcommunity rt** *value* **additive**
9. **exit**
10. **route-map** *map-tag* {**permit** | **deny**} [*sequence-number*]
11. **exit**
12. **router bgp** *as-number*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **address-family vpnv4**
15. **neighbor** *ip-address* **activate**
16. **neighbor** *ip-address* **route-map** *map-tag* **in**
17. **exit-address-family**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 extcommunity-list** *expanded-list* {**permit** | **deny**} **rt** *reg-exp* 例： `Device(config)# ip extcommunity-list 128 permit rt 500:[1-9]`	IP 拡張コミュニティ リストを設定して、指定した RT 範囲の RT を持つルートが拡張コミュニティ リストに含まれるように、バーチャル プライベート ネットワーク（VPN）ルート フィルタリングを設定します。 • この例では、500:1 ～ 500:9 の範囲内の RT を持つルートを拡張コミュニティ リスト 128 に対して許可しています。
ステップ 4	**exit** 例： `Device(config-extcomm-list)# exit`	コンフィギュレーション モードを終了し、次に高い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	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map rtmap2 permit 10`	後続の **match** コマンドで一致と認められたルートを許可または拒否するルートマップを設定します。 • この例では、後続の **match** コマンドで一致と認められたルートを許可します。
ステップ 6	**match extcommunity** *extended-community-list-name* 例： `Device(config-route-map)# match extcommunity 128`	指定したコミュニティ リストを照合します。 • この例では、拡張コミュニティ リスト 128（手順 3 で設定）に一致するルートが後続の **set** コマンドの対象となります。
ステップ 7	**set extcomm-list** *extcommunity-name* **delete** 例： `Device(config-route-map)# set extcomm-list 128 delete`	指定した拡張コミュニティ リスト内のルートから範囲内の RT を削除します。 • この例では、拡張コミュニティ リスト 128 内のルートから範囲内の RT が削除されます。
ステップ 8	**set extcommunity rt** *value* **additive** 例： `Device(config-route-map)# set extcommunity rt 400:1 additive`	ルート マップで許可されているルートに、指定した RT を設定します。 • この例では、拡張コミュニティ 128 に一致するルートに RT 400:1 を設定します。**additive** キーワードを指定すると、RT を置き換えずに RT が RT リストに追加されます。
ステップ 9	**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、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 10	**route-map** *map-tag* {**permit** | **deny**} [*sequence-number*] 例： `Device(config)# route-map rtmap2 permit 20`	（任意）ルートを許可するルート マップ エントリを設定します。 • この例では、RT 範囲から RT へのマッピングの対象とならない他のルートを許可するルート マップ エントリを設定します。この手順を実行しない場合、他のすべてのルートは暗黙の deny の対象となります。
ステップ 11	**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、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 12	**router bgp** *as-number* 例： `Device(config)# router bgp 4000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 13	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.0.50 remote-as 4000`	自律システムに属するネイバーを指定します。
ステップ 14	**address-family vpnv4** 例： `Device(config-router-af)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 15	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.0.50 activate`	指定したネイバーをアクティブにします。
ステップ 16	**neighbor** *ip-address* **route-map** *map-tag* **in** 例： `Device(config-router-af)# neighbor 192.168.0.50 route-map rtmap2 in`	指定した着信ルート マップを指定したネイバーに適用します。
ステップ 17	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP-RT および VPN 識別子属性の書き換えワイルドカードの設定例

例：RT を RT 範囲に置き換える

次の例では、出力 ASBR で、RT 101:100 を持つルートが拡張コミュニティ リスト 22 に含まれます。rt-mapping という名前のルート マップで拡張コミュニティ リスト 22 を照合し、コミュニティ リスト内のルートから RT を削除します。コミュニティ リストに一致するルートに対して、500:1 ～ 500:9 の範囲内の RT を設定します。このルート マップはネイバー 192.168.103.1 に適用されます。

出力 ASBR

```
ip extcommunity-list 22 permit rt 101:100
!
route-map rt-mapping permit 10
 match extcommunity 22
 set extcomm-list 22 delete
 set extcommunity rt range 500:1 500:9
!
route-map rt-mapping permit 20
!
router bgp 3000
 neighbor 192.168.103.1 remote-as 3000
 address-family vpnv4
  neighbor 192.168.103.1 activate
  neighbor 192.168.103.1 route-map rt-mapping out
  exit-address-family
!
```

入力 ASBR では、500:1 ～ 500:9 の範囲内の RT が拡張コミュニティ リスト 128 に属します。rtmap2 という名前のルート マップで、これらの RT を RT 400:1 にマッピングします。このルート マップはネイバー 192.168.0.50 に適用されます。

入力 ASBR

```
ip extcommunity-list 128 permit RT:500:[1-9]
!
route-map rtmap2 permit 10
 match extcommunity 128
 set extcomm-list 128 delete
 set extcommunity rt 400:1 additive
!
route-map rtmap2 permit 20
!
router bgp 4000
 neighbor 192.168.0.50 remote-as 4000
 address-family vpnv4
  neighbor 192.168.0.50 activate
  neighbor 192.168.0.50 route-map rtmap2 in
```

```
  exit-address-family
!
```

例：RT を VPN 識別子範囲に置き換える

次の例では、出力 ASBR で、RT 201:100 を持つルートが拡張コミュニティ リスト 22 に含まれます。rt-mapping という名前のルート マップで拡張コミュニティ リスト 22 を照合し、コミュニティ リスト内のルートから RT を削除します。コミュニティ リストに一致するルートに対して、600:1 ～ 600:8 の範囲内の VPN 識別子を設定します。このルート マップはネイバー 192.168.103.1 に適用されます。

出力 ASBR

```
ip extcommunity-list 22 permit rt 201:100
!
route-map rt-mapping permit 10
 match extcommunity 22
 set extcomm-list 22 delete
 set extcommunity vpn-distinguisher range 600:1 600:8
!
route-map rt-mapping permit 20
!
router bgp 3000
 neighbor 192.168.103.1 remote-as 3000
 address-family vpnv4
  neighbor 192.168.103.1 activate
  neighbor 192.168.103.1 route-map rt-mapping out
  exit-address-family
!
```

入力 ASBR では、600:1 ～ 600:8 の範囲内の VPN 識別子が拡張コミュニティ リスト 101 に属します。rtmap2 という名前のルート マップで、これらの VPN 識別子を RT 範囲 700:1 ～ 700:10 にマッピングします。このルート マップはネイバー 192.168.0.50 に適用されます。additive オプションを指定すると、新しい範囲が既存の値に置き換えなしに追加されます。

入力 ASBR

```
ip extcommunity-list 101 permit VD:600:[1-8]
!
route-map rtmap2 permit 10
 match extcommunity 101
 set extcomm-list 101 delete
 set extcommunity rt 700:1 700:10 additive
!
route-map rtmap2 permit 20
!
router bgp 4000
 neighbor 192.168.0.50 remote-as 4000
 address-family vpnv4
  neighbor 192.168.0.50 activate
  neighbor 192.168.0.50 route-map rtmap2 in
  exit-address-family
!
```

BGP-RT および VPN 識別子属性の書き換えワイルドカードに関する追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP—VPN 識別子属性	『*IP : BGP Configuration Guide, XE 3S*』の「BGP—VPN Distinguisher Attribute」モジュール

シスコのテクニカル サポート

説明	リンク
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

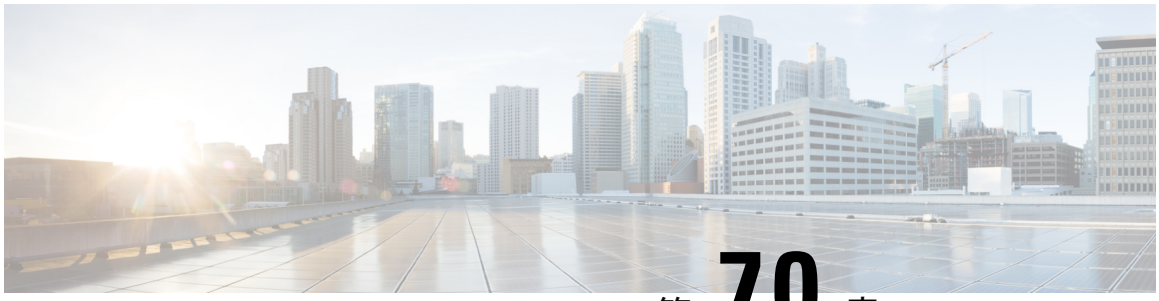
BGP—RT および VPN 識別子属性の書き換えワイルドカードに関する機能情報

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 *89 : BGP—RT* および *VPN* 識別子属性の書き換えワイルドカードに関する機能情報

機能名	リリース	機能情報
BGP—RT および VPN 識別子属性の書き換えワイルドカード		BGP—RT および VPN 識別子属性の書き換えワイルドカード機能は、マッピングの際にルート ターゲット（RT）コミュニティ属性または VPN 識別子コミュニティ属性の範囲を設定できるようにします。出力 ASBR における 1 つ以上の RT を入力 ASBR における別の RT にマッピングすることが必要となる場合があります。VPN 識別子属性機能により、管理者は、eBGP を介して伝送される VPN 識別子に RT をマッピングし、次に入力 ASBR で RT にマッピングすることができます。このマッピングは、拡張コミュニティ属性の RT 範囲または VPN 識別子範囲を指定するルート マップを設定することによって実現されます。個々の RT ではなく範囲を指定することにより、時間が節約され、設定が簡素化されます。また、VPN 識別子範囲では、route-map 句ごとに複数の VPN 識別子属性を使用できるため、この機能が導入される前に適用されていた制約がなくなります。 次のコマンドが変更されました。 • **set extcommunity rt** • **set extcommunity vpn-distinguisher**



第 70 章

VPLS BGP シグナリング

仮想プライベート LAN サービス（VPLS）コントロール プレーンの 2 つの主要機能は、自動検出とシグナリングです。VPLS BGP シグナリング機能は、RFC 4761 に準拠した VPLS 用の自動検出とシグナリング プロトコルの両方として BGP を使用できるようにします。

- 機能情報の確認 （1161 ページ）
- VPLS BGP シグナリングの前提条件 （1161 ページ）
- VPLS BGP シグナリングに関する情報 （1162 ページ）
- VPLS BGP シグナリングの設定方法 （1163 ページ）
- VPLS BGP シグナリングの設定例 （1166 ページ）
- VPLS BGP シグナリングの追加情報 （1166 ページ）
- VPLS BGP シグナリングの機能情報 （1167 ページ）

機能情報の確認

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

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

VPLS BGP シグナリングの前提条件

『』の「Configuring Virtual Private LAN Services」モジュールおよび「VPLS Autodiscovery BGP Based」モジュールで示されている概念を十分に理解している必要があります。

VPLS BGP シグナリングに関する情報

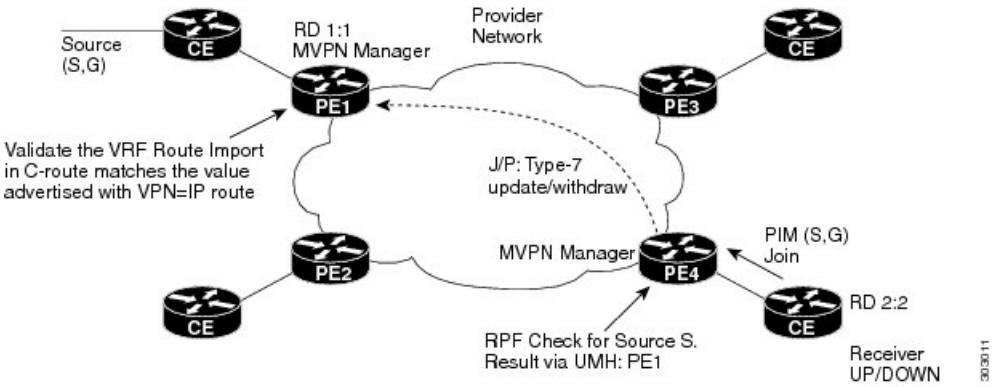
VPLS BGP シグナリングの概要

VPLS BGP シグナリング機能が導入される前は、BGP は、RFC 6074 に準拠したシグナリング用の自動検出および Label Distribution Protocol（LDP; ラベル配布プロトコル）に使用されていました。VPLS BGP シグナリング機能は、RFC 4761 に準拠した自動検出とシグナリング用のコントロール プレーン プロトコルとして BGP を使用できるようにします。

RFC 4761 で指定されているように、内部 BGP（iBGP）ピアでは、L2VPN 情報を含む L2VPN AFI/SAFI のアップデート メッセージを交換して、自動検出とシグナリングの両方を実行します。BGP マルチプロトコルのネットワーク層到達可能性情報（NLRI）は、ルート識別子（RD）、VPLS エンドポイント ID（VE ID）、VE ブロック オフセット（VBO）、VE ブロック サイズ（VBS）、ラベル ベース（LB）で構成されます。

下の図に、RFC 4761 の NLRI 形式を示します。

図 *89 : RFC 4761 NLRI*



ネクストホップ、ルート ターゲット（VPLS インスタンス用に指定）、その他のレイヤ 2 データなどの追加情報は、BGP 拡張コミュニティ属性で伝送されます。L3VPN に似たルート ターゲット ベースのインポートおよびエクスポート メカニズムは、特定の VPLS インスタンスの L2VPN NLRI をフィルタ処理するために BGP により実行されます。

BGP シグナリング（RFC 4761）を使用するか LDP シグナリング（RFC 6074）を使用するかは、指定するコマンドによって決まります。VPLS BGP シグナリング機能を有効にするには、L2 VFI コンフィギュレーション モードで **autodiscovery bgp signaling bgp** コマンドを使用します。このコマンドは、VPLS インスタンス単位でサポートされます。

無効な（つまり、設定に一致しない）BGP アップデート アドバタイズメント（更新または取り消し）は、BGP セッションで受信された場合に無視されます。

VPLS のサポートにおける BGP の主なタスクは、L2VPN アドレス ファミリでのルート配布、および L2VPN との連携です。BGP とその他のコンポーネントの間における連携はそのまま維持されます。ベストパス選択、ネクストホップ処理、アップデート生成などの基本的な BGP

機能は、VPLS BGP シグナリングでも同様に機能し続けます。BGP RT 制約は、BGP VPLS シグナリング機能とシームレスに連携します。

VPLS BGP シグナリングの設定方法

VPLS BGP シグナリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **l2vpn vfi context** *name*
4. **vpn id** *vpn-id*
5. **autodiscovery bgp signaling** {**bgp** | **ldp**} [**template** *template-name*]
6. **ve id** *ve-id*
7. **ve range** *ve-range*
8. **exit**
9. **exit**
10. **router bgp** *autonomous-system-number*
11. **bgp graceful-restart**
12. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
13. **address-family l2vpn** [**vpls**]
14. **neighbor** *ip-address* **activate**
15. **neighbor** *ip-address* **send-community** [**both** | **standard** | **extended**]
16. **neighbor** *ip-address* **suppress-signaling-protocol ldp**
17. **end**
18. **show bgp l2vpn vpls** {**all** | **rd** *route-distinguisher*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**l2vpn vfi context** *name* 例： `Device(config)# l2vpn vfi context vfi1`	複数の異なるネットワーク間の L2VPN 仮想転送インターフェイス（VFI）を確立し、レイヤ 2 VFI コンフィギュレーション モードを開始します。
ステップ 4	**vpn id** *vpn-id* 例： `Device(config-vfi)# vpn id 100`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**autodiscovery bgp signaling** {**bgp** | **ldp**} [**template** *template-name*] 例： `Device(config-vfi)# autodiscovery bgp signaling bgp`	BGP シグナリングおよび検出または LDP シグナリングを有効にし、L2VPN VFI 自動検出コンフィギュレーション モードを開始します。 （注） VPLS BGP シグナリング機能では、**autodiscovery bgp signaling bgp** コマンドを使用します。
ステップ 6	**ve id** *ve-id* 例： `Device(config-vfi-autodiscovery)# ve id 1001`	VPLS エンドポイント（VE）デバイス ID 値を指定します。VE ID は、VPLS サービス内の VFI を識別します。VE デバイス ID の値は 1 ～ 16384 です。
ステップ 7	**ve range** *ve-range* 例： `Device(config-vfi-autodiscovery)# ve range 12`	VE デバイス ID の範囲値を指定します。VE 範囲は VE ブロックの最小サイズをオーバーライドします。デフォルトの最小サイズは 10 です。設定する VE の範囲は、10 よりも高い必要があります。
ステップ 8	**exit** 例： `Device(config-vfi-autodiscovery)# exit`	L2VPN VFI 自動検出コンフィギュレーション モードを終了し、L2VPN VFI コンフィギュレーション モードを開始します。
ステップ 9	**exit** 例： `Device(config-vfi)# exit`	L2VPN VFI コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。

	コマンドまたはアクション	目的
ステップ 11	**bgp graceful-restart** 例： `Device(config-router)# bgp graceful-restart`	BGP グレースフル リスタート機能と BGP ノンストップ フォワーディング（NSF）認識を有効にします。
ステップ 12	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.10.10.1 remote-as 100`	指定された自律システム内の BGP ネイバーとのピアリングを設定します。
ステップ 13	**address-family l2vpn** [**vpls**] 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • オプションの **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布されるように指定します。 この例では、L2VPN VPLS アドレス ファミリ セッションが作成されます。
ステップ 14	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 10.10.10.1 activate`	ネイバーを有効にして、L2VPN VPLS アドレス ファミリの情報をローカル デバイスと交換します。
ステップ 15	**neighbor** *ip-address* **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 10.10.10.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。
ステップ 16	**neighbor** *ip-address* **suppress-signaling-protocol ldp** 例： `Device(config-router-af)# neighbor 10.10.10.1 suppress-signaling-protocol ldp`	LDP シグナリングを抑止し、BGP シグナリングを有効にします。 • この例では、10.10.10.1 のネイバーに対する LDP シグナリングが抑止されます（BGP シグナリングが有効化されます）。
ステップ 17	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 18	**show bgp l2vpn vpls** {**all** | **rd** *route-distinguisher*} 例： `Device# show bgp l2vpn vpls all`	（任意）L2VPN VPLS アドレス ファミリに関する情報を表示します。

VPLS BGP シグナリングの設定例

例：VPLS BGP シグナリングの設定と確認

```
l2vpn vfi context vfi1
 vpn id 100
 autodiscovery bgp signaling bgp
  ve id 1001
  ve range 10
 !
!
router bgp 100
 bgp graceful-restart
 neighbor 209.165.200.224 remote-as 100
 neighbor 209.165.200.224 update-source Loopback1
 !
 address-family l2vpn vpls
  neighbor 209.165.200.224 activate
  neighbor 209.165.200.224 send-community extended
  neighbor 209.165.200.224 suppress-signaling-protocol ldp
  exit-address-family
 !
show bgp l2vpn vpls all

Network                          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:100
*>100:100:VEID-1001:Blk-1001/136    0.0.0.0                                32768  ?

*>i 100:100:VEID-1003:Blk-1000/136  209.165.200.224              0      100     0
?
```

VPLS BGP シグナリングの追加情報

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』

関連項目	マニュアル タイトル
BGP 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、コマンド履歴、使用上の注意事項、および例	『Cisco IOS IP Routing: BGP Command Reference』
仮想プライベート LAN サービスの設定	
アクセス ポートの設定	「Configuring Virtual Private LAN Services」、『』
『VPLS Autodiscovery BGP Based』	

標準および RFC

標準/RFC	タイトル
RFC 4761	『*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*』
RFC 6074	『*Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

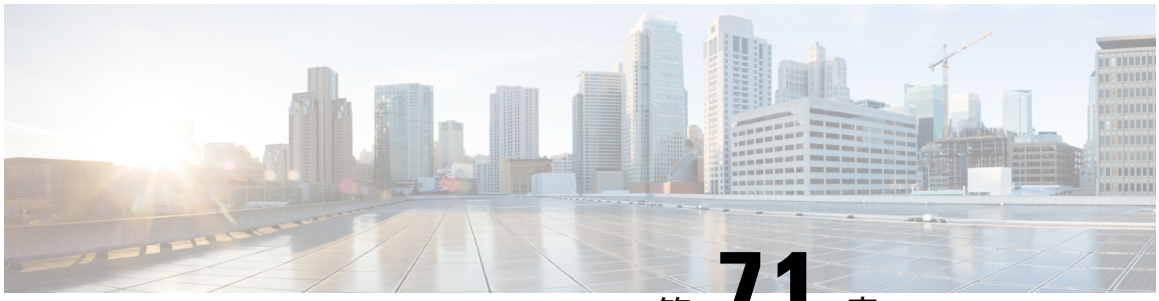
VPLS BGP シグナリングの機能情報

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

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 *90 : VPLS BGP* シグナリングの機能情報

機能名	リリース	機能情報
VPLS BGP シグナリング		VPLS BGP シグナリング機能は、RFC 4761 に準拠した VPLS用の自動検出とシグナリング プロトコルの両方として BGP を使用できるようにします。 次のコマンドが導入または変更されました。**autodiscovery (MPLS)**、**neighbor suppress-signaling-protocol**、**show bgp l2vpn vpls**、**ve**



第 71 章

マルチキャスト VPN BGP ダンプニング

特定のマルチキャスト グループ内の単一の受信者、またはアップ状態とダウン状態を頻繁に行き来し、特定のマルチキャスト グループに関係する受信者のグループによって、マルチキャスト VPN BGP ダンプニング機能がアクティブ化され、BGP シグナリングを使用してコア内でタイプ 7 ルート（C-マルチキャスト ルートの Join/Prune）のダンプニングが行われます。この機能は、カスタマー側の join/prune リクエストによるチャーンを低減して、不要な BGP MVPN タイプ 6/7 C-ルート制御情報の発生を防ぎます。

- 機能情報の確認 （1169 ページ）
- マルチキャスト VPN BGP ダンプニングの前提条件 （1170 ページ）
- マルチキャスト VPN BGP ダンプニングに関する情報 （1170 ページ）
- マルチキャスト VPN BGP ダンプニングの設定方法 （1171 ページ）
- マルチキャスト VPN BGP ダンプニングの設定例 （1174 ページ）
- マルチキャスト VPN BGP ダンプニングの追加情報 （1174 ページ）
- マルチキャスト VPN BGP ダンプニングの機能情報 （1175 ページ）

機能情報の確認

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

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

マルチキャスト VPN BGP ダンプニングの前提条件

- 『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP ルート ダンプニング」モジュールに示されている概念を理解しておく必要があります。

マルチキャスト VPN BGP ダンプニングに関する情報

マルチキャスト VPN BGP ダンプニングの概要

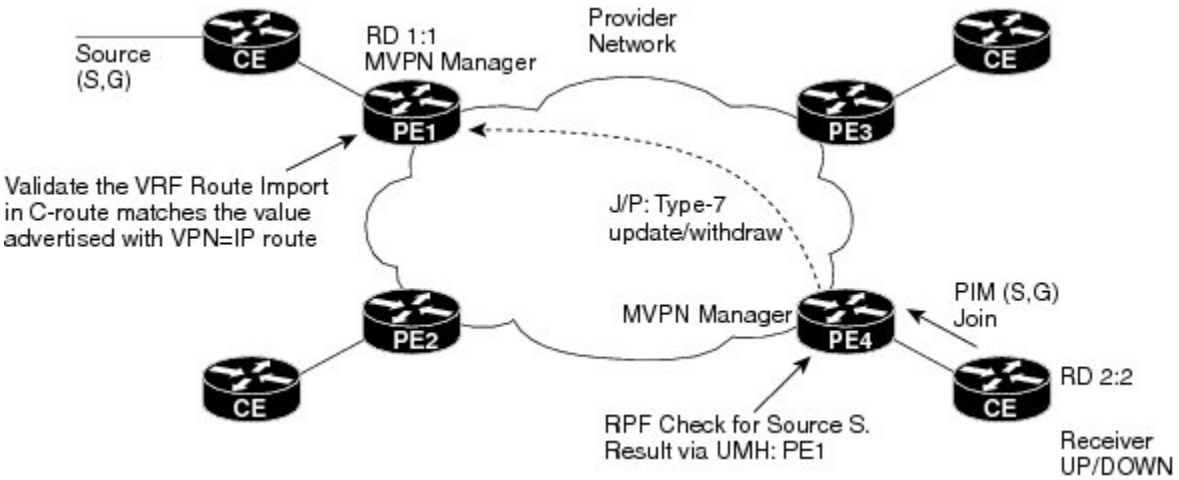
BGP ルート ダンプニング

ルート ダンプニングは、インターネットワーク間でフラッピング ルートの伝搬を最小限に抑えるように設計された BGP 機能です。ルートは、その可用性が繰り返し切り替わる場合にフラッピングすると見なされます。BGP を実行しているシスコ デバイスは、フラッピング ルートの不安定な影響を「ダンプニング」するように設計されたメカニズムを備えています。BGP を実行しているシスコ デバイスは、フラッピング ルートを検出すると、そのルートのダンプニングを自動的に行います。

下の図に、マルチキャスト VPN BGP ダンプニングのメカニズムを示します。

マルチキャスト VPN BGP ダンプニング

図 *90 :* マルチキャスト *VPN BGP* ダンプニング



マルチキャスト グループ内の単一の受信者、または頻繁に状態が変化（フラッピング）し、特定のマルチキャスト グループに関係する受信者のグループによって、マルチキャスト VPN（MVPN）BGP ダンプニングがアクティブ化されます。MVPN BGP ダンプニングで、BGP シ

グナリングを使用してコア内でタイプ 7 マルチキャスト ルート（カスタマー マルチキャスト（C-マルチキャスト）ルートの join/prune）のダンプニングが行われます。

MVPN BGP ダンプニングが有効になっていない場合、送信元は、受信者がダウン状態でもデータを送信します。受信者がダウン状態になると、プロバイダー エッジ（PE）デバイスに対する 60 秒間隔の C-PIM join がなくなるため、デフォルトの期間（3 分）が経過すると、PE 側で PIM がタイムアウトします。MVPN マネージャは、タイプ 7 ルート（C-マルチキャスト ルートの取り消し）である prune メッセージを BGP に送信します。

受信者は、アップ状態になると、新しい (S,G) join リクエストをカスタマー エッジ（CE）デバイスに送信します。C-PIM join を PE デバイスが受信し、新しいタイプ 7 C-マルチキャスト アップデートが BGP から自動検出された MVPN ピアに送信されます。アップストリーム マルチキャスト ピアは、BGP タイプ 7 アップデートを送信元に対する PIM join に変換し、送信元は、MDT トンネルを使用してダウンストリーム PE 経由で受信者が受信することになる、データ トラフィックを送信します。受信者がアップ状態とダウン状態を頻繁に行き来する場合、送信元側の PIM は join/prune メッセージを頻繁に受信するため、それに応じて送信元が応答することになります。

MVPN BGP ダンプニングが有効になっている場合、BGP の一般的なダンプニング メカニズムが MVPN VRF インスタンスに適用されます。CE 側からの Join/Prune メッセージは、更新/取り消しとして MVPN マネージャから MVPN PE デバイスに送信されます。PE デバイス上の MVPN マネージャは、リバース パス フォワーディング（RPF）およびアップストリーム マルチホップ（UMH）のネクストホップ変更のために、join/prune メッセージをカスタマー側に送信します。

マルチキャスト VPN BGP ダンプニングの設定方法

マルチキャスト VPN BGP ダンプニングの設定

マルチキャスト VPN BGP ダンプニングを有効にして設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** [**ipv4** | **ipv6**] **mvpn vrf** *vrf-name*
5. **bgp dampening** [*half-life reuse suppress max-suppress-time*]
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	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family** [**ipv4** | **ipv6**] **mvpn vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 mvpn vrf blue`	アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **ipv4** キーワードを使用して、IPv4 マルチキャスト C-ルート交換を有効にします。 • **ipv6** キーワードを使用して、IPv6 マルチキャスト C-ルート交換を有効にします。 （注） 次の手順でマルチキャスト VPN BGP ダンプニングを有効にするには、この時点で **vrf** キーワードと *vrf-name* 引数を指定する必要があります。
ステップ 5	**bgp dampening** [*half-life reuse suppress max-suppress-time*] 例： `Device(config-router-af)# bgp dampening 30 1500 10000 120`	BGP ルート ダンプニングをイネーブルにして、ルート ダンプニング係数のデフォルト値を変更します。*half-life*、*reuse*、*suppress*、および *max-suppress-time* 引数は、すべて位置に依存します。引数を 1 つ入力する場合は、すべての引数を入力する必要があります。 （注） 手順 4 および 5 を繰り返して、代替 VRF でマルチキャスト VPN BGP ダンプニングを有効にします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

マルチキャスト VPN BGP ダンプニングのモニタとメンテナンス

マルチキャスト VPN BGP ダンプニングをモニタおよびメンテナンスするには、必要に応じてこの作業の手順を実行します。

手順の概要

1. **enable**
2. **show bgp** {**ipv4** | **ipv6**} **mvpn** {**all** | **rd** *route-distinguisher* | **vpn** *vrf-name*} [**dampening** {**dampened-paths** | **flap-statistics** [**filter-list** *access-list-number* | **quote-regexp** *regexp* | **regexp** *regexp*]}]
3. **clear ip bgp** {**ipv4** | **ipv6**} **mvpn vrf** *vrf-name* {**dampening** | **flap-statistics**}

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show bgp {ipv4 | ipv6} mvpn {all | rd route-distinguisher | vpn vrf-name} [dampening {dampened-paths | flap-statistics [filter-list access-list-number | quote-regexp regexp | regexp regexp]}]

マルチキャスト VPN BGP ダンプニングをモニタするには、このコマンドを使用します。

- **dampened-path** キーワードは、ダンプニングされた BGP ルートに関する情報を表示します。
- **parameters** キーワードは、詳細な BGP ダンプニング情報を表示します。
- **flap-statistics** キーワードは、BGP フラップ統計情報を表示します。

例：

```
Device# show bgp ipv4 mvpn vrf blue route-type 7 111.111.111.111:11111 55 202.100.0.6 232.1.1.1

BGP routing table entry for [7][111.111.111.111:11111][55][202.100.0.6/32][232.1.1.1/32]/22, version
 17
Paths: (1 available, no best path)
Flag: 0x820
  Not advertised to any peer
  Refresh Epoch 1
  Local, (suppressed due to dampening)
    0.0.0.0 from 0.0.0.0 (205.3.0.3)
      Origin incomplete, localpref 100, weight 32768, valid, sourced, local
      Extended Community: RT:205.1.0.1:1
      Dampinfo: penalty 3472, flapped 4 times in 00:04:42, reuse in 00:00:23
      rx pathid: 0, tx pathid: 0
```

ステップ 3 clear ip bgp {ipv4 | ipv6} mvpn vrf vrf-name {dampening | flap-statistics}

マルチキャスト VPN BGP ダンプニングが有効になったルータで受信したルートの累積ペナルティをクリアするには、このコマンドを使用します。

- **dampening** キーワードは、マルチキャスト VPN BGP ダンプニング情報をクリアします。
- **flap-statistic** キーワードは、マルチキャスト VPN BGP ダンプニングのフラップ統計をクリアします。

例：

```
Device# clear ip bgp ipv4 mvpn vrf blue dampening
```

マルチキャスト VPN BGP ダンプニングの設定例

例：マルチキャスト VPN BGP ダンプニングの設定

次の例では、マルチキャスト VPN BGP ダンプニングが blue という VRF と red という VRF に適用されますが、green という VRF には適用されません。

```
address-family ipv4 mvpn vrf blue
 bgp dampening

address-family ipv4 mvpn vrf red
 bgp dampening

address-family ipv4 mvpn vrf green
 no bgp dampening
```

マルチキャスト VPN BGP ダンプニングの追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

関連項目	マニュアル タイトル
BGP ルート ダンプニング	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「内部 BGP 機能の設定」モジュールの「BGP ルート ダンプニング」の項

標準および RFC

標準/RFC	タイトル
RFC 2439	『*BGP Route Flap Damping*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

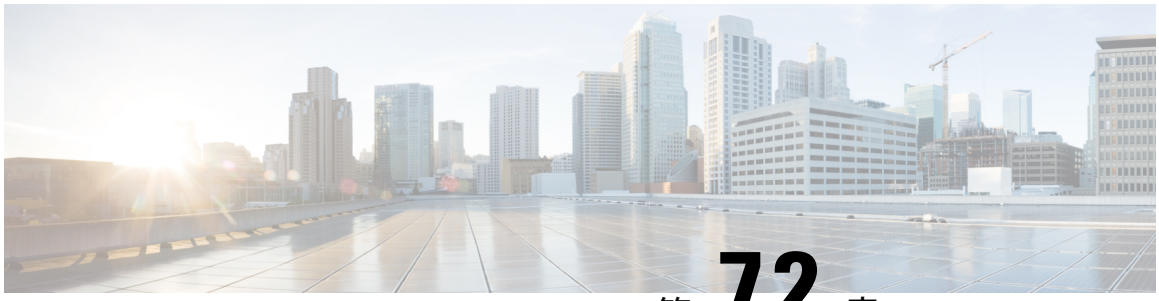
マルチキャスト VPN BGP ダンプニングの機能情報

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 *91 :* マルチキャスト *VPN BGP* ダンプニングの機能情報

機能名	リリース	機能情報
マルチキャスト VPN BGP ダンプニング	Cisco IOS XE Release 3.8S	特定のマルチキャスト グループ内の単一の受信者、またはアップ状態とダウン状態を頻繁に行き来し、特定のマルチキャスト グループに関係する受信者のグループによって、マルチキャスト VPN BGP ダンプニング機能で、BGP シグナリングを使用してコア内でタイプ 7 ルート（C-マルチキャスト ルートの join/prune）のダンプニングが行われます。 次のコマンドが導入または変更されました。**address-family mvpn**、**clear ip bgp mvpn**、**show bgp mvpn**、**show ip bgp ipv4**



第 72 章

BGP—IPv6 NSR

ノンストップルーティング（NSR）に対するボーダーゲートウェイプロトコル（BGP）サポート機能により、プロバイダーエッジ（PE）ルータはカスタマーエッジ（CE）ルータとともにBGP の状態を維持でき、ルート プロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的なインサービス ソフトウェア アップグレード（ISSU）中に、継続的なパケットの転送を確実に行えるようになります。BGP—IPv6 NSR 機能は、NSR に対する BGP サポートを Cisco IPv6 VPN プロバイダー エッジ ルータ（6VPE）に拡張します。

- 機能情報の確認 （1177 ページ）
- BGP—IPv6 NSR の前提条件 （1177 ページ）
- BGP-IPv6 NSR に関する情報 （1178 ページ）
- BGP-IPv6 NSR の設定方法 （1179 ページ）
- BGP-IPv6 NSR の設定例 （1180 ページ）
- BGP—IPv6 NSR の追加情報 （1181 ページ）
- BGP—IPv6 NSR の機能情報 （1181 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

BGP—IPv6 NSR の前提条件

- BGP を実行するようにネットワークが設定されている必要があります。

- マルチプロトコル レイヤ スイッチング（MPLS）レイヤ 3 バーチャル プライベート ネットワーク（VPN）が設定されている必要があります。
- すべてのプラットフォームが HA に対応している必要があります。
- 『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「ステートフル スイッチオーバー（SSO）によ るノンストップ ルーティング（NSR）に対する BGP サポート」モジュールおよび「iBGP ピアの BGP NSR サポート」モジュールに示されている概念について十分に理解している必要があります。

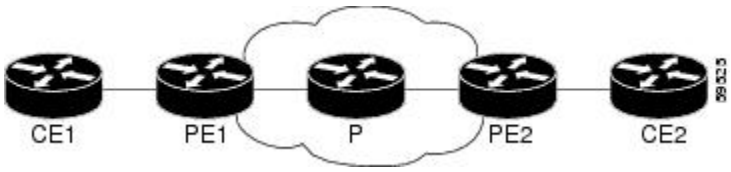
BGP-IPv6 NSR に関する情報

BGP—IPv6 NSR の概要

ノンストップ ルーティング（NSR）は、アクティブ ルート プロセッサ（RP）からスタンバイ RP へのスイッチオーバー時にパケットがドロップされる可能性を低減するため、BGP ピアで役立ちます。スイッチオーバーは何らかの理由によりアクティブ RP で障害が発生した場合に行われ、スタンバイ RP がアクティブ RP の機能を制御することになります。BGP—IPv6 NSR 機能は、次の IPv6 ベースのアドレス ファミリを含むように NSR に対する BGP サポートを拡張します。

- IPv6 ユニキャスト
- IPv6 ユニキャスト+ラベル
- IPv6 PE-CE
- VPNv6 ユニキャスト

図 *91 :* 基本的な *6VPE* ネットワーク設定



上の図は、基本的な展開シナリオを示しています。プロバイダー エッジ（PE）ルータ 1、P、PE2 が 6VPE クラウドを形成しています。カスタマー エッジ（CE）ルータ 1 から PE1 への接続は IPv6（VRF）です。PE は HA/SSO および NSF 対応です。P ルータは、マルチプロトコル ラベル スイッチング（MPLS）のラベル保持（NSF に相当）に対応しています。

CE1 は顧客機器であるため、NSF 対応となるようにアップグレードする必要があるかどうかをプロバイダーは判断できません。PE1 が CE1 への接続で NSR を実行できる場合は、PE1 が SSO モードでスイッチオーバーを実行した際に CE1 はそれを認識できないかその影響を受けません。自律システム内のその他のすべての接続では、この操作は NSF である場合もグレースフル リスタートである場合もあります。つまり、コントロール プレーンがリセットされ、直接

接続されたすべてのピアがそれを認識してセッションの再確立に役立つデータを再送信しますが、転送は中断されません。

NSR で動作していないネイバーは、引き続き NSF 対応/認識であると想定されます。CE がすでに NSF 認識である（つまり、そのピアで BGP グレースフル リスタートを処理できる）場合、PE-CE 接続は NSR ではなく、通常の NSF 処理モデルに従います。これは、 VPNv4 向け NSR と同様であり、ネットワーク リソースの節約に役立ちます。

BGP-IPv6 NSR の設定方法

BGP—IPv6 NSR の設定

BGP—IPv6 NSR をサポートするように BGP ピアを設定する場合は、PE ルータで次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. 次のいずれか 1 つを入力します。
   - **address-family ipv6** [**unicast** | **multicast** | **vpnv6**] [**vrf** *vrf-name*]
   - **address-family vpnv6** [**unicast** | **multicast**]
5. **neighbor** *ipv6-address%* **remote-as** *as-number*
6. **neighbor** *ipv6-address%* **activate**
7. **neighbor** *ipv6-address%* **ha-mode sso**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 4000`	
ステップ 4	次のいずれか 1 つを入力します。 • **address-family ipv6** [**unicast** | **multicast** | **vpnv6**] [**vrf** *vrf-name*] • **address-family vpnv6** [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6 unicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv6 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスの名前を指定します。
ステップ 5	**neighbor** *ipv6-address%* **remote-as** *as-number* 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 4000`	ネイバーの自律システムを指定します。
ステップ 6	**neighbor** *ipv6-address%* **activate** 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 activate`	指定したピアをアクティブにします。
ステップ 7	**neighbor** *ipv6-address%* **ha-mode sso** 例： `Device(config-router-af)# neighbor 2001:DB8:0:CC00::1 ha-mode sso`	BGP NSR をサポートするように BGP ネイバーを設定します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP-IPv6 NSR の設定例

例：BGP—IPv6 NSR の設定

```
router bgp 4000
 address-family ipv6 unicast
```

```
neighbor 2001:DB8:0:CC00::1 remote-as 4000
neighbor 2001:DB8:0:CC00::1 activate
neighbor 2001:DB8:0:CC00::1 ha-mode sso
```

BGP—IPv6 NSR の追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

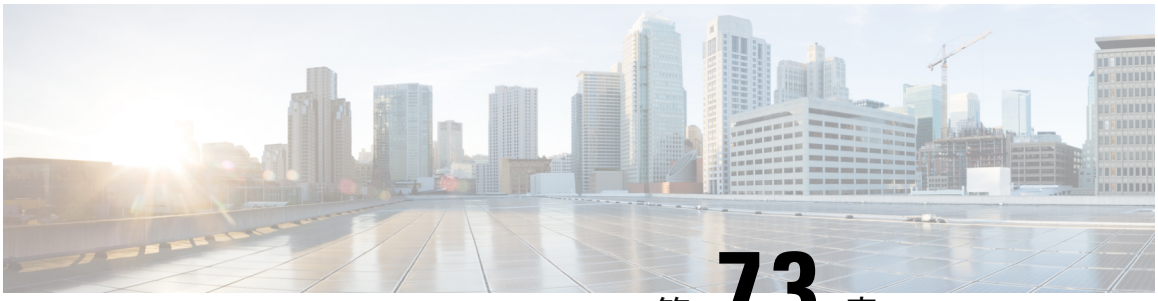
BGP—IPv6 NSR の機能情報

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 *92 : BGP—IPv6 NSR* の機能情報

機能名	リリース	機能情報
BGP—IPv6 NSR	Cisco IOS XE Release 3.9S	NSR に対する BGP サポート機能により、プロバイダー エッジ（PE）ルータはカスタマー エッジ（CE）ルータとともに BGP の状態を維持でき、ルートプロセッサ（RP）スイッチオーバー中または PE ルータに対する定期的な ISSU 中に、継続的なパケットの転送を確実に行えるようになります。 BGP—IPv6 NSR 機能は、NSR に対する BGP サポートを Cisco IPv6 VPN プロバイダー エッジ ルータ（6VPE）に拡張します。



第 73 章

BGP-VRF認識の条件付きアドバタイズメント

ボーダー ゲートウェイ プロトコル（BGP）VRF 認識の条件付きアドバタイズメント機能は、ルートアドバタイズメントの制御を拡充し、この制御を Virtual Routing and Forwarding（VRF）インスタンス内に拡張します。

- 機能情報の確認 （1183 ページ）
- BGP VRF 認識条件付きアドバタイズメントに関する情報 （1184 ページ）
- BGP VRF 認識条件付きアドバタイズメントの設定方法 （1185 ページ）
- BGP VRF 認識条件付きアドバタイズメントの設定例 （1188 ページ）
- BGP VRF 認識の条件付きアドバタイズメントの追加情報 （1192 ページ）
- BGP VRF 認識の条件付きアドバタイズメントの機能情報 （1193 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

BGP VRF 認識条件付きアドバタイズメントに関する情報

VRF 認識の条件付きアドバタイズメント

ボーダー ゲートウェイ プロトコル（BGP）VRF 認識の条件付きアドバタイズメント機能は、ルートアドバタイズメントの制御を拡充し、この制御を Virtual Routing and Forwarding（VRF）インスタンス内に拡張します。

BGP 条件付きアドバタイズメント

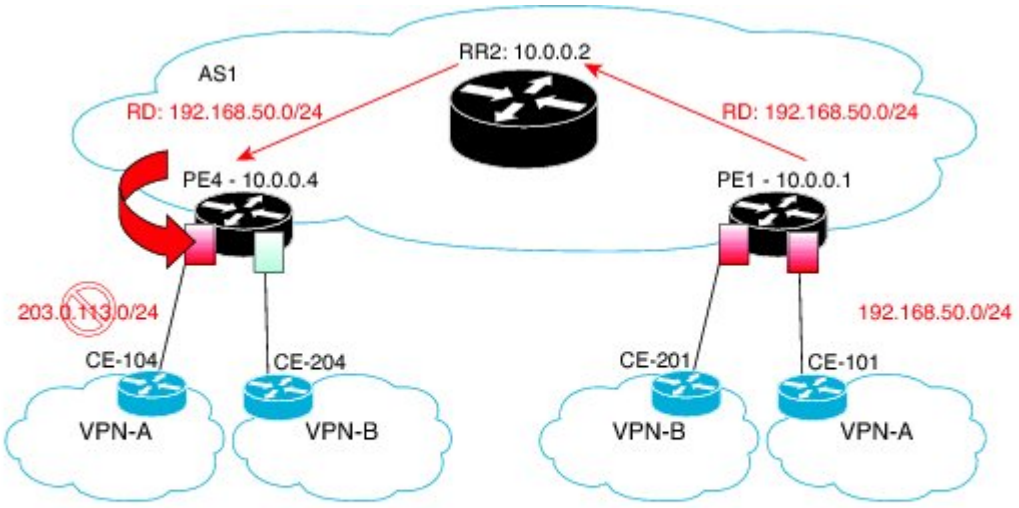
通常、ルートは別のルートの有無にかかわらず伝播されます。BGPの条件付きアドバタイズメント機能では、**neighbor** コマンドの **exist-map**、**non-exist-map**、**advertise-map** キーワードを使用して、ルート プレフィックスによりルートを追跡します。ルート プレフィックスが **non-exist-map** コマンドの出力に存在しない場合、**advertise-map** で指定されたルートが通知されます。この機能は、マルチホーム ネットワークで、いずれかのプロバイダーに対して他のプロバイダーからの情報が存在しない場合（これはピアリング セッションでの障害や不完全な到達可能性を示します）にのみ特定のプレフィックスをアドバタイズするときに便利です。条件付き BGP 通知は、BGP ルータからピアに送信される通常の通知と併せて送信されます。

VRF 認識の条件付きアドバタイズメント

この機能は、BGP VRF 認識の条件付きアドバタイズメントのサポートを次のアドレス ファミリに拡張します。

- IPv4 ユニキャスト
- IPv4 ユニキャスト VRF
- IPv6 ユニキャスト
- IPv6 ユニキャスト VRF

図 *92 : VRF* ベースの条件付きアドバタイズメント



PE4: VRF RED Routing Table	
EXIST	192.168.50.0/24
ADVERT	203.0.113.0/24

336577

上の図では、IPv4 プレフィックス 192.168.50.0/24 がリモート CE101 から PE1 上の VRF RED にアドバタイズされています。このプレフィックスは、MP-BGP VPN プレフィックスとして伝送され、PE4 上の VRF RED にインポートされます。PE4 で、BGP VRF RED テーブル内のこのプレフィックスに関して **exist-map** コマンドで設定された条件は、プレフィックス 203.0.113.0/24 を CE104 にアドバタイズする条件となり、PE4 上の VRF RED でピアのアクティブ化が実現されます。このシナリオでは、203.0.113.0/24 が VRF RED BGP テーブル内にあることを前提としています。203.0.113.0/24 がテーブルにない場合、このポリシーは無視されます。

- PE4 の BGP テーブル内に 192.168.50.0/24 が存在する場合、203.0.113.0/24 ネットワークは CE104 にアドバタイズされます。
- PE4 の BGP テーブル内に 192.168.50.0/24 が存在しない場合、203.0.113.0/24 ネットワークは CE104 にアドバタイズされません。

BGP VRF 認識条件付きアドバタイズメントの設定方法

BGP VRF 認識の条件付きアドバタイズメントの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*

4. 次のいずれか 1 つを入力します。
   - **address-family ipv4** [**unicast**] [**vrf** *vrf-name*]
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *ipv6-address*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *ipv6-address*} **activate**
7. **neighbor** {*ip-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	次のいずれか 1 つを入力します。 • **address-family ipv4** [**unicast**] [**vrf** *vrf-name*] • **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf VRFRED`	IPv4 または IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードは、IPv4 または IPv6 ユニキャスト アドレス ファミリを指定します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 または IPv6 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける Virtual Routing and Forwarding（VRF）インスタンスの名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*} **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.0.2.1 remote-as 104`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスの IPv4 または IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.0.2.1 activate`	ネイバーが IPv4 または IPv6 アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} 例： `Device(config-router-af)# neighbor 192.0.2.1 advertise-map ADV-1 exist-map EXIST-1`	ネイバーに対する条件付きアドバタイズメントを有効にし、**exist** または **non-exist** マップで定義された基準に基づいて、**advertise-map** コマンドによってマッピングされたプレフィックスのアドバタイズを許可します。 • **advertise-map** *map-name* キーワードと引数のペアは、アドバタイズするルートの定義に使用するルート マップの名前を指定します。 • **exist-map** *map-name* キーワードと引数のペアは、BGP テーブル内の一連のルートが満たす必要がある条件を指定します。条件を満たしている場合、**advertise map** で指定されたルートに一致する BGP テーブル内のルートがアドバタイズされます。**exist-map** で指定されたルートに一致するルートが BGP テーブル内に存在しない場合、ルートはアドバタイズされません。 • **non-exist-map** *map-name* キーワードと引数のペアは、BGP テーブル内の一連のルートと比較する条件を指定します。**non-exist-map** のルートが BGP テーブル内に存在しない場合、**advertise map** で指定されたルートに一致するルートがアドバタイズされます。**non-exist-map** で指定されたルートに一致するルートが BGP テーブル内に存在する場合、**advertise-map** に一致するルートはアドバタイズされません。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

次のタスク

BGP VRF 認識の条件付きアドバタイズメント機能の設定を確認するには、**show bgp ip neighbors** コマンドを使用します。

BGP VRF 認識条件付きアドバタイズメントの設定例

例：BGP VRF 認識の条件付きアドバタイズメントの設定

次の例では、図 1 の設定を使用します。

CE 101：プレフィックスの送信元

```
router bgp 101
 bgp log-neighbor-changes
 timers bgp 0 0
 neighbor 172.16.1.2 remote-as 65000
 !
 address-family ipv4
  network 21.21.21.0 mask 255.255.255.0
  network 22.22.22.22 mask 255.255.255.255
  network 31.0.0.0
  network 33.0.0.0
  network 44.0.0.0
  network 192.0.254 mask 255.255.255.0
  network 192.0.2.50
  neighbor 172.16.1.3 activate
 exit-address-family
```

PE 1

```
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 timers bgp 0 0
 neighbor 10.0.0.2 remote-as 65000
 neighbor 10.0.0.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf blue
  neighbor 198.51.100.10 remote-as 201
  neighbor 198.51.100.10 activate
 exit-address-family
 !
 address-family ipv4 vrf red
  neighbor 172.16.1.2 remote-as 101
  neighbor 172.16.1.2 activate
 exit-address-family
```

PE 4

```
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
```

```
 timers bgp 0 0
 neighbor 10.0.0.2 remote-as 65000
 neighbor 10.0.0.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf blue
  neighbor 198.51.100.12 remote-as 204
  neighbor 198.51.100.12 activate
 exit-address-family
 !
 address-family ipv4 vrf red
  neighbor 198.51.100.3 remote-as 104
  neighbor 198.51.100.3 activate
  neighbor 198.51.100.3 advertise-map ADV-1 exist-map EXIST-1
  neighbor 198.51.100.3 advertise-map ADV-2 exist-map EXIST-2
  neighbor 198.51.100.3 advertise-map ADV-3 exist-map EXIST-3
  neighbor 198.51.100.3 advertise-map ADV-4 exist-map EXIST-4
 exit-address-family
!
ip prefix-list pl-adv-1 seq 5 permit 22.22.22.22/32
!
ip prefix-list pl-adv-2 seq 5 permit 44.0.0.0/8 □
!
ip prefix-list pl-adv-3 seq 5 permit 33.0.0.0/8
!
ip prefix-list pl-adv-4 seq 5 permit 128.16.16.0/24
!
ip prefix-list pl-exist-1 seq 5 permit 21.21.21.0/24
!
ip prefix-list pl-exist-2 seq 5 permit 41.0.0.0/8 □
!
ip prefix-list pl-exist-3 seq 5 permit 31.0.0.0/8
!
ip prefix-list pl-exist-4 seq 5 permit 192.168.50.0/24
!
route-map EXIST-4 permit 10
 match ip address prefix-list pl-exist-4
!
route-map ADV-4 permit 10
 match ip address prefix-list pl-adv-4
!
route-map EXIST-2 permit 10
 match ip address prefix-list pl-exist-2
!
route-map ADV-2 permit 10
 match ip address prefix-list pl-adv-2
!
route-map EXIST-3 permit 10
 match ip address prefix-list pl-exist-3
!
route-map ADV-3 permit 10
 match ip address prefix-list pl-adv-3
!
route-map EXIST-1 permit 10
 match ip address prefix-list pl-exist-1
!
```

```
route-map ADV-1 permit 10
 match ip address prefix-list pl-adv-1
```

例：BGP VRF 認識の条件付きアドバタイズメントの確認

次の例では、図 1 の設定を使用します。

CE 101

```
CE101# show ip bgp all

For address family: IPv4 Unicast
BGP table version is 28, local router ID is 203.0.113.11
     Network          Next Hop            Metric LocPrf Weight Path
 *>  21.21.21.0/24     0.0.0.0                  0         32768 i
 *>  22.22.22.22/32    0.0.0.0                  0         32768 i
 *>  31.0.0.0          0.0.0.0                  0         32768 i
 *>  33.0.0.0          0.0.0.0                  0         32768 i
 *>  44.0.0.0          0.0.0.0                  0         32768 i
 *>  192.0.2.254/24    0.0.0.0                  0         32768 i
 *>  192.0.2.50        0.0.0.0                  0         32768 i
```

PE 1

```
PE1# show ip bgp all

For address family: IPv4 Unicast


For address family: VPNv4 Unicast

BGP table version is 46, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf red)
 *>  21.21.21.0/24    172.16.1.2               0             0 101 i
 *>  22.22.22.22/32   172.16.1.2               0             0 101 i
 *>  31.0.0.0         172.16.1.2               0             0 101 i
 *>  33.0.0.0         172.16.1.2               0             0 101 i
 *>  44.0.0.0         172.16.1.2               0             0 101 i
 *>  192.0.2.254/24   172.16.1.2               0             0 101 i
 *>  192.0.2.50       172.16.1.2               0             0 101 i
```

PE 4

（注） アドバタイズの条件が満たされていないため、exist-map EXIST-2 の状態は Withdraw になります。

```
PE4# show ip bgp all
```

```
For address family: VPNv4 Unicast

BGP table version is 82, local router ID is 10.0.0.4

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf red)
 *>i 21.21.21.0/24    10.0.0.1                 0    100      0 101 i
 *>i 22.22.22.22/32   10.0.0.1                 0    100      0 101 i
 *>i 31.0.0.0         10.0.0.1                 0    100      0 101 i
 *>i 33.0.0.0         10.0.0.1                 0    100      0 101 i
 *>i 44.0.0.0         10.0.0.1                 0    100      0 101 I     <- missing
41.0.0.0/8
 *>i 192.0.2.254/24   10.0.0.1                 0    100      0 101 i
 *>i 192.0.2.50       10.0.0.1                 0    100      0 101 i


PE4# show ip bgp vpnv4 all neighbors 198.51.100.3
…
…
 For address family: VPNv4 Unicast
  Translates address family IPv4 Unicast for VRF red
  Session: 198.51.100.3
  BGP table version 48, neighbor version 48/0
  Output queue size : 0
  Index 3, Advertise bit 0
  3 update-group member
  Condition-map EXIST-1, Advertise-map ADV-1, status: Advertise
  Condition-map EXIST-2, Advertise-map ADV-2, status: Withdraw
  Condition-map EXIST-3, Advertise-map ADV-3, status: Advertise
  Condition-map EXIST-4, Advertise-map ADV-4, status: Advertise
  Slow-peer detection is disabled
  …
…
PE4#


PE4# show ip bgp vpnv4 all update-group

…
…
BGP version 4 update-group 3, external, Address Family: VPNv4 Unicast
  BGP Update version : 48/0, messages 0
  Condition-map EXIST-1, Advertise-map ADV-1, status: Advertise
  Condition-map EXIST-2, Advertise-map ADV-2, status: Withdraw
  Condition-map EXIST-3, Advertise-map ADV-3, status: Advertise
  Condition-map EXIST-4, Advertise-map ADV-4, status: Advertise
  Topology: red, highest version: 47, tail marker: 47
  Format state: Current working (OK, last not in list)
                Refresh blocked (not in list, last not in list)
  Update messages formatted 4, replicated 4, current 0, refresh 0, limit 1000
  Number of NLRIs in the update sent: max 3, min 0
  Minimum time between advertisement runs is 0 seconds
  Has 1 member:
   198.51.100.3
```

CE 104

（注） CE 104 へのアドバタイズをトリガーする PE 4 では 41.0.0.0/8 が表示されないため、プレフィックス 44.0.0.0 は見つかりません。状態は Withdraw になります。

```
CE104# show ip bgp all

For address family: IPv4 Unicast

BGP table version is 45, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  21.21.21.0/24    104.0.0.1                0      65000 101     i
 *>  22.22.22.22/32   104.0.0.1                0      65000 101     i
 *>  31.0.0.0         104.0.0.1                0      65000 101     i
 *>  33.0.0.0         104.0.0.1                0      65000 101     i
 *>  192.0.2.254/24   104.0.0.1                0      65000 101     i
 *>  192.0.2.50       104.0.0.1                0      65000 101     i
```

BGP VRF 認識の条件付きアドバタイズメントの追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

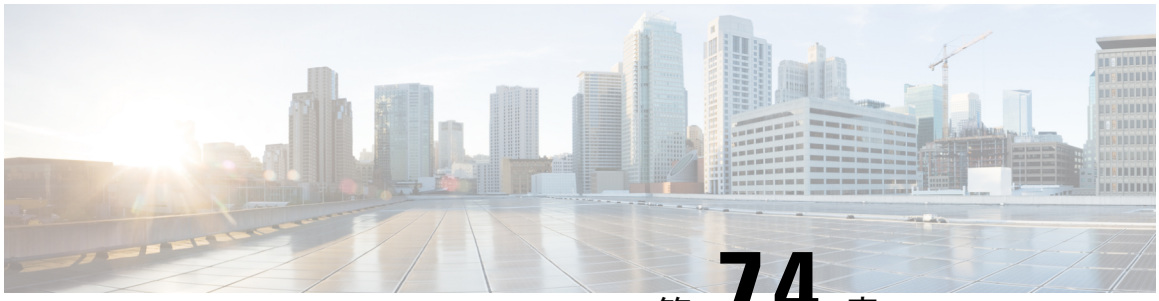
BGP VRF 認識の条件付きアドバタイズメントの機能情報

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 *93 : BGP VRF* 認識の条件付きアドバタイズメントの機能情報

機能名	リリース	機能情報
BGP VRF 認識の条件付きアドバタイズメント		ボーダー ゲートウェイ プロトコル（BGP）VRF 認識の条件付きアドバタイズメント機能は、ルート アドバタイズメントの制御を拡充し、この制御を Virtual Routing and Forwarding（VRF）インスタンス内に拡張します。



第 74 章

BGP—選択的なルート ダウンロード

BGP—選択的なルート ダウンロード機能により、ネットワーク管理者は、BGP ルートをルーティング情報ベース（RIB）に選択的に（一部を選択することも何も選択しないことも可能）ダウンロードできます。この機能の主な用途は、中継トラフィックの伝送なしに BGP アップデートを伝播する専用ルート リフレクタで RIB または Forwarding Information Base（FIB; 転送情報ベース）に特定の BGP ルートが不必要にダウンロードされるのを防ぐことです。したがって、この機能は、利用可能なリソースの最大化、および専用ルート リフレクタでのルーティングの拡張性やコンバージェンスの向上に役立ちます。

- 機能情報の確認 （1195 ページ）
- BGP—選択的ルート ダウンロードに関する情報 （1196 ページ）
- BGP ルートを選択的にダウンロードする方法 （1197 ページ）
- BGP—選択的ルート ダウンロードの設定例 （1200 ページ）
- 選択的なルート ダウンロードの追加情報 （1202 ページ）
- 選択的なルート ダウンロードの機能情報 （1202 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—選択的ルート ダウンロードに関する情報

専用ルート リフレクタには一部のルートしか必要ない

専用ルート リフレクタ（RR）の役割は、中継トラフィックの実際の転送には参加せずに BGP アップデートを伝播することです。つまり、RR では、必ずしもすべての BGP ルートを RIB または FIB にダウンロードする必要はありません。そのようなルートを処理および保存しないと、RR でリソースを節約できるため便利です。

デフォルトでは、BGP ルートは RIB にダウンロードされます。専用ルート リフレクタでリソースを節約するには、テーブル マップを設定して、このようなダウンロードを低減または防止する必要があります。テーブル マップという名前は、何を BGP ルーティング テーブルに挿入するかを制御するその機能に由来します。

ここでは、テーブル マップは、ルートのダウンロードを制御するルート マップを指します。テーブル マップは、BGP ポリシー アカウンティング出力インターフェイス アカウンティングなど、他の機能で使用できます。

table-map コマンドでの **filter** キーワードの使用法について理解することが重要です。

- **table-map** コマンドを **filter** キーワードなしで使用した場合は、**table-map** コマンドで参照されているルートマップを使用して、RIB にインストールするためにルートの特定のプロパティ（トラフィック インデックスなど）が設定されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
- **table-map** コマンドを **filter** キーワードありで使用した場合は、参照されているルートマップを使用して、BGP ルートを RIB にダウンロードするかどうかが制御されます（つまり、フィルタ）。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。

マルチプロトコル ラベル スイッチング（MPLS）レイヤ 3 VPN については、ルートのダウンロードはルート リフレクタであらかじめ自動的に抑止されるため、選択的なルート ダウンロード機能は適用されないことに注意してください。

選択的なルート ダウンロードの利点

BGP—選択的なルート ダウンロード機能により、ネットワーク管理者は、BGP ルートをルーティング情報ベース（RIB）に選択的に（一部を選択することも何も選択しないことも可能）ダウンロードできます。この機能の主な用途は、中継トラフィックの伝送なしに BGP アップデートを伝播する専用ルート リフレクタで RIB または Forwarding Information Base（FIB; 転送情報ベース）に特定の BGP ルートが不必要にダウンロードされるのを防ぐことです。したがって、この機能は、利用可能なリソースの最大化、および専用ルート リフレクタでのルーティングの拡張性やコンバージェンスの向上に役立ちます。

BGP ルートを選択的にダウンロードする方法

専用 RR でのすべての BGP ルートのダウンロード抑止

どのBGPルートもRIBにダウンロードされないようにしてリソースを節約するには、専用ルート リフレクタ（RR）でこの作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *route-map-name* **deny** [*sequence-number*]
4. **exit**
5. **router bgp** *as-number*
6. **address-family ipv4 unicast**
7. **table-map** *route-map-name* **filter**
8. **end**
9. **clear ip bgp ipv4 unicast table-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**route-map** *route-map-name* **deny** [*sequence-number*] 例： `Router(config)# route-map bgp-to-rib deny 10`	ルート マップ コンフィギュレーション モードを開始して、ルート マップを設定します。 • この例では、bgp-to-rib という名前のルート マップですべてのルートを拒否します。
ステップ 4	**exit** 例： `Router(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、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 5	**router bgp** *as-number* 例： `Router(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 6	**address-family ipv4 unicast** 例： `Router(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。
ステップ 7	**table-map** *route-map-name* **filter** 例： `Router(config-router-af)# table-map bgp-to-rib filter`	BGP ルーティング テーブル（ルーティング情報ベース（RIB））に挿入する項目をフィルタ処理するルート マップを指定します。 • ルート マップで許可されているルートが RIB にダウンロードされます。 • ルート マップで拒否されているルートは、RIB から除外されます（ダウンロードされない）。
ステップ 8	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 9	**clear ip bgp ipv4 unicast table-map** 例： `Router# clear ip bgp ipv4 unicast table-map`	テーブル マップまたはルート マップを設定または変更した後に、変更を有効にするには、BGP RIB をリロードします。

専用 RR での BGP ルートの選択的なダウンロード

BGP ルートを RIB に選択的にダウンロードするには、専用ルート リフレクタ（RR）でこの作業を実行します。BGP で外部接続ルートを伝送する場合は、RR でのネクスト ホップ解決のためにこれらのルートを RIB にダウンロードする必要があります。選択的なルート ダウンロードを実現するスケーラブルなアプローチの 1 つは、BGP コミュニティを使用して外部接続ルートを識別することです。つまり、ASBR で外部接続ルートの再配布時に特定の BGP コミュニティを付加し、その後、RR でその BGP コミュニティに基づいてルートのダウンロードをフィルタ処理します。この作業では、RR でルート マップによってコミュニティ リストを照合してダウンロードするルートを制御するための設定を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip community-list** *standard-list-number* **permit** *AA*:*NN*

4. **route-map** *route-map-name* **permit** [*sequence-number*]
5. **match community** *standard-list-number*
6. **exit**
7. **router bgp** *as-number*
8. **address-family ipv4 unicast**
9. **table-map** *route-map-name* **filter**
10. **end**
11. **clear ip bgp ipv4 unicast table-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip community-list** *standard-list-number* **permit** *AA*:*NN* 例： `Router(config)# ip community-list 100 permit 65510:100`	標準のコミュニティ リストを作成し、コミュニティ リストで許可される自律システムおよびネットワーク番号を指定します。
ステップ 4	**route-map** *route-map-name* **permit** [*sequence-number*] 例： `Router(config)# route-map bgp-to-rib permit 10`	ルート マップ コンフィギュレーション モードを開始して、ルート マップを設定します。 • bgp-to-rib という名前のルート マップにより、次の手順で指定するコミュニティ リストに一致するルートを許可します。
ステップ 5	**match community** *standard-list-number* 例： `Router(config-route-map)# match community 100`	コミュニティ リスト 100 で許可されているルートと照合します。
ステップ 6	**exit** 例： `Router(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、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 7	**router bgp** *as-number* 例：	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
	`Router(config)# router bgp 65510`	
ステップ 8	**address-family ipv4 unicast** 例： `Router(config-router)# address-family ipv4 unicast`	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、アドレス ファミリ固有の設定を受け入れるように BGP ピアを設定します。
ステップ 9	**table-map** *route-map-name* **filter** 例： `Router(config-router-af)# table-map bgp-to-rib filter`	BGP ルーティング テーブル（ルーティング情報ベース（RIB））に挿入する項目をフィルタ処理するルート マップを指定します。
ステップ 10	**end** 例： `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 11	**clear ip bgp ipv4 unicast table-map** 例： `Router# clear ip bgp ipv4 unicast table-map`	テーブル マップまたはルート マップを設定または変更した後に、変更を有効にするには、BGP RIB をリロードします。

BGP—選択的ルート ダウンロードの設定例

例：選択的なルート ダウンロード

専用ルート リフレクタ（RR）の役割は、中継トラフィックの実際の転送には参加せずに BGP アップデートを伝播することです。場合によっては、専用 RR で、選択したルートのみをダウンロードすることや、どのルートもダウンロードしないことが必要になります。

たとえば、IS-IS ルーティング プロトコルが使用されている場合に専用 RR で過負荷ビットを設定したり、OSPF が使用されている場合に OSPF スタブ ルータを設定したりすることが考えられます。

例：ネクスト ホップがループバック アドレスの場合—すべてのルートをダウンロードから除外する

この例では、**next-hop-self** コマンドで iBGP セッションに対して ASBR が設定されています（この設定は示されていません）。iBGP セッションにアドバタイズされる BGP ルートのネクスト ホップは、IGP（OSPF または IS-IS）で伝送されるループバック アドレスです。どの BGP ルー

トも RIB にダウンロードする必要はありません。専用 RR の次の設定では、**table map** コマンドに **filter** キーワードが含まれているため、すべての BGP ルートのダウンロードが抑止され、テーブル マップで参照しているルート マップによってすべてのルートが拒否されます。

```
route-map bgp-to-rib deny 10
!
router bgp 65000
 address-family ipv6 unicast
 table-map bgp-to-rib filter
```

例：IGP での接続ルートの再配布—すべてのルートをダウンロードから除外する

この例では、BGP ルートのネクスト ホップは、プレフィックス リストに基づく接続ルートの選択的再配布を介して、OSPF や IS-IS などの IGP で伝送される外部接続ルートで解決されます。ルートは iBGP から受信されます。

このシナリオは前の例とは異なりますが、設定は同じです。専用 RR の次の設定では、**table map** コマンドに **filter** キーワードが含まれているため、すべての BGP ルートのダウンロードが抑止され、テーブル マップで参照しているルート マップによってすべてのルートが拒否されます。

```
route-map bgp-to-rib deny 10
!
router bgp 65000
 address-family ipv6 unicast
 table-map bgp-to-rib filter
```

例：BGP での接続ルートの再配布—一部のルートをダウンロードから除外する

BGP で外部接続ルートを伝送する場合は、RR でのネクスト ホップ解決を計算できるように、これらのルートを RIB にダウンロードする必要があります。選択的なルート ダウンロードを実現するスケーラブルな方法の 1 つは、ASBR で BGP コミュニティを使用してこれらの外部接続ルートを識別することです。つまり、境界ルータで、外部接続ルートの再配布時に特定の BGP コミュニティを付加し、その後、RR でその BGP コミュニティに基づいてルートのダウンロードをフィルタ処理します。次に、ASBR の設定と RR の設定を示します。

ASBR の設定

```
router bgp 65510
 address-family ipv4 unicast
 redistribute connected route-map connected-to-bgp
!
route-map connected-to-bgp permit 10
 match ip address prefix-list extend-connected
 set community 65510:100
!
ip prefix-list extend-connected permit 192.168.1.1/30
```

RR の設定

```
ip community-list 100 permit 65510:100
```

```
!
route-map bgp-to-rib permit 10
 match community 100
!
router bgp 65510
 address-family ipv4 unicast
 table-map bgp-to-rib filter
```

選択的なルート ダウンロードの追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

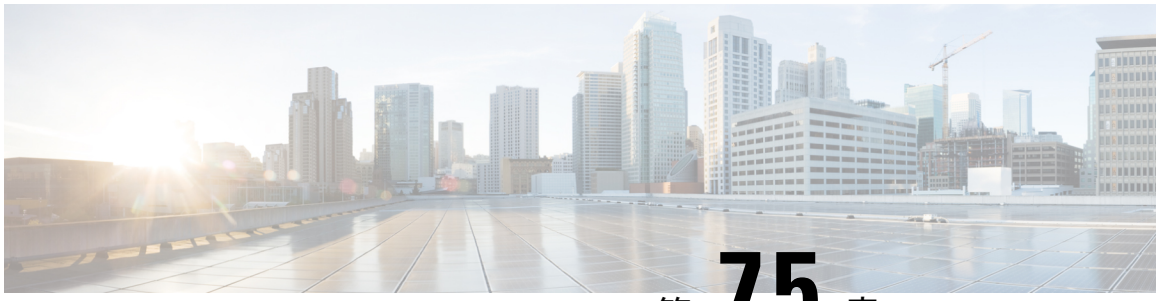
選択的なルート ダウンロードの機能情報

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 *94 :* 選択的なルート ダウンロードの機能情報

機能名	リリース	機能情報
選択的なルート ダウンロード	Cisco IOS XE リリース 2.3S	BGP—選択的なルート ダウンロード機能により、ネットワーク管理者は、BGP ルートをルーティング情報ベース（RIB）に選択的に（一部を選択することも何も選択しないことも可能）ダウンロードできます。この機能の主な用途は、中継トラフィックの伝送なしに BGP アップデートを伝播する専用ルート リフレクタで RIB または Forwarding Information Base（FIB; 転送情報ベース）に特定の BGP ルートが不必要にダウンロードされるのを防ぐことです。したがって、この機能は、利用可能なリソースの最大化、および専用ルート リフレクタでのルーティングの拡張性やコンバージェンスの向上に役立ちます。 次のコマンドが変更されました。 • **table-map**



第 75 章

iBGP ローカル AS に対する BGP サポート

iBGP ローカル AS に対する BGP サポート機能が導入される前は、eBGP ネイバーに対してネゴシエートされる AS を変更するため、および送受信される AS_PATH を変更するために、BGP スピーカーで **neighbor local-as** コマンドを使用していました。現在では、**neighbor local-as** コマンドを使用して、iBGP セッションで同じ操作を実行できます。AS ネゴシエーションによって iBGP セッションが作成された後、このセッションで iBGP 属性（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_LIST）を送信し、このセッションから iBGP 属性を受信して受け入れることができます。この機能は、2 つの自律システムを 1 つに結合する場合に便利です。

- 機能情報の確認 （1205 ページ）
- iBGP ローカル AS に対するサポートの制約事項 （1206 ページ）
- iBGP ローカル AS に対するサポートに関する情報 （1206 ページ）
- iBGP ローカル AS に対するサポート （1206 ページ）
- iBGP ローカル AS の利点 （1207 ページ）
- iBGP ローカル AS の設定方法 （1207 ページ）
- iBGP ローカル AS の設定 （1207 ページ）
- iBGP ローカル AS の設定例 （1210 ページ）
- 例：iBGP ローカル AS の設定 （1210 ページ）
- iBGP ローカル AS に対するサポートの追加情報 （1211 ページ）
- iBGP ローカル AS に対する BGP サポートの機能情報 （1211 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。

iBGP ローカル AS に対するサポートの制約事項

- この機能は、コンフェデレーションに属するピアではサポートされていません。
- 単一の AS 内にある非ローカル AS iBGP ネイバーは、iBGP ローカル AS 機能を使用して設定されている iBGP ネイバーとは別のアップデート グループに配置されます。
- 2 つの異なる自律システム内にあり、iBGP ローカル AS ネイバーとして設定されている 2 つの iBGP ネイバーは、別々のアップデート グループに配置されます。

iBGP ローカル AS に対するサポートに関する情報

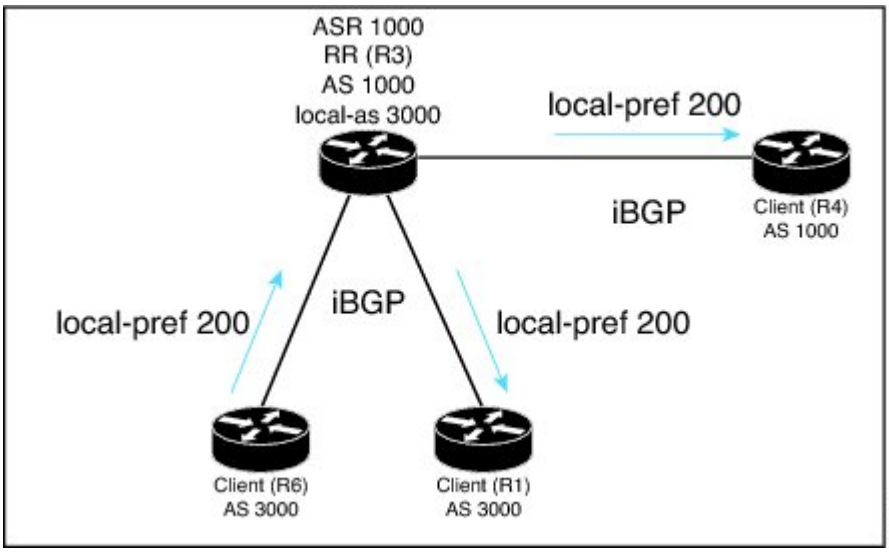
iBGP ローカル AS に対するサポート

iBGP ローカル AS に対するサポート機能が導入される前は、同じ AS 番号を指定した **neighbor local-as** コマンドと **neighbor remote-as** コマンドを使用してピア（またはピア グループ）が設定されている場合、セッションは iBGP セッションとしてネゴシエートされていました（この動作は、両方の OPEN メッセージ内のアドバタイズされる AS が同じである場合に発生します）。しかし、アップデートは eBGP セッション内として伝播されるため（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_LIST は伝播されません）、このセッションで受信するとエラーが発生する可能性がありました。つまり、iBGP ローカル AS は完全にはサポートされていませんでした。

iBGP ローカル AS に対するサポート機能では、これらの iBGP 属性がすべて伝播されます。また、どの iBGP セッション内でも、AS は、iBGP ローカル AS セッションへのルートのアドバタイズ時に AS_PATH 属性の前に付加されません。

下の図に、この機能を使用して 2 つの自律システムの結合を促進するシナリオを示します。ルート リフレクタ R3 と R4 は AS 1000 に属しています。R1 と R6 は AS 3000 に属しています。RR は、**neighbor local-as 3000** および **neighbor remote-as 3000** コマンドを使用して設定されています。2 つの異なる自律システムにルータが属していても、LOCAL_PREF などの属性は、R6 から R4 へのアップデートおよび R6 から R1 へのアップデート（図を参照）で保持され、同様に R4 から R1 へのアップデートおよび R4 から R6 へのアップデート（図には非表示）でも保持されます。

図 *93 : iBGP* ローカル *AS* に対するサポートによる *2* つの自律システム間での *iBGP* ポリシーの保持



iBGP ローカル AS の利点

この機能は、異なる自律システム番号を持つ 2 つの ISP を結合する場合に使用します。他の自律システムに伝播されるルートで内部と見なされる属性（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_LIST）は保持することが望ましい動作となります。

iBGP ローカル AS の設定方法

iBGP ローカル AS の設定

特定のネイバーに対して BGP スピーカーで iBGP ローカル AS 機能を設定すると、そのセッションを完全な iBGP セッションとして動作させることができます。この設定は、通常はルート リフレクタ上で実行しますが、それに限定されるものではありません。ルート リフレクタでは、必要に応じ、**allow-policy** コマンドによってネイバーに送信される iBGP 属性を変更するように設定できます（このコマンドはこの機能専用ではなく、どの RR でも使用できます）。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **router bgp** *autonomous-system-number*
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **remote-as** *as-number*
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **local-as** *as-number*
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **route-reflector-client**
10. **address-family vpnv4**
11. **neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **allow-policy**
12. **exit**
13. **address-family vpnv6**
14. **neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **allow-policy**
15. **end**
16. **show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*} **policy**
17. **show ip bgp vpnv4 all update-group** *update-group*
18. **show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 1000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-router)# neighbor rr-client-ab peer-group`	（任意）ピア グループを識別します。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name* 例： `Device(config-router)# neighbor 192.168.3.3 peer-group rr-client-ab`	（任意）ピア グループのメンバになるように BGP ネイバーを設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **remote-as** *as-number*	ネイバーまたはピア グループの AS を識別します。

	コマンドまたはアクション	目的
	例： `Device(config-router)# neighbor rr-client-ab remote-as 3000`	
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **local-as** *as-number* 例： `Device(config-router)# neighbor rr-client-ab local-as 3000`	ネイバーまたはピア グループのローカル AS 機能を設定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **route-reflector-client** 例： `Device(config-router)# neighbor rr-client-ab route-reflector-client`	ローカル デバイスをルート リフレクタとして設定し、そのクライアントになるようにネイバーまたはピア グループを設定します。
ステップ 10	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	（任意）ルータを VPNv4 アドレス ファミリ コンフィギュレーション モードにします。
ステップ 11	**neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **allow-policy** 例： `Device(config-router-af)# neighbor rr-client-ab allow-policy`	（任意）指定したネイバーまたはピア グループの iBGP 属性を変更するように RR を設定できるようにします。
ステップ 12	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了して、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 13	**address-family vpnv6** 例： `Device(config-router)# address-family vpnv6`	（任意）ルータを VPNv6 アドレス ファミリ コンフィギュレーション モードにします。
ステップ 14	**neighbor** {*ip-address* | *ipv6-address* | *peer-group*} **allow-policy** 例： `Device(config-router-af)# neighbor rr-client-ab allow-policy`	（任意）指定したネイバーまたはピア グループの iBGP 属性を変更するように RR を設定できるようにします。
ステップ 15	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 16	**show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*} **policy** 例： `Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy`	（任意）ネイバーのローカルに設定されたポリシーを表示します。 • **neighbor allow-policy** コマンドがそのネイバーに対して設定されている場合は、「allow-policy」という語句が出力に表示されます。
ステップ 17	**show ip bgp vpnv4 all update-group** *update-group* 例： `Device# show ip bgp vpnv4 all update-group 2`	（任意）アップデート グループの情報を表示します。 • **neighbor allow-policy** コマンドがアップデート グループのネイバーに対して設定されている場合は、「allow-policy」という語句が出力に表示されます。
ステップ 18	**show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*} 例： `Device# show ip bgp vpnv4 all neighbors 192.168.3.3`	（任意）ネイバーに関する情報を表示します。 • リモート AS とローカル AS が出力に表示され、iBGP ローカル AS に対するサポート機能が設定されている場合には同じ AS 番号が示されます。

iBGP ローカル AS の設定例

例：iBGP ローカル AS の設定

この例では、AS 2500 のピア グループ rr-client-2 との BGP セッションを iBGP セッションとして処理するように、AS 4000 のルート リフレクタ（RR）を設定します。つまり、iBGP 属性（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_LIST）は、このピア グループに属するネイバーとの間のアドバタイズメントでルートからドロップされません。属性は変更されずに渡されます。AS 2500 は、ピア グループとの間のルートの AS_PATH 属性の前に付加されません。

また、 **neighbor allow-policy** コマンドにより、ネットワーク管理者が RR で iBGP ポリシーを設定できるように設定します。つまり、ダウンストリーム ピアに送信される属性を変更するように発信ルート マップを設定できます。この例では、このコマンドは VPNv4 および VPNv6 アドレス ファミリに適用されます。

```
router bgp 4000
 neighbor rr-client-2 peer-group
 neighbor 192.168.1.1 peer-group rr-client-2
 neighbor 192.168.4.1 peer-group rr-client-2
 neighbor rr-client-2 remote-as 2500
 neighbor rr-client-2 local-as 2500
```

```
 neighbor rr-client-2 route-reflector-client
 address-family vpnv4
  neighbor rr-client-2 allow-policy
!
 address-family vpnv6
  neighbor rr-client-2 allow-policy
```

iBGP ローカル AS に対するサポートの追加情報

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 Commands List, All Releases』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
自律システムの移行	『*IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S*』の「BGP Support for Dual AS Configuration for Network AS Migrations」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

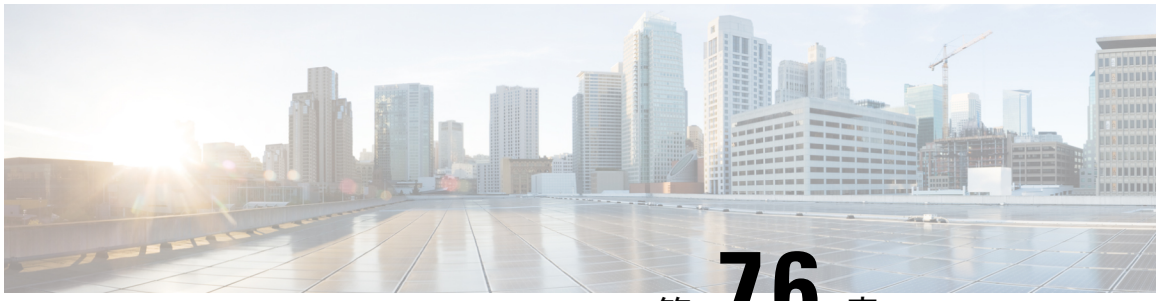
iBGP ローカル AS に対する BGP サポートの機能情報

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 *95 : iBGP* ローカル *AS* に対する *BGP* サポートの機能情報

機能名	リリース	機能情報
iBGP ローカル AS に対する BGP サポート		ローカル AS に対する BGP サポート機能が提供される前は、ルートリフレクタで **neighbor local-as** コマンドを使用して、eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズしていました。現在は、**neighbor local-as** コマンドを使用して、iBGP ローカル AS セッションでの iBGP 属性（LOCAL_PREF、ORIGINATOR_ID、CLUSTER_ID、CLUSTER_LIST）の送信を有効にすることができます。この機能は、ルートで iBGP 属性を保持することが有効な場合に、2 つの自律システムをマージするのに役立ちます。 iBGP ローカル AS に対する BGP サポート機能が提供される前は、iBGP 属性を変更するように RR を設定することはできませんでした。この機能の導入により、iBGP 属性を変更するように RR を設定できるため、柔軟性が向上します。 次のコマンドが導入されました。 • **neighbor allow-policy** 次のコマンドが変更されました。 • **neighbor local-as** • **show ip bgp vpnv4**



第 76 章

非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）

非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）機能により、ネイティブ IPv4 および IPv6 の外部ボーダー ゲートウェイ プロトコル（eBGP）パスと内部 BGP（iBGP）パスの間でマルチパス ロード シェアリングを設定して、展開環境でのロード バランシングを改善できます。このモジュールでは、その機能および設定方法について説明します。

- 機能情報の確認 （1213 ページ）
- 非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）に関する情報 （1214 ページ）
- 非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の設定方法 （1214 ページ）
- 非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の設定例 （1215 ページ）
- 非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）の機能情報 （1216 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。

非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）に関する情報

非 VRF インターフェイスの eiBGP マルチパスの概要

ボーダー ゲートウェイ プロトコル（BGP）パス選択アルゴリズムでは、内部 BGP（iBGP）パスよりも外部 BGP（eBGP）パスが優先されます。非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）機能では、このアルゴリズムが、ネイティブ IPv4 および IPv6 の eBGP パスと iBGP パスの間でマルチパス ロード シェアリングを実現できるように変更されます。非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）機能が導入される前は、この機能は VPN ルーティングおよび転送（VRF）インスタンスでしか使用できませんでした。この機能の導入により、非 VRF インターフェイスに機能が拡張されています。**maximum-paths** コマンドを使用すると、マルチパス ロード シェアリングのために複数のパスをルーティング情報ベース（RIB）にインストールするように BGP を設定できます。BGP ベスト パス アルゴリズムでは、1 つのマルチパスをベスト パスとして選択し、そのパスを BGP ピアにアドバタイズします。その他のマルチパスは BGP テーブルと RIB の両方に挿入され、これらのマルチパスが Cisco Express Forwarding でロード バランシングを実行するために使用されます（ロード バランシングは、パケット単位で、または送信元単位か宛先単位で実行されます）。

この機能は、顧客のプロバイダー エッジ（PE）デバイスで設定できます。ただし、この機能は、顧客サイトにある 1 つの PE デバイスでのみ設定する必要があります。この機能を複数の PE デバイスで設定すると、トラフィックの一部が顧客サイトの PE デバイス間でループすることがあります。したがって、トラフィック ループを避けるために、機能を適切にセットアップすることが重要となります。この機能は、デフォルトでイネーブルにされています。

非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）の設定方法

非 VRF インターフェイスでの IPv4/IPv6 マルチパスの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. 次のいずれか 1 つを入力します。
   - **address-family ipv4 unicast**
   - **address-family ipv6 unicast**

5. **maximum-paths eibgp** *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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 64496`	ルータ コンフィギュレーション モードを開始して、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを作成または設定します。

ステップ 4	次のいずれか 1 つを入力します。
	• **address-family ipv4 unicast**
	• **address-family ipv6 unicast**
	例：
	`Device(config-router)# address-family ipv4 unicast`
	`Device(config-router)# address-family ipv6 unicast`
		IPv4 または IPv6 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	**maximum-paths eibgp** *number* 例： `Device(config-router-af)# maximum-paths eibgp 3`	複数の外部 BGP（eBGP）パスと内部 BGP（iBGP）パスを介してパケットを転送します。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）の設定例

例：非 VRF インターフェイスでの IPv4/IPv6 マルチパスの有効化

次の例は、非 VRF インターフェイスで IPv4 マルチパスを有効にする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 64496
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# maximum-paths eibgp 4
Device(config-router-af)# end
```

次の例は、非 VRF インターフェイスで IPv6 マルチパスを有効にする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 64497
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# maximum-paths eibgp 4
Device(config-router-af)# end
```

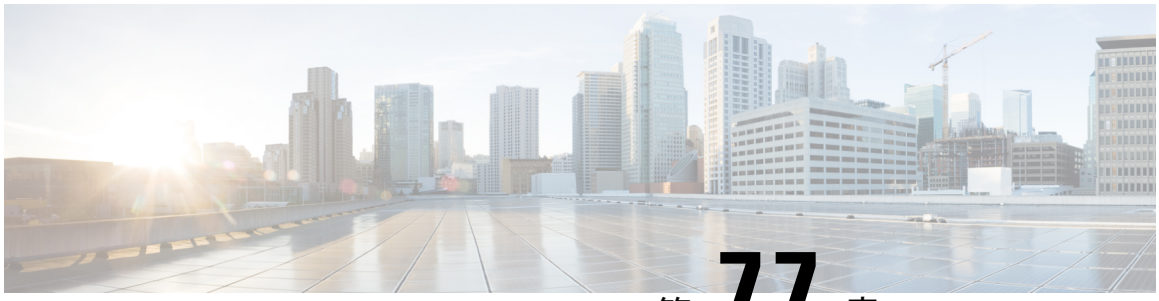
非VRFインターフェイスのeiBGPマルチパス（IPv4/IPv6）の機能情報

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 *96 :* 非 *VRF* インターフェイスの *eiBGP* マルチパス（*IPv4/IPv6*）の機能情報

機能名	リリース	機能情報
非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）		非 VRF インターフェイスの eiBGP マルチパス（IPv4/IPv6）機能により、ネイティブ IPv4 および IPv6 の外部ボーダー ゲートウェイ プロトコル（eBGP）パスと内部 BGP（iBGP）パスの間でマルチパス ロード シェアリングを設定して、展開環境でのロード バランシングを改善できます。 **maximum-paths eibgp** コマンドが変更されました。



第 77 章

L3VPN iBGP PE-CE

L3VPN iBGP PE-CE機能では、プロバイダーエッジ（PE）デバイスとカスタマーエッジ（CE）デバイスが、PE と CE 間で外部 BGP ピアリングの代わりに iBGP としてピアリングを行ってボーダー ゲートウェイ プロトコル（BGP）ルーティング情報を交換できます。

- 機能情報の確認 （1217 ページ）
- L3VPN iBGP PE-CE の制限 （1217 ページ）
- L3VPN iBGP PE-CE に関する情報 （1218 ページ）
- L3VPN iBGP PE-CE の設定方法 （1218 ページ）
- L3VPN iBGP PE-CE の設定例 （1219 ページ）
- L3VPN iBGP PE-CE の追加情報 （1219 ページ）
- L3VPN iBGP PE-CE の機能情報 （1220 ページ）

機能情報の確認

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

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

L3VPN iBGP PE-CE の制限

iBGP PE CE では soft-reconfiguration inbound または bgp soft-reconfig-backup 機能を使用しないことをお勧めします。

L3VPN iBGP PE-CE に関する情報

L3VPN iBGP PE-CE

プロバイダーエッジ（PE）またはカスタマーエッジ（CE）のルーティングプロトコルとして BGP を使用すると、VPN プロバイダー自律システム（AS）とカスタマー ネットワーク自律システム間の外部ピアリングとしてピアリング セッションが設定されます。L3VPN iBGP PE-CE 機能では、PE デバイスと CE デバイスが、PE と CE 間で広く使用されている外部 BGP ピアリングの代わりに内部ボーダーゲートウェイ プロトコル（iBGP）としてピアリングを行ってボーダーゲートウェイ プロトコル（BGP）ルーティング情報を交換できます。このメカニズムは、VRF ベースの CE が iBGP として設定されている各 PE デバイスで適用されます。これにより、サービス プロバイダー（SP）は、CE に自律システムのオーバーライドを設定する必要がなくなります。この機能を有効にした場合は、異なる自律システムを使用した仮想プライベート ネットワーク（VPN）サイトの設定は不要です。

neighbor internal-vpn-client コマンドの導入により、PE デバイスで VPN クラウド全体を内部 VPN クライアントのように CE デバイスに対して機能させることができます。これらの CE デバイスは、VRF 内部の iBGP PE-CE 接続を通じて VPN クラウドに内部的に接続されます。この接続が確立されると、PE デバイスは CE-learned パスを ATTR_SET という属性内にカプセル化し、それを VPN コアからリモートの PE デバイスまで iBGP-sourced パスで伝送します。リモートの PE デバイスでは、この属性に個別の属性が割り当てられ、送信元 CE パスが抽出されてリモート CE デバイスに送信されます。ATTR_SET は任意の推移的属性で、 一連の BGP パス属性を伝送します。これには、送信元 CE デバイスから受信した BGP アップデート メッセージで使用される可能性がある任意の BGP 属性を含めることができます。

L3VPN iBGP PE-CE の設定方法

L3VPN iBGP PE-CE の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4 vrf** *name*
5. **neighbor** *ip-address* **internal-vpn-client**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4 vrf** *name* 例： `Device(config-router)# address-family ipv4 vrf blue`	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、VPN ルーティングおよび転送を設定します。
ステップ 5	**neighbor** *ip-address* **internal-vpn-client** 例： `Device(config-router-af)# neighbor 10.0.0.1 internal-vpn-client`	ルーティング情報を交換するネイバーデバイスを定義します。**neighbor internal-vpn-client** コマンドは VPN 属性セット内に iBGP CE ネイバー パスをスタックします。

L3VPN iBGP PE-CE の設定例

例：L3VPN iBGP PE-CE の設定

次の例は、L3VPN iBGP PE-CE の設定方法を示しています。

```
Device# enable
Device(config)# configure terminal
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 vrf blue
Device(config-router-af)# neighbor 10.0.0.1 internal-vpn-client
```

L3VPN iBGP PE-CE の追加情報

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』

関連項目	マニュアル タイトル
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

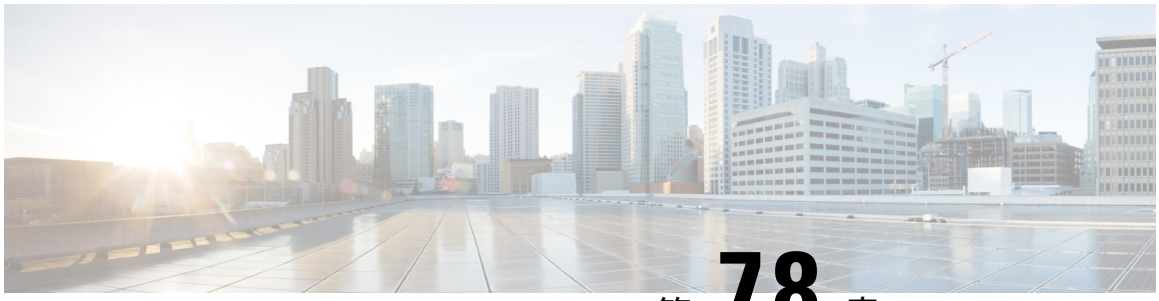
L3VPN iBGP PE-CE の機能情報

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 *97 : L3VPN iBGP PE-CE* の機能情報

機能名	リリース	機能情報
L3VPN iBGP PE-CE		L3VPN iBGP PE-CE 機能では、プロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスが、PE と CE 間で外部 BGP の代わりに iBGP としてピアリングを行ってボーダー ゲートウェイ プロトコル（BGP）ルーティング情報を交換できます。 **neighbor internal-vpn-client** コマンドが導入されました。



第 78 章

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート

ボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）は、アクティブ ルート プロセッサ（RP）からスタンバイ RP へのスイッチオーバーが発生した場合における NSR およびノンストップ フォワーディング（NSF）のサポートを提供します。BGP NSR は、IPv4 および IPv6 アドレス ファミリについて、また IPv4、IPv6、VPN バージョン 4（VPNv4）、および VPN バージョン 6（VPNv6）アドレス ファミリの PE デバイスでの内部 BGP（iBGP）ピアについて、プロバイダー エッジとカスタマー エッジの間（PE-CE）の接続をサポートします。MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート機能は、VPNv4 および VPNv6 アドレス ファミリについて、マルチプロトコル ラベル スイッチング（MPLS）相互自律システム（Inter-AS）オプション B の展開における自律システム境界ルータ（ASBR）での NSR のサポートを提供します。

このモジュールでは、VPNv4 および VPNv6 アドレス ファミリの Inter-AS オプション B の ASBR で BGP NSR サポートを有効にする方法について説明します。

- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する制約事項（1222 ページ）
- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する情報 （1222 ページ）
- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定方法 （1225 ページ）
- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定例 （1227 ページ）
- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する追加情報（1228 ページ）
- MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する機能情報（1228 ページ）

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する制約事項

- ノンストップ ルーティング（NSR）がサポートされていないアドレス ファミリでピアがアクティブ化されている場合（マルチキャスト配信ツリー（MDT）など）、および NSR がサポートされている他のアドレス ファミリ トポロジと同じセッションにアドレス ファミリ トポロジが関連付けられている場合（VPN バージョン 4（VPNv4）など）、そのピアで確立されたセッションでは NSR はサポートされません。NSR がサポートされていないアドレスファミリでのピアのアクティブ化がセッションの確立に含まれている場合、そのセッションでは NSR をサポートできません。回避策として、マルチセッションを作成し、サポート対象外のトポロジを新しいセッションの一部としてアクティブ化することができます。
- NSR はネイバー単位でのみ設定できます。
- Inter-AS オプション B の自律システム境界ルータ（ASBR）で BGP NSR サポートを有効にすると、パフォーマンスおよびメモリに影響が生じることがあります。

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する情報

BGP NSR の概要

ステートフル スイッチオーバー（SSO）によるボーダー ゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）では、高可用性（HA）ソリューションをサービス プロバイダーに提供して、BGP グレースフル リスタート（GR）をサポートしないカスタマー エッジ（CE）ルータとの外部 BGP（eBGP）ピアリング関係にプロバイダー エッジ（PE）ルータが関与できるようにします。BGP NSR は SSO と連携して、アクティブ ルート プロセッサ（RP）とスタンバイ ルート プロセッサの間で BGP 状態情報を同期します。SSO により、スイッチオーバー後にユーザがネットワークを使用できない時間が最小限になります。

BGP NSR with SSO は、BGP ピア、BGP ピア グループ、および BGP セッション テンプレート コンフィギュレーションでサポートされます。

BGP ピアおよび BGP ピア グループ コンフィギュレーションで BGP NSR with SSO サポートを設定するには、IPv4 Virtual Routing and Forwarding（VRF）アドレス ファミリ BGP ピア セッションのアドレス ファミリ コンフィギュレーション モードで **neighbor ha-mode sso** コマンドを使用します。BGP セッション テンプレートで Cisco BGP NSR with SSO のサポートを含めるには、セッション テンプレート コンフィギュレーション モードで **ha-mode sso** コマンドを使用します。

相互自律システム

BGP 自律システム（AS）は、グローバルな外部ネットワークをローカル ルーティング ポリシーが適用できる個別のルーティング ドメインに分割する場合に使用されます。個々の BGP AS は外部 BGP（eBGP）ピアリング セッションを通じて、ルーティング情報をダイナミックに交換します。同じ AS 内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

VPN の複数のサイトが別々の AS に接続されている場合、相互自律システム（Inter-AS） の展開は、異なる AS 間で VPN サービスを提供するために役立ちます。このシナリオでは、VPN に接続されているプロバイダー エッジ（PE）ルータは、iBGP 接続を互いに維持したり、共通のルート リフレクタ（RR）を使用して維持したりすることはできません。eBGP は、VPN-IPv4/IPv6 アドレスを配布するために使用します。RFC 2547bis では、次の VPN ソリューションが提示されています。

- 自律システム境界ルータ（ASBR）での Virtual Routing and Forwarding（VRF）間の接続：PE は、その AS の ASBR として機能します。ASBR は、直接接続され、複数のサブインターフェイスを介してそれらの間の VPN ルートを管理します。ASBR は、このような各インターフェイスを VRF に関連付け、eBGP を使用してラベルのない IPv4 アドレスを互いに配布します。このソリューションは「Inter-AS オプション A」とも呼ばれます。Inter-AS オプション A は、異なる AS を接続する ASBR 間の IP ベース転送を提供します。ただし、VPN 接続ごとに 1 つの BGP セッションも必要になります。Inter-AS オプション A は簡単に実装できますが、拡張性が制限されています。
- ラベル付き VPN-IPv4 ルートの eBGP 再配布：隣接する ASBR で、マルチプロトコル外部 BGP（MP-eBGP）を使用して、各 AS 内の PE から取得したラベル付き VPN-IPv4 ルートを交換します。PE ルータは、iBGP を使用して、ラベル付き VPN-IPv4 ルートを ASBR に、または ASBR がクライアントになっている RR に再配布します。このソリューションは、「Inter-AS オプション B」とも呼ばれます。Inter-AS オプション B は、異なる AS を接続する ASBR 間のマルチプロトコル ラベル スイッチング（MPLS）ベース転送を提供します。Inter-AS オプション B は、ASBR 間のすべての VPN プレフィックスを交換するために 1 つの BGP セッションしか必要としないため、Inter-AS オプション A よりも拡張性に優れています。
- ラベル付き VPN-IPv4 ルートのマルチホップ eBGP 再配布：PE は、ASBR の介在なしに、MP-eBGP を通じてラベル付き VPN IPv4 ルートを相互に直接交換します。ASBR は、MP-iBGP を通じてラベル付き IPv4 ルートを各 AS 内の PE にアドバタイズします。ASBR は、VPN-IPv4 ルートを維持することも、VPN-IPv4 ルートを相互にアドバタイズすることもありません。このソリューションは、「Inter-AS オプション C」とも呼ばれます。

MPLS VPNv4 および VPNv6 Inter-AS オプション B の概要

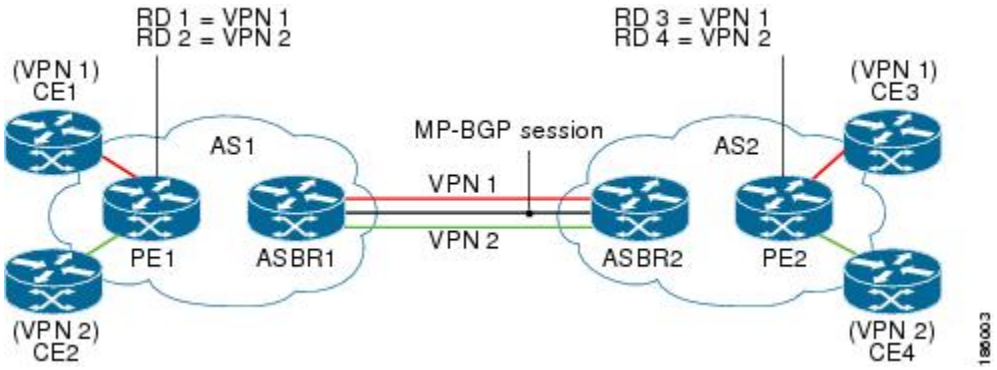
相互自律システム（Inter-AS）オプション B ソリューションでは、2 つの自律システム境界ルータ（ASBR）が、マルチプロトコル外部 BGP（MP-eBGP）を使用して、各 AS 内のプロバイダー エッジ（PE）デバイスから取得したラベル付き VPN-IPv4 ルートを交換します。ASBR 間では、マルチプロトコル ラベル スイッチング（MPLS）ベース転送が使用されます。ASBR で障害が発生した場合、ノンストップ ルーティング（NSR）またはグレースフル リスタート（GR）が

ないと、ルーティングおよび転送は影響を受けることになります。NSR により、冗長ルートプロセッサ（RP）は、ルーティング状態を保持できるようになるため、フェールオーバーが発生した場合にアクティブ RP の機能を引き継ぐことができます。ノンストップ フォワーディング（NSF）に伴い、フェールオーバー時に影響を受けずにルーティングおよび転送状態を維持できます。

下の図には、異なる VPN に属するカスタマー エッジ（CE）ルータを含む 2 つの自律システム（AS1 と AS2）が示されています。各 PE は、どのルート識別子（RD）がどの VPN に対応するかを追跡して、各 VPN に属するトラフィックを制御します。

- カスタマー エッジ 1（CE1）と CE3 は VPN 1 に属しています。
- CE2 と CE4 は VPN 2 に属しています。
- プロバイダー エッジ 1（PE1）では、VPN 1（VRF 1）にルート識別子 1（RD 1）を、VPN 2（VRF 2）に RD 2 を使用しています。
- PE2 は、VPN 1（VRF 1）に RD 3 を、VPN 2（VRF 2）に RD 4 を使用しています。

図 *94 : Inter-AS* オプション *B* でのルートのフロー



上の図に示されているような Inter-AS オプション B のシナリオでは、ルートは、MP-eBGP セッションを介して ASBR1 から AS 境界を越えて ASBR2 に伝送されます。

Inter-AS オプション B では、ルートは、次のようにアドバタイズされます。

1. AS1 の PE は、マルチプロトコル内部 BGP（MP-iBGP）を通じてラベル付き VPN-IPv4 ルートを AS1 の ASBR または ASBR のルート リフレクタ（RR）にアドバタイズします。
2. AS1 の ASBR は、MP-eBGP を通じてラベル付き VPN-IPv4 ルートを AS2 の ASBR にアドバタイズします。
3. AS2 の ASBR は、MP-iBGP を通じてラベル付き VPN-IPv4 ルートを AS2 の PE または PE の RR にアドバタイズします。

ASBR では、ラベル付き VPN IPv4 ルートに対して、ASBR 拡張方式とも呼ばれる特別な処理を実行する必要があります。

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定方法

Inter-AS オプション B の BGP NSR サポートを有効にするための ASBR の設定

相互自律システム（Inter-AS）オプション B の自律システム境界ルータ（ASBR）でのボーダーゲートウェイ プロトコル（BGP）ノンストップ ルーティング（NSR）サポートは、プロバイダーエッジ（PE）でマルチプロトコル内部 BGP（MP-iBGP）ピアに対して BGP NSR を設定する場合と同様に設定できます。設定は、ネイバーごとにグローバル ルータ モードで実行します。NSR サポートは、ネイバーがアクティブになっているすべてのアドレス ファミリに適用されます（そのネイバーがサポート対象外のアドレス ファミリでアクティブになっていない場合）。サポート対象外のアドレス ファミリでネイバーがアクティブになっている場合は、そのトポロジを、マルチセッションを使用する別のセッションの一部にする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **ha-mode sso**
6. **address-family** {**vpnv4** | **vpnv6**} [**multicast** | **unicast**]
7. **neighbor** *ip-address* **activate**
8. **end**
9. **show ip bgp vpnv4 all sso summary**
10. **show ip bgp vpnv4 neighbors** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# router bgp 400`	
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 192.168.1.1 remote-as 4000`	ネイバーの AS を指定します。
ステップ 5	**neighbor** *ip-address* **ha-mode sso** 例： `Device(config-router)# neighbor 192.168.1.1 ha-mode sso`	ステートフル スイッチオーバー（SSO）による BGP NSR をサポートするように BGP ネイバーを設定します。
ステップ 6	**address-family** {**vpnv4** | **vpnv6**} [**multicast** | **unicast**] 例： `Device(config-router)# address-family vpnv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 または VPNv6 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	指定したピアをアクティブにします。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp vpnv4 all sso summary** 例： `Device# show ip bgp vpnv4 all sso summary`	BGP NSR with SSO をサポートする BGP ピアに関する情報を表示します。
ステップ 10	**show ip bgp vpnv4 neighbors** *ip-address* 例： `Device# show ip bgp vpnv4 neighbors 192.168.1.1`	ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートの設定例

例：Inter-AS オプション B の BGP NSR サポートを有効にするための ASBR の設定

VPNv4 アドレス ファミリ レベルで ASBR を NSR 対応にするための設定

```
router bgp 200
  neighbor 192.168.1.1 remote-as 200
  neighbor 192.168.1.1 ha-mode sso
  address-family vpnv4 unicast
    neighbor 192.168.1.1 activate
```

VPNv6 アドレス ファミリ レベルで ASBR を NSR 対応にするための設定

```
router bgp 300
  neighbor 192.168.1.10 remote-as 300
  neighbor 192.168.1.10 ha-mode sso
  address-family vpnv6 multicast
    neighbor 192.168.1.10 activate
```

ASBR が NSR 対応であることを確認するには、**show ip bgp vpnv4 neighbors** コマンドの [Stateful switchover support enabled] フィールドの出力をチェックします。

```
ASBR# show ip bgp vpnv4 neighbors 192.168.1.10

BGP neighbor is 192.168.1.10,  vrf A,  remote AS 200, external link
  BGP version 4, remote router ID 192.168.1.10
  BGP state = Established, up for 00:16:01
  Last read 00:00:04, last write 00:00:35, hold time is 180, keepalive interval is 60
seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: YES for session 1
```

MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポ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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

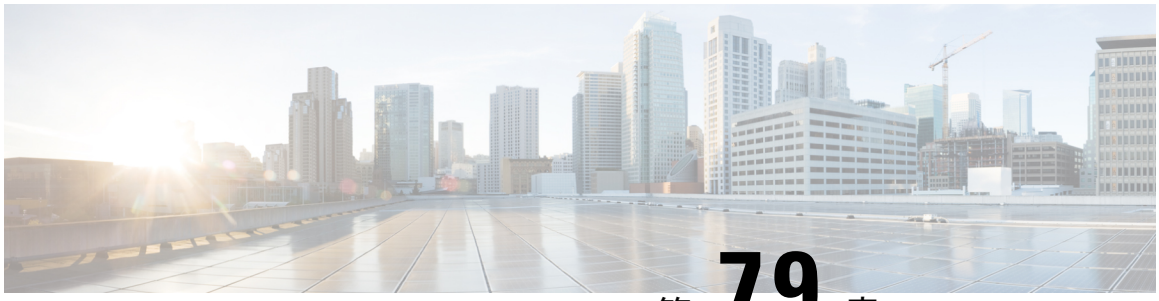
MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポートに関する機能情報

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。

表 *98 : Inter-AS* オプション *B* の *BGP NSR* サポートに関する機能情報

機能名	リリース	機能情報
MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート	Cisco IOS XE Release 3.10S	MPLS VPNv4 および VPNv6 Inter-AS オプション B の BGP NSR サポート機能は、VPNv4 および VPNv6 アドレス ファミリについて、相互自律システム（Inter-AS）オプション B の展開における自律システム境界ルータ（ASBR）でのノンストップ ルーティング（NSR）のサポートを提供します。 追加または変更されたコマンドはありません。



第 79 章

レガシー PE の BGP-RTC

レガシー PE の BGP ルート ターゲット制約（RTC）機能は、VPN に関与していないプロバイダーエッジ（PE）デバイスにVPN ネットワーク層到達可能性情報（NLRI）が伝播されるのを防ぐメカニズムです。この機能は、ピアに渡すルートを決定するためにボーダー ゲートウェイ プロトコル（BGP）スピーカーで使用されるアウトバウンド フィルタを構築し、内部 BGP（iBGP）メッシュ間でルート ターゲット（RT）の到達可能性情報を伝播します。

- 機能情報の確認 （1231 ページ）
- レガシー PE の BGP-RTC の前提条件 （1231 ページ）
- レガシー PE の BGP-RTC に関する情報 （1232 ページ）
- レガシー PE の BGP-RTC の設定方法 （1233 ページ）
- レガシー PE の BGP-RTC の設定例 （1234 ページ）
- レガシー PE の BGP-RTC の追加情報 （1235 ページ）
- レガシー PE の BGP-RTC の機能情報 （1236 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。

レガシー PE の BGP-RTC の前提条件

レガシー PE の BGP-RTC 機能を設定する前に、RT フィルタ ユニキャスト アドレス ファミリ タイプを設定する必要があります。詳細については、『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP：RT 制約ルート配布の設定」モジュールを参照してください。

レガシー PE の BGP-RTC に関する情報

レガシー PE の BGP-RTC の概要

レガシー PE の BGP—RTC 機能では、レガシー プロバイダー エッジ（PE）デバイスから新しいボーダー ゲートウェイ プロトコル（BGP）スピーカー（ルート リフレクタ（RR））へのVPN ユニキャスト ルート交換を利用して、ルート ターゲット（RT）メンバーシップについて通知します。レガシー PE は、マッピングされた RT を持つ特別なルートのセットを標準コミュニティとともに RR に通知します。コミュニティがあることにより、RR で、RT の抽出および RT メンバーシップ情報の構築がトリガーされます。

VPN メンバーシップが正常なシナリオでは、この機能によって、PE デバイスおよび RR のスケーリング要件を軽減できます。PE デバイスでは、不要なルートを除外するためにリソースを費やす必要がなくなります。共通のアウトバウンド ポリシーを持つ BGP ピアは、単一のフォーマット グループに分類されます。フォーマット グループ内で、BGP ピアをそのピアベース ポリシーと分離するために、個別のレプリケーション グループが使用されます。ルート ターゲット制約（RTC）対応ピアは、別々のフォーマット グループに配置されます。各 RTC ピアには、個別のレプリケーション グループがあります。ピアに対してレガシー RT が設定されている場合は、機能ネゴシエーションがないことを除いて、RTC ピアと同様に扱う必要があります。

レガシー PE 対応 PE の動作

各レガシー ルート ターゲット制約（RTC）対応ネイバーには、個別のレプリケーション グループが割り当てられます。BGP では、VPN テーブルをチェックして予約済みのコミュニティ値を持つルートを探し、そのルートを使用して、コミュニティ値とともにレガシー RTC ピアから受信した VPN プレフィックスに基づき、RTC ネットワークを作成します。PE デバイスは、既存の VPN アドバタイズメント メカニズムを使用して、レガシー プロバイダー エッジ（PE）デバイスからのルート ターゲット（RT）メンバーシップを伝達します。ルート リフレクタ（RR）は、レガシー PE デバイスからの RT メンバーシップ情報のアドバタイズメント メカニズムを処理します。RR は、レガシー PE RT メンバーシップ情報を同等の RTC ネットワーク層到達可能性情報（NLRI）に変換して、他の RR に伝播します。

レガシー PE 対応 RR の動作

ルート リフレクタ（RR）は、コミュニティ値によってルート ターゲット（RT）メンバーシップ情報を取得するためにレガシー プロバイダー エッジ（PE）デバイスからのルートを識別し、レガシー PE デバイスへの VPN ルートをフィルタ処理します。RR は、既存の VPN アドバタイズメント メカニズムを使用して、レガシー PE からの RT メンバーシップを伝達および処理します。レガシー PE RT メンバーシップ情報は、クライアントからの同等の RT メンバーシップ ネットワーク層到達可能性情報（NLRI）に変換されて、他の RR に伝播されます。その後、RR は、ルート ターゲットのセット全体を収集して、レガシー クライアントごとにルート ターゲット フィルタ リストを作成します。

レガシー PE の BGP-RTC の設定方法

レガシー PE の BGP-RTC の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**vpnv4** | **vpnv6** } **unicast**
5. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **accept-route-legacy-rt**
6. **address-family rtfilter**
7. **end**
8. **show ip bgp vpnv4 all update-group** *update-group*
9. **show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*}
10. **show ip bgp vpnv4 all peer-group**
11. **debug ip bgp all updates in**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 1`	ボーダーゲートウェイプロトコル（BGP）ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family** {**vpnv4**	**vpnv6** } **unicast** 例： `Device(config-router)# address-family vpnv4 unicast`	VPNv4 または VPNv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*ip-address*	*peer-group-name*	*ipv6-address*} **accept-route-legacy-rt** 例： `Device(config-router-af)# neighbor 10.0.0.1 accept-route-legacy-rt`	プロバイダー エッジ（PE）デバイスをルート ターゲット（RT）のレガシー PE として扱うようにルート リフレクタ（RR）上のネイバーを設定し、特別なコミュニティでタグ付けされた VPN ルートを受け入れます。

	コマンドまたはアクション	目的
ステップ 6	**address-family rtfilter** 例： `Device(config-router-af)# address-family rtfilter`	RT フィルタ アドレス ファミリ タイプを指定します。
ステップ 7	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show ip bgp vpnv4 all update-group** *update-group* 例： `Device# show ip bgp vpnv4 all update-group 2`	（任意）アップデート グループのネイバーに関する情報を表示します。
ステップ 9	**show ip bgp vpnv4 all neighbors** {*ip-address* | *ipv6-address*} 例： `Device# show ip bgp vpnv4 all neighbors 192.168.3.3`	（任意）BGP VPNv4 ネイバーに関する情報を表示します。
ステップ 10	**show ip bgp vpnv4 all peer-group** 例： `Device# show ip bgp vpnv4  all peer-group`	（任意）ピア グループに関する情報を表示します。
ステップ 11	**debug ip bgp all updates in** 例： `Device# debug ip bgp all updates in`	（任意）BGP アップデート メッセージを表示します。

レガシー PE の BGP-RTC の設定例

例：レガシー PE の BGP-RTC

ルート リフレクタでの設定

次の例は、プロバイダー エッジ（PE）デバイスをルート ターゲット（RT）のレガシー PE として扱うようにルート リフレクタ（RR）上のネイバーを設定し、特別なコミュニティでタグ付けされた VPN ルートを受け入れる方法を示しています。

```
Device# configure terminal
Device(config)# router bgp 1
Device(config-router)# address-family vpnv4 unicast
Device(config-router-af)# neighbor 10.1.1.1 accept-route-legacy-rt
Device(config-router-af)# address-family rtfilter
Device(config-router-af)# exit address-family
```

レガシー PE での設定

次の例は、ルート フィルタ VRF を作成し、レイヤ 3 VPN Virtual Routing and Forwarding（VRF）でローカルに設定されたすべての RT を収集して伝送するエクスポート マップを付加する方法を示しています。

```
ip vrf route-filter
 rd 55:1111
 export map SET_RT

route-map SET_RT permit 10
 match ip address prefix-list RT_NET1
 set community 4294901762 (0xFFFF0002)
 set extcommunity rt  255.220.0.0:12241 255.220.0.0:12242 additive
 set extcommunity rt  255.220.0.0:12243 255.220.0.0:12244 additive
 set extcommunity rt  255.220.0.0:12245 255.220.0.0:12246 additive
 set extcommunity rt  255.220.0.0:12247 255.220.0.0:12248 additive
 set extcommunity rt  255.220.0.0:12249 255.220.0.0:12250 additive
!
route-map SET_RT permit 20
 match ip address prefix-list RT_NET2
 set community 4294901762 (0xFFFF0002)
 set extcommunity rt  255.220.0.0:12251 255.220.0.0:12252 additive
 set extcommunity rt  255.220.0.0:12253 255.220.0.0:12254 additive
 set extcommunity rt  255.220.0.0:12255 additive
!

ip route vrf route-filter 5.5.5.5 255.255.255.255 Null0 - (matching prefix-set RT_NET1)
ip route vrf route-filter 6.6.6.6 255.255.255.255 Null0 -(matching prefix-set RT_NET2)

route-map LEG_PE permit 10
 match ip address prefix-list RT_NET1 RT_NET2
 set community no-advertise additive
```

次の例は、ルート マップを VPNv4 ネイバーに適用する方法を示しています。

```
router bgp 55
 address-family vpnv4 unicast
 neighbor x.x.x.x  route-map LEG_PE out
```

次の例は、network コマンドを使用してボーダー ゲートウェイ プロトコル（BGP）ネットワークへのスタティック ルートを送信元にする方法を示しています。

```
router bgp 55
 address-family ipv4 vrf route-filter
 network 5.5.5.5 mask 255.255.255.255
 network 6.6.6.6 mask 255.255.255.255
```

レガシー PE の BGP-RTC の追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

関連項目	マニュアル タイトル
BGP：RT 制約ルート配布の設定	『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP：RT 制約ルート配布の設定」モジュール

標準および RFC

標準/RFC	タイトル
RFC 4684	『*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	リンク
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

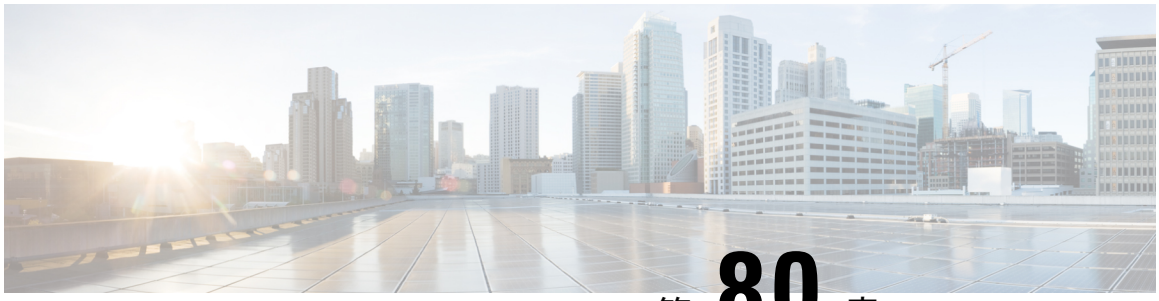
レガシー PE の BGP-RTC の機能情報

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 *99 :* レガシー *PE* の *BGP-RTC* の機能情報

機能名	リリース	機能情報
レガシー PE の BGP-RTC		レガシー PE の BGP-RTC 機能は、VPN に関与していないプロバイダー エッジ（PE）デバイスに VPN ネットワーク層到達可能性情報（NLRI）が伝播されるのを防ぐメカニズムです。この機能は、ピアに渡すルートを決定するためにボーダー ゲートウェイ プロトコル（BGP）スピーカーで使用されるアウトバウンド フィルタを構築し、内部 BGP（iBGP）メッシュ間でルート ターゲット（RT）の到達可能性情報を伝播します。 **neighbor accept-route-legacy-rt** コマンドが導入されました。



第 80 章

BGP PBB EVPN ルート リフレクタのサポート

BGP PBB EVPN ルート リフレクタのサポート機能は、レイヤ 2 VPN アドレス ファミリのイーサネット VPN（EVPN）およびプロバイダー バックボーン ブリッジ（PBB）EVPN 用のボーダー ゲートウェイ プロトコル（BGP）ルート リフレクタ機能を提供します。EVPN は、カスタマー MAC アドレスをルーティング可能なアドレスとして有効にし、BGP で配布して、マルチプロトコル ラベル スイッチング（MPLS）コア ネットワークを介したデータ プレーンの MAC アドレス ラーニングを防止します。ルート リフレクタは、ルート リフレクタ上で明示的に EVPN を設定しなくても受信した EVPN アップデートを保存できるように拡張され、それらのアップデートを他のプロバイダー エッジ（PE）デバイスにアドバタイズします。これにより、PE で BGP セッションのフル メッシュを確立する必要がなくなります。

- 機能情報の確認 （1239 ページ）
- BGP PBB EVPN ルート リフレクタのサポートの前提条件 （1240 ページ）
- BGP PBB EVPN ルート リフレクタのサポートに関する情報 （1240 ページ）
- BGP PBB EVPN ルート リフレクタのサポートの設定方法 （1241 ページ）
- BGP PBB EVPN ルート リフレクタのサポートの設定例 （1243 ページ）
- BGP PBB EVPN ルート リフレクタのサポートに関する追加情報 （1243 ページ）
- BGP PBB EVPN ルート リフレクタのサポートの機能情報 （1244 ページ）

機能情報の確認

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

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

BGP PBB EVPN ルート リフレクタのサポートの前提条件

- BGP PBB EVPN ルート リフレクタのサポート機能を設定する前に、EVPN アドレス ファミリをサポートするように RT フィルタ ユニキャスト アドレス ファミリ タイプを設定する必要があります。詳細については、『*IP* ルーティング：*BGP* コンフィギュレーション ガイド』の「BGP：RT 制約ルート配布の設定」モジュールを参照してください。
- EVPN 後続アドレス ファミリ識別子（SAFI）を BGP ネイバーで有効にする前にグローバルに有効にする必要があります。

BGP PBB EVPN ルート リフレクタのサポートに関する情報

EVPN の概要

イーサネット VPN（EVPN）により、マルチプロトコル ラベル スイッチング（MPLS）ネットワークでマルチポイント レイヤ 2 VPN（L2VPN）サービスを提供できます。

EVPN では、カスタマー MAC アドレスは、カスタマー デバイス（CE）をプロバイダー エッジ（PE）デバイスに接続するリンクを介してデータ プレーンで学習されます。この MAC アドレスは、サービス インスタンスを識別するマルチプロトコル ラベル スイッチング（MPLS）ラベルとともに、ボーダー ゲートウェイ プロトコル（BGP）を使用して MPLS コア ネットワーク上で配布されます。受信側 PE デバイスがディスポジション パスで MAC ルックアップを実行する限り、EVPN インスタンスごとに 1 つの MPLS ラベルで対応できます。受信側 PE デバイスは、このルーティング可能な MAC アドレスを、関連付けられた隣接関係とともに、レイヤ 2 ルーティング情報ベース（RIB）および Forwarding Information Base（FIB; 転送情報ベース）に挿入します。

EVPN は、さまざまなルート タイプおよびルート属性をアドバタイズする BGP ネットワーク層到達可能性情報（NLRI）を定義します。EVPN NLRI は、アドレス ファミリ識別子（AFI）および後続アドレス ファミリ識別子（SAFI）とともに、BGP マルチプロトコル拡張を使用して BGP で伝送されます。サポートされていないルート タイプは、BGP によって削除されるため、ネイバーに伝播されません。

ルート リフレクタでの BGP VPLS 自動検出のサポート

デフォルトでは、内部 BGP（iBGP）ピアから受信したルートは、自律システム（AS）内のすべてのボーダー ゲートウェイ プロトコル（BGP）デバイス間でフル メッシュ設定が形成されていない限り、他の iBGP ピアに送信されません。ルート リフレクタを設定すると、デバイスが iBGP の学習済みルートを他の iBGP スピーカーにアドバタイズまたは反映することができます。

イーサネット VPN（EVPN）自動検出は BGP ルート リフレクタをサポートしています。BGP ルート リフレクタは、ルート リフレクタ上で EVPN を明示的に設定しなくても、BGP EVPN プレフィックスを反映するために使用することができます。ルート リフレクタは、自動検出に参加しません。つまり、ルート リフレクタとプロバイダー エッジ（PE）デバイスの間で擬似回線はセットアップされません。ルート リフレクタは EVPN プレフィックスを他の PE デバイスに反映し、これらの PE デバイスが BGP セッションのフル メッシュを持つ必要がないようにします。ネットワーク管理者はルート リフレクタの BGP EVPN アドレス ファミリだけを設定します。

BGP では、エンドポイント プロビジョニング情報を保存する際にレイヤ 2 VPN（L2VPN）ルーティング情報ベース（RIB）が使用されます。これは、レイヤ 2 仮想転送インスタンス（VFI）が設定される度に更新されます。プレフィックスおよびパス情報は L2VPN データベースに保存され、ベスト パスが BGP により決定されるようになります。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、このエンドポイント情報を使用して擬似回線メッシュが設定されます。

EVPN アドレス ファミリ

BGP では、L2VPN EVPN 自動検出とシグナリングのネットワーク層到達可能性情報（NLRI）をボーダーゲートウェイ プロトコル（BGP）ネイバーに伝送するために、ルータ コンフィギュレーション モードでレイヤ 2 VPN（L2VPN）EVPN アドレス ファミリをサポートしています。このアドレス ファミリは、IPv4 ネイバーと IPv6 ネイバーに対するデフォルト Virtual Routing and Forwarding（VRF）で、内部 BGP（iBGP）と外部 BGP（eBGP）の両方で使用できます。EVPN SAFI は、VRF および VRF ネイバーではサポートされていません。

BGP PBB EVPN ルート リフレクタのサポートの設定方法

BGP PBB EVPN ルート リフレクタの設定

デバイスを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定するには、また BGP ルーティング テーブルから情報を表示するには、ボーダー ゲートウェイ プロトコル（BGP）ルート リフレクタでこの作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family l2vpn [vpls | evpn]**
5. **neighbor** {*ip-address* | *peer-group-name*} **activate**
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
7. **end**
8. **show bgp l2vpn evpn all**

9. **debug bgp l2vpn evpn updates**
10. **clear bgp l2vpn evpn**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 1`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family l2vpn [vpls | evpn]** 例： `Device(config-router)# address-family l2vpn evpn`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。オプションの **evpn** キーワードは、EVPN エンドポイント プロビジョニング情報が BGP ピアに配布されるように指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.2 activate`	指定した BGP ネイバーで PBB EVPN を有効にします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 10.0.0.2 route-reflector-client`	ローカル デバイスを BGP ルート リフレクタとして、指定したネイバーをそのクライアントとして設定します。
ステップ 7	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show bgp l2vpn evpn all** 例： `Device# show bgp l2vpn evpn all`	（任意）L2VPN EVPN データベース全体を表示します。
ステップ 9	**debug bgp l2vpn evpn updates** 例： `Device# debug bgp l2vpn evpn updates events`	（任意）BGP アップデートのデバッグ メッセージを指定します。

	コマンドまたはアクション	目的
ステップ 10	**clear bgp l2vpn evpn** 例： `Device# clear bgp l2vpn evpn *`	（任意）現在のすべての BGP セッションをリセットすることを指定します。

BGP PBB EVPN ルート リフレクタのサポートの設定例

例：BGP PBB EVPN ルート リフレクタの設定

次の例では、ローカル デバイスはルート リフレクタです。これは、学習した iBGP ルートを 10.0.0.2 のネイバーに渡します。

```
Device# configure terminal
Device(config)# router bgp 1
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 10.0.0.2 activate
Device(config-router-af)# neighbor 10.0.0.2 route-reflector-client
Device(config-router-af)# exit address-family
```

次の例では、**show bgp l2vpn evpn all route-type 1** コマンドによってイーサネット自動検出ルート情報を表示します。

```
show bgp l2vpn evpn all route-type 1

BGP routing table entry for
[1][100.100.100.100:11111][AAAABBBBCCCCDDDDEEEE][23456789][101234]/25, version 2
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Advertised to update-groups:
     1          2          3
  Refresh Epoch 1
  Local, (Received from a RR-client)
    19.0.101.1 from 19.0.101.1 (19.0.101.1)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:100:101 EVPN LABEL:0x1:Label-101234
      rx pathid: 0, tx pathid: 0x0
```

BGP PBB EVPN ルート リフレクタのサポ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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 4456	『*BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*』
RFC 4684	『*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	リンク
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

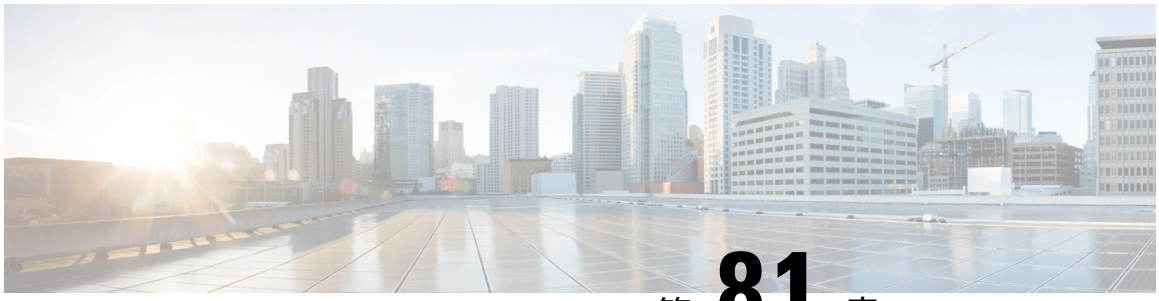
BGP PBB EVPN ルート リフレクタのサポートの機能情報

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 *100 : BGP PBB EVPN* ルート リフレクタのサポートの機能情報

機能名	リリース	機能情報
BGP PBB EVPN ルートリフレクタのサポート		BGP PBB EVPN ルート リフレクタのサポート機能は、レイヤ 2 VPN アドレス ファミリのイーサネット VPN（EVPN）およびプロバイダーバックボーンブリッジ（PBB）EVPN 用のボーダー ゲートウェイ プロトコル（BGP）ルート リフレクタ機能を提供します。EVPN は、カスタマー MAC アドレスをルーティング可能なアドレスとして有効にし、BGP で配布して、マルチプロトコル ラベル スイッチング（MPLS）コア ネットワークを介したデータ プレーンの MAC アドレス ラーニングを防止します。ルート リフレクタは、ルート リフレクタ上で明示的に EVPN を設定しなくても受信した EVPN アップデートを保存できるように拡張され、それらのアップデートを他のプロバイダーエッジ（PE）デバイスにアドバタイズします。これにより、PE で BGP セッションのフル メッシュを確立する必要がなくなります。 **address-family l2vpn** コマンドが変更されました。



第 81 章

BGP Monitoring Protocol

BGP Monitoring Protocol（BMP; BGP モニタリング プロトコル）機能は、ボーダー ゲートウェイ プロトコル（BGP）ネイバー（BMP クライアントとも呼ばれます）をモニタするために、次の機能をサポートしています。

- BMP サーバとして機能するようにデバイスを設定し、BGP ネイバーのモニタリングに必要なサーバのパラメータをセットアップします。
- モニタリング用に BMP サーバと BGP ネイバーの接続を確立します。
- BGP ネイバーのモニタリングから統計レポートを生成します。
- BGP ネイバーで適切なエラー処理を実行します。
- BMP サーバと BGP ネイバーの間の接続を閉じる時点までのグレースフルなスケールアップおよびスケールダウンを実行します。

- 機能情報の確認 （1247 ページ）
- BGP Monitoring Protocol の前提条件 （1248 ページ）
- BGP Monitoring Protocol に関する情報 （1248 ページ）
- BGP Monitoring Protocol の設定方法 （1249 ページ）
- BGP Monitoring Protocol の確認 （1254 ページ）
- BGP Monitoring Protocol のモニタ （1255 ページ）
- BGP Monitoring Protocol の設定例 （1256 ページ）
- BGP Monitoring Protocol の追加情報 （1260 ページ）
- BGP Monitoring Protocol の機能情報 （1261 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 Monitoring Protocol の前提条件

BGP Monitoring Protocol（BMP）サーバを設定する前に、BMP クライアントとして機能するボーダー ゲートウェイ プロトコル（BGP）ネイバーを設定し、IPv4/IPv6 または VPNv4/VPNv6 アドレス ファミリ識別子を使用してピアとのセッションを確立する必要があります。

BGP Monitoring Protocol に関する情報

BGP Monitoring Protocol の概要

BGP Monitoring Protocol（BMP）機能により、BGP ネイバー（BMP クライアントとも呼ばれる）をモニタできるようになります。BMP サーバとして機能するようにデバイスを設定して、複数のアクティブ ピア セッションが確立された 1 つまたは複数の BMP クライアントをモニタできます。また、1 つ以上の BMP サーバに接続するように BMP クライアントを設定することもできます。BMP 機能では、複数の BMP サーバ（プライマリ サーバとして設定）を、アクティブな状態で相互に独立して機能しながら BMP クライアントをモニタするように設定できます。

各 BMP サーバを番号で指定し、コマンド ライン インターフェイス（CLI）を使用して、IP アドレス、ポート番号などのパラメータを設定できます。BMP サーバは、アクティブになると、開始メッセージを送信して BMP クライアントへの接続を試行します。CLI により、複数（独立かつ非同期）の BMP サーバ接続が可能になります。

BGP ネイバー（BMP クライアント）は、モニタリング目的で特定の BMP サーバにデータを送信するように設定されます。これらのクライアントはキューに設定されます。BMP クライアントからの接続リクエストが BMP サーバに着信すると、リクエストが着信した順序に基づいて接続が確立されます。BMP サーバは、最初の BMP ネイバーと接続した後、BMP クライアントをモニタするためにリフレッシュ リクエストを送信し、接続がすでに確立されている BMP クライアントのモニタを開始します。

キュー内の他の BMP クライアントから BMP サーバへのセッション接続リクエストは、**initial-delay** コマンドを使用して設定できる初期遅延の経過後に開始されます。何らかの理由により、接続が確立後に切断された場合は、**failure-retry-delay** コマンドを使用して設定できる遅延の経過後に接続リクエストが再試行されます。接続の確立でエラーが繰り返し発生する場合は、**flapping-delay** コマンドを使用して設定された遅延に基づいて接続の再試行が遅延されます。このようなリクエストの遅延を設定することは重要な作業になります。これは、接続されているすべての BMP クライアントにルート リフレッシュ リクエストが送信されると、ネットワーク トラフィックが大量に発生し、デバイスに負荷がかかるためです。

デバイスに過度の負荷がかかるのを避けるために、BMP サーバは、キュー内で接続が確立された順序に従って、一度に 1 つの BMP クライアントにルート リフレッシュ リクエストを送信します。すでに接続されている BMP クライアントは、「レポート中」の状態になると、「ピアアップ」メッセージを BMP サーバに送信します。ルート リフレッシュ リクエストをクライアントが受信すると、そのネイバーのルート モニタリングが開始されます。ルート リフレッシュ リクエストが終了すると、キュー内の次のネイバーが処理されます。このサイクルは「レポート中」の BGP ネイバーがすべてレポートされるまで続き、これらの「レポート中」の BGP ネイバーによって送信されたすべてのルートが継続的にモニタされます。BMP モニタリングの開始後にネイバーが確立された場合、ルート リフレッシュ リクエストは必要ありません。そのクライアントから受信したすべてのルートが BMP サーバに送信されます。

複数の BMP サーバが立て続けにアクティブ化される場合は、BMP クライアントからのリフレッシュ リクエストをバッチ化すると便利です。**bmp initial-refresh delay** コマンドを使用して、最初の BMP サーバが起動したときにリフレッシュ メカニズムをトリガーする際の遅延を設定できます。このタイムフレーム内に他の BMP サーバがオンラインになった場合は、1 セットのリフレッシュ リクエストのみが BMP クライアントに送信されます。また、BMP サーバからのすべてのリフレッシュ リクエストをスキップし、ピアからのすべての着信メッセージだけをモニタするように、**bmp initial-refresh skip** コマンドを設定することもできます。

クライアントとサーバの設定では、デバイスのリソース負荷を最小限に抑え、過度なネットワーク トラフィックが発生しないようにすることが推奨されます。BMP 設定では、サーバとクライアントの間の接続でフラッピングが発生しないように、BMP サーバ上でさまざまな遅延タイマーを設定できます。過度なメッセージ スループットやシステム リソースの大量使用を避けるために、BMP セッションの最大バッファ制限を設定できます。

BGP Monitoring Protocol の設定方法

BGP Monitoring Protocol セッションの設定

BMP サーバの BGP Monitoring Protocol（BMP）セッション パラメータを設定して BMP クライアントとの接続を確立するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bmp** { **buffer-size** *buffer-bytes* | **initial-refresh** { **delay** *refresh-delay* | **skip**} | **server** *server-number-n*
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**bmp** { **buffer-size** *buffer-bytes* | **initial-refresh** { **delay** *refresh-delay* | **skip**} | **server** *server-number-n* 例： `Device(config-router)# bmp initial-refresh delay 30`	BGP ネイバーの BMP パラメータを設定し、BMP サーバ コンフィギュレーション モードを開始して BMP サーバを設定します。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

BGP ネイバーでの BGP Monitoring Protocol の設定

BGP ネイバー（BMP クライアントとも呼ばれる）で BGP Monitoring Protocol（BMP）をアクティブ化して、ネイバーで設定された BMP サーバによってクライアント アクティビティがモニタされるようにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ipv4-addr* | *neighbor-tag* | *ipv6-addr*} **bmp-activate** {**all** | **server** *server-number-1* [**server** *server-number-2* . . . [**server** *server-number-n*]]}
   - 手順 1 ～ 4 を繰り返して、セッション内の他の BMP クライアントを設定します。
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**neighbor** {*ipv4-addr* | *neighbor-tag* | *ipv6-addr*} **bmp-activate** {**all** | **server** *server-number-1* [**server** *server-number-2* . . . [**server** *server-number-n*]]} • 手順 1 ～ 4 を繰り返して、セッション内の他の BMP クライアントを設定します。 例： `Device(config-router)# neighbor 30.1.1.1 bmp-activate server 1 server 2`	BGP ネイバーで BMP モニタリングをアクティブにします。
ステップ 5	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

BGP Monitoring Protocol サーバの設定

BMP サーバ コンフィギュレーション モードで BGP Monitoring Protocol（BMP）サーバおよびそのパラメータを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bmp** {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n*
5. **activate**

6. **address** {*ipv4-addr* | *ipv6-addr*} **port-number** *port-number*
7. **description LINE** *server-description*
8. **failure-retry-delay** *failure-retry-delay*
9. **flapping-delay** *flap-delay*
10. **initial-delay** *initial-delay-time*
11. **set ip dscp** *dscp-value*
12. **stats-reporting-period** *report-period*
13. **update-source** *interface-type interface-number*
14. **exit-bmp-server-mode**
    - 手順 1 ～ 14 を繰り返して、セッション内の他の BMP サーバを設定します。
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**bmp** {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n* 例： `Device(config-router)# bmp server 1`	BMP サーバ コンフィギュレーション モードを開始して BMP サーバを設定します。
ステップ 5	**activate** 例： `Device(config-router-bmpsrvr)# activate`	BMP サーバと BGP ネイバーの間の接続を開始します。
ステップ 6	**address** {*ipv4-addr* | *ipv6-addr*} **port-number** *port-number* 例：	IP アドレスおよびポート番号を特定の BMP サーバに設定します。

	コマンドまたはアクション	目的
	`Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000`	
ステップ 7	**description LINE** *server-description* 例： `Device(config-router-bmpsrvr)# description LINE SERVER1`	BMP サーバの説明を設定します。
ステップ 8	**failure-retry-delay** *failure-retry-delay* 例： `Device(config-router-bmpsrvr)# failure-retry-delay 40`	BMP サーバ アップデートの送信時にエラーが発生した場合における再試行リクエストの遅延を設定します。
ステップ 9	**flapping-delay** *flap-delay* 例： `Device(config-router-bmpsrvr)# flapping-delay 120`	BMP サーバ アップデートの送信時におけるフラッピングの遅延を設定します。
ステップ 10	**initial-delay** *initial-delay-time* 例： `Device(config-router-bmpsrvr)# initial-delay 20`	BMP サーバからのアップデートの初期リクエストを送信する際の遅延を設定します。
ステップ 11	**set ip dscp** *dscp-value* 例： `Device(config-router-bmpsrvr)# set ip dscp 5`	BMP サーバの IP Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定します。
ステップ 12	**stats-reporting-period** *report-period* 例： `Device(config-router-bmpsrvr)# stats-reporting-period 30`	BMP サーバが BGP ネイバーから統計レポートを受信する時間間隔を設定します。
ステップ 13	**update-source** *interface-type interface-number* 例： `Device(config-router-bmpsrvr)# update-source ethernet 0/0`	BMP サーバ上のルーティング アップデートの送信元インターフェイスを設定します。
ステップ 14	**exit-bmp-server-mode** • 手順 1 ～ 14 を繰り返して、セッション内の他の BMP サーバを設定します。	BMP サーバ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	例： `Device(config-router-bmpsrvr)# exit-bmp-server-mode`	
ステップ 15	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。

BGP Monitoring Protocol の確認

BGP 監視プロトコル (BMP) サーバおよび BMP クライアントの構成を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show ip bgp bmp**
3. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp bmp** 例： `Device# show ip bgp bmp neighbors`	BMP サーバおよびネイバーに関する情報を表示します。
ステップ 3	**show running-config** 例： `Device# show running-config | section bmp`	BMP サーバおよびネイバーに関する情報を表示します。

BGP Monitoring Protocol のモニタ

デバッグを有効にして BGP Monitoring Protocol（BMP）サーバをモニタするには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug ip bgp bmp**
3. **show debugging**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug ip bgp bmp** 例： `Device# debug ip bgp bmp server`	BMP 属性のデバッグを有効にします。
ステップ 3	**show debugging** 例： `Device# show debugging`	デバイスで有効になっているデバッグのタイプに関する情報を表示します。

BGP Monitoring Protocol の設定例

BGP Monitoring Protocol の設定、確認、およびモニタの例

例：BGP Monitoring Protocol の設定

（注） BGP Monitoring Protocol（BMP）を設計どおりに機能させるには、2 つのレベルの設定が必要になります。ネットワーク内で複数のピアが接続されている各 BGP ネイバー（BMP クライアントとも呼ばれる）で BMP モニタリングを有効にし、BMP サーバとクライアント間の接続を確立する必要があります。次に、関連する BMP クライアントをモニタするために必要なパラメータを指定して、特定のサーバの BMP サーバ コンフィギュレーション モードで各 BMP サーバを設定します。

次の例は、IP アドレスが 30.1.1.1 のネイバーで BMP をアクティブにする方法を示しています。このネイバーは BMP サーバ（この場合はサーバ 1 および 2）によってモニタされます。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# neighbor 30.1.1.1 bmp-activate server 1 server 2
Device(config-router)# end
```

次の例は、**neighbor bmp-activate** コマンドを使用して BMP がアクティブ化される BGP ネイバーに対して 30 秒の初期リフレッシュ遅延を設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp initial-refresh delay 30
Device(config-router)# bmp buffer-size 2048
Device(config-router)# end
```

次の例は、BMP サーバ コンフィギュレーション モードを開始し、特定の BMP サーバと BGP BMP ネイバーの間の接続を開始する方法を示しています。この例では、モニタリング パラメータの設定に従って、BMP サーバ 1 および 2 からクライアントへの接続が開始されます。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# description LINE SERVER1
Device(config-router-bmpsrvr)# failure-retry-delay 40
```

```
Device(config-router-bmpsrvr)# flapping-delay 120
Device(config-router-bmpsrvr)# initial-delay 20
Device(config-router-bmpsrvr)# set ip dscp 5
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# update-source ethernet 0/0
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# description LINE SERVER2
Device(config-router-bmpsrvr)# failure-retry-delay 40
Device(config-router-bmpsrvr)# flapping-delay 120
Device(config-router-bmpsrvr)# initial-delay 20
Device(config-router-bmpsrvr)# set ip dscp 7
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# update-source ethernet 2/0
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# end
```

例：BGP Monitoring Protocol の確認

次に、サーバ番号 1 の **show ip bgp bmp server** コマンドの出力例を示します。表示される属性は、BMP サーバ コンフィギュレーション モードで設定します。

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

次に、サーバ番号 2 の **show ip bgp bmp server** コマンドの出力例を示します。表示される属性は、BMP サーバ コンフィギュレーション モードで設定します。

```
Device# show ip bgp bmp server 2

Print detailed info for 1 server number 2.

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

次に、BMP サーバ 1 および 2 の接続を非アクティブ化した後の **show ip bgp bmp server summary** コマンドの出力例を示します。

```
Device# show ip bgp bmp server summary
```

```
Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x0                Down              0
2  20.1.1.1          9000  0x0                Down              0
```

次に、BMP サーバ 1 および 2 の接続を再アクティブ化した後の **show ip bgp bmp neighbors** コマンドの出力例を示します。BGP BMP ネイバーの状態が表示されています。

```
Device# show ip bgp bmp server neighbors

Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

Neighbor           PriQ      MsgQ      CfgSvr#            ActSvr#            RM Sent
30.1.1.1           0         0         1  2               1  2               16
2001:DB8::2001     0         0         1  2               1  2               15
40.1.1.1           0         0         1  2               1  2               26
2001:DB8::2002     0         0         1  2               1  2               15
50.1.1.1           0         0         1  2               1  2               16
60.1.1.1           0         0         1  2               1  2               26
2001:DB8::2002     0         0         1                  1                  9
70.1.1.1           0         0         2                  2                  12
Neighbor           PriQ      MsgQ      CfgSvr#            ActSvr#            RM Sent
80.1.1.1           0         0         1                  1                  10
2001:DB8::2002     0         0         1  2               1  2               16
```

次に、BMP サーバ番号 1 および 2 の **show ip bgp bmp server** コマンドの出力例を示します。BMP サーバ 1 および 2 の統計レポートの間隔は 30 秒に設定されているため、各サーバは、30 秒のサイクルごとに、接続されている BGP BMP ネイバーから統計メッセージを受信します。

```
Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x2A98B07138       Up      00:38:49  162       00:00:09
2  20.1.1.1          9000  0x2A98E17C88       Up      00:38:49  46        00:00:04


Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
```

```
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x2A98B07138       Up      00:40:19  189       00:00:07
2  20.1.1.1          9000  0x2A98E17C88       Up      00:40:19  55        00:00:02
```

（注） BMP サーバによってモニタする BGP BMP ネイバーを複数、たとえば 10 台設定した場合は、設定されている周期サイクルごとに、両方のサーバで 10 個の統計メッセージが受信されます。

次に、デバイスの実行コンフィギュレーションを表示する **show running-config** コマンドの出力例を示します。

```
Device# show running-config | section bmp

bmp server 1
address 10.1.1.1 port-number 8000
description SERVER1
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet0/0
set ip dscp 3
activate
exit-bmp-server-mode
bmp server 2
address 20.1.1.1 port-number 9000
description SERVER2
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet2/0
set ip dscp 5
activate
exit-bmp-server-mode
bmp initial-refresh delay 30
bmp-activate all
```

例：BGP Monitoring Protocol のモニタ

次の例は、各種の BMP 属性のデバッグを有効にする方法を示しています。

```
Device# debug ip bgp bmp event

BGP BMP events debugging is on

Device# debug ip bgp bmp neighbor

BGP BMP neighbor debugging is on

Device# debug ip bgp bmp server
```

```
BGP BMP server debugging is on
```

次に、BGP BMP サーバのデバッグを有効にした後の **show debugging** コマンドの出力例を示します。

```
Device# show debugging

IP routing:
BGP BMP server debugging is on

Device#

*Apr  8 21:04:13.164: BGPBMP: BMP server connection attempt timer expired for server 1
- 10.1.1.1/8000
*Apr  8 21:04:13.165: BGPBMP: BMP server 1 active open process success - 10.1.1.1/8000
*Apr  8 21:04:13.165: BGPBMP: TCP KA interval is set to 15

Device#

*Apr  8 21:04:15.171: BGPBMP: Register read/write notification callbacks with BMP server
 1 TCB - 10.1.1.1/8000
*Apr  8 21:04:15.171: BGPBMP: Initiation msg sent to BMP server 1 - 10.1.1.1/8000
*Apr  8 21:04:15.171: BGPBMP: BMP server 1 connection - 10.1.1.1/8000 up, invoke refresh
 event

Device#

*Apr  8 21:04:16.249: BGPBMP: BMP server connection attempt timer expired for server 2
- 20.1.1.1/9000
*Apr  8 21:04:16.249: BGPBMP: BMP server 2 active open process success - 20.1.1.1/9000
*Apr  8 21:04:16.249: BGPBMP: TCP KA interval is set to 15
*Apr  8 21:04:16.250: BGPBMP: Register read/write notification callbacks with BMP server
 2 TCB - 20.1.1.1/9000
*Apr  8 21:04:16.250: BGPBMP: Initiation msg sent to BMP server 2 - 20.1.1.1/9000
*Apr  8 21:04:16.250: BGPBMP: BMP server 2 connection - 20.1.1.1/9000 up, invoke refresh
 event
```

BGP Monitoring Protocol の追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

BGP Monitoring Protocol 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。

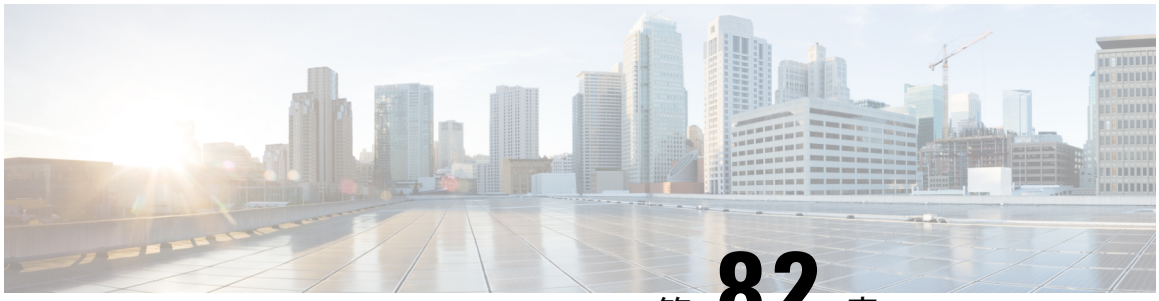
プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *101 : BGP Monitoring Protocol* の機能情報

機能名	リリース	機能説明
BGP Monitoring Protocol		

機能名	リリース	機能説明
		BMP機能は、BMPクライアントとなるボーダー ゲートウェイ プロトコル（BGP）ネイバーをモニタできるように、次の機能をサポートしています。 • BMP サーバとして機能するようにデバイスを設定し、BGP ネイバーのモニタリングに必要なサーバのパラメータをセットアップします。 • モニタリング用に BMP サーバと BGP ネイバーの接続を確立します。 • BGP ネイバーのモニタリングから統計レポートを生成します。 • BGP ネイバーで適切なエラー処理を実行します。 • BMP サーバと BGP ネイバーの間の接続を閉じる時点までのグレースフルなスケールアップおよびスケールダウンを実行します。 次のコマンドが導入または変更されました。 **bmp** **debug ip bgp bmp** **neighbor bmp-activate** **show ip bgp bmp** 特定のBMPサーバを設定するために、BMPサーバ コンフィギュレーション モードに次のコマンドが導入されました。 **activate** **address** **default**

機能名	リリース	機能説明
		description **exit-bmp-server-mode** **failure-retry-delay** **flapping-delay** **initial-delay** **set ip dscp** **stats-reporting-period** **update-source**



第 82 章

VRF 認識 BGP 変換アップデート

VRF 認識 BGP 変換アップデート機能を使用すると、マルチキャスト BGP（mBGP）ルーティングをサポートしない旧バージョンのシスコ ソフトウェアを搭載したカスタマーエッジ（CE）デバイスでのマルチキャスト転送が可能になります。

プロバイダーエッジ（PE）デバイスは、ネイバーCEデバイスとのVirtual Routing and Forwarding（VRF）セッションを確立し、IPv4/IPv6 VRF アドレス ファミリで変換アップデート機能を設定します。PEデバイスは、アップデートをユニキャストからCEデバイス上のマルチキャストに変換し、マルチキャスト アップデートとして PE デバイスのボーダー ゲートウェイ プロトコル（BGP）VRF ルーティング テーブルに配置して処理できるようにします。

- 機能情報の確認 （1265 ページ）
- VRF 認識 BGP 変換アップデートの前提条件 （1266 ページ）
- VRF 認識 BGP 変換アップデートの制約事項 （1266 ページ）
- VRF 認識 BGP 変換アップデートに関する情報 （1266 ページ）
- VRF 認識 BGP 変換アップデートの設定方法 （1267 ページ）
- VRF 認識 BGP 変換アップデートの設定例 （1271 ページ）
- VRF 認識 BGP 変換アップデートの追加情報 （1275 ページ）
- VRF 認識 BGP 変換アップデートの機能情報 （1275 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 認識 BGP 変換アップデートの前提条件

- VRF 認識変換アップデート機能は、IPv4/IPv6 Virtual Routing and Forwarding（VRF）アドレス ファミリにのみ適用されます。
- IPv4/IPv6 VRF アドレス ファミリでは、ネイバーの設定にピアグループを使用する必要があります。
- ユニキャスト ルーティングのみに対応する BGP ネイバーは、ユニキャスト アドレス ファミリとマルチキャスト アドレス ファミリの両方でアクティブ化する必要があります。
- また、VRF 認識変換アップデート機能を設計どおりに動作させるには、互換性のあるマルチキャスト アドレス ファミリで BGP ネイバーを有効にする必要もあります。
- プロバイダー エッジ（PE）デバイスでは、マルチキャスト VRF が有効になっており、カスタマー エッジ（CE）デバイスとのセッションが確立されている必要があります。

VRF 認識 BGP 変換アップデートの制約事項

- VRF 認識 BGP 変換アップデート機能用に（非 VRF）IPv4/IPv6 アドレス ファミリを設定することはできません。IPv4/IPv6 アドレス ファミリは、後続アドレス ファミリ識別子（SAFI）機能を使用してマルチキャスト ルーティング用に設定する必要があります。
- VRF 認識 BGP 変換アップデート機能は、ピアテンプレートを使用した BGP ネイバーの設定をサポートしていません。

VRF 認識 BGP 変換アップデートに関する情報

VRF 認識 BGP 変換アップデートの概要

VRF 認識 BGP 変換アップデート機能を使用すると、マルチキャスト BGP（mBGP）ルーティングをサポートしない旧バージョンのシスコ ソフトウェアを搭載したカスタマーエッジ（CE）デバイスでのマルチキャスト転送が可能になります。

この機能は、後続アドレス ファミリ識別子（SAFI）に類似しています。SAFI は、サービス プロバイダーのコア IPv4 ネットワークでマルチキャスト ルーティングをサポートする機能を提供しますが、サポートは IPv4/IPv6 アドレス ファミリに制限されています。Virtual Routing and Forwarding（VRF）認識 BGP 変換アップデート機能の場合、プロバイダー エッジ（PE）デバイスは、ネイバー CE デバイスとの VRF セッションを確立し、IPv4/IPv6 VRF アドレス ファミリで変換アップデート機能を設定します。

（IPv4 VRF）アドレス ファミリ コンフィギュレーション モードまたは（IPv6 VRF）アドレス ファミリ コンフィギュレーション モードで **neighbor translate-update** コマンドが PE デバイス

上で設定されている場合、PEデバイスは、アップデートをユニキャストからCEデバイス上のマルチキャストに変換し、マルチキャストアップデートとしてPEデバイスのボーダー ゲートウェイ プロトコル（BGP）VRF ルーティング テーブルに配置して処理できるようにします。また、オプションのキーワード**unicast**を設定した場合は、変換されていないアップデートが、PE デバイスのユニキャスト キューに配置され、ユニキャスト VRF BGP テーブルに入力されます。ユニキャスト ルートからマルチキャスト ルートへの変換は、CE デバイスから PE デバイスのみで行われ、マルチキャスト プレフィックスとユニキャスト プレフィックスは、CE デバイスから PE デバイスのマルチキャスト ネイバーにのみアドバタイズされます。

たとえば、ネイバー CE デバイス（CE1）の VRF（v1）で VRF 認識 BGP 変換アップデート機能を設定した場合は、IPv4 マルチキャスト VRF または IPv6 マルチキャスト VRF アドレス ファミリのネイバー トポロジが PE デバイス（PE1）との CE1 のセッションに追加されます。マルチキャスト VRF ネイバー トポロジは、このマルチキャスト セッションにアクティブな状態で参加することはなく、CE1 から着信した通知を転送するだけです。このような通知は、着信後、マルチキャストに変換され、非アクティブなマルチキャスト VRF ネイバーのルーティング テーブルに配置されます。シスコ ソフトウェアは、IPv4/IPv6 VRF アドレス ファミリで設定された CE1 によってアドバタイズされるルートが、PE1 の IPv4/IPv6 マルチキャスト VRF v1 アドレス ファミリ BGP テーブルで使用できるようにします。**neighbor translate-update** コマンドを設定している場合、これらのルートは、PE1 の IPv4/IPv6 マルチキャスト VRF v1 アドレス ファミリ BGP テーブルとともに、PE1 のマルチキャスト ピアにアドバタイズされます。オプションの **unicast** キーワードも設定している場合は、PE1 のユニキャスト ピアにもルートがアドバタイズされます。

unicast キーワードは、PE デバイスが CE デバイスからのユニキャスト アドバタイズメントを PE デバイスのユニキャスト BGP テーブルに配置できるようにするため、オプションではあるものの重要です。したがって、CE デバイスからのルート アドバタイズメントは、ユニキャスト BGP テーブルとマルチキャスト BGP テーブルの両方に入力されますが、その他の CE デバイスのルートは PE デバイスのマルチキャスト BGP テーブルのみに入力されます。

（注） VRF 認識 BGP 変換アップデート機能を設計どおりに動作させるには、互換性のあるマルチキャスト アドレス ファミリでアドレス ファミリを有効にする必要もあります。

VRF 認識 BGP 変換アップデートの設定方法

VRF 認識 BGP 変換アップデートの設定

VRF 認識 BGP 変換アップデート機能を設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*

4. **address-family ipv4** [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** {*ipv4-addr* | *ipv6-addr* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ipv4-addr* | *ipv6-addr*} **peer-group** *peer-group-name*
8. **neighbor** {*ipv4-addr* | *ipv6-addr* | *peer-group-name*} **activate**
9. **neighbor** {*ipv4-address* | *ipv6-address*} **translate-update multicast** [**unicast**]
10. **end**
11. **show bgp vpnv4 multicast** {**all** | **vrf** *vrf-name* | **rd** *route-distinguisher*}
12. **show ip route multicast vrf** *vrf-name*
13. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**mdt**	**tunnel**	{**multicast**	**unicast**} [**vrf** *vrf-name*]	**vrf** *vrf-name*] 例： `Device(config)# address-family ipv4 vrf v1`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IP バージョン 4（IPv4）アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 5	**neighbor** *peer-group-name* **peer-group** 例： `Device(config-af)# neighbor n2 peer-group`	BGP ピア グループまたはマルチプロトコル BGP ピア グループを作成します。
ステップ 6	**neighbor** {*ipv4-addr*	*ipv6-addr*	*peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-af)# neighbor n2 remote-as 4`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ipv4-addr* | *ipv6-addr*} **peer-group** *peer-group-name* 例： `Device(config-af)# neighbor 10.1.1.1 peer-group n2`	ピア グループのメンバになるように BGP ネイバーを設定します。
ステップ 8	**neighbor** {*ipv4-addr* | *ipv6-addr* | *peer-group-name*} **activate** 例： `Device(config-af)# neighbor 10.1.1.1 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 9	**neighbor** {*ipv4-address* | *ipv6-address*} **translate-update multicast** [**unicast**] 例： `Device(config-af)# neighbor 10.1.1.1 translate-update multicast unicast`	マルチキャスト BGP（mBGP）ルーティングに対応していないデバイスでマルチキャスト ルーティングを有効にします。
ステップ 10	**end** 例： `Device(config-af)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show bgp vpnv4 multicast** {**all** | **vrf** *vrf-name* | **rd** *route-distinguisher*} 例： `Device# show bgp vpnv4 mul vrf v1 summary`	BGP テーブル内のバーチャル プライベート ネットワーク バージョン 4（VPNv4）マルチキャスト エントリを表示します。
ステップ 12	**show ip route multicast vrf** *vrf-name* 例： `Device# show ip route multicast vrf v1`	特定のマルチキャスト VPN ルーティングおよび転送（VRF）インスタンスに関連する IP ルーティング テーブルを表示します。
ステップ 13	**show running-config** 例： `Device# show running-config`	デバイスの実行コンフィギュレーションを表示します。

VRF 認識 BGP 変換アップデート設定の削除

VRF 認識 BGP 変換アップデート機能を無効にするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **no neighbor** {*ipv4-address* | *ipv6-address*} **translate-update multicast** [**unicast**]
6. **end**
7. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 65000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4** [**mdt**	**tunnel**	{**multicast**	**unicast**} [**vrf** *vrf-name*]	**vrf** *vrf-name*] 例： `Device(config)# address-family ipv4 vrf v1`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IP バージョン 4（IPv4）アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 5	**no neighbor** {*ipv4-address*	*ipv6-address*} **translate-update multicast** [**unicast**] 例： `Device(config-af)# no neighbor 10.1.1.1 translate-update multicast unicast`	マルチキャスト BGP（mBGP）ルーティングに対応していないデバイスでマルチキャスト ルーティングを無効にします。
ステップ 6	**end** 例： `Device(config-af)# end`	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 7	**show running-config** 例： `Device# show running-config`	デバイスの実行コンフィギュレーションを表示します。

VRF 認識 BGP 変換アップデートの設定例

例：VRF 認識 BGP 変換アップデートの設定

次の例では、v1 という名前の IPv4 VRF アドレス ファミリおよび VRF 設定用の BGP ネイバー n2 ピアグループについて変換アップデート機能を設定する方法を示します。

（注） BGP ネイバーのピアテンプレート設定は、シスコ ソフトウェアの以前のバージョンとの競合により、この機能ではサポートされていません。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf v1
Device(config-router-af)# neighbor n2 peer-group
Device(config-router-af)# neighbor n2 remote-as 4
Device(config-router-af)# neighbor 10.1.1.1 peer-group n2
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 translate-update multicast unicast
Device(config-router-af)# end
```

次に、**show bgp vpnv4 multicast vrf** コマンドの出力例を示します。VRF 認識 BGP 変換アップデート機能を設定すると、ネイバーの状態として「NoNeg」と表示されます。

```
Device# show bgp vpnv4 multicast vrf v1 summary

BGP router identifier 10.1.3.1, local AS number 65000
BGP table version is 8, main routing table version 8
7 network entries using 1792 bytes of memory
8 path entries using 960 bytes of memory
5/3 BGP path/bestpath attribute entries using 1280 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4168 total bytes of memory
BGP activity 23/2 prefixes, 33/9 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.1        4            4       5      10        1    0    0 00:01:10 (NoNeg)

10.1.3.2        4            2      12      10        8    0    0 00:01:33
```

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

（注） 変換アップデート機能を使用して設定されたルートには、ルーティング情報ベース（RIB）テーブル内のプレフィックスに対する「+」記号がありません。1 つ目のエントリに表示されているこの記号は、ユニキャストルートがマルチキャストテーブルにリークされていることを示します。ただし、2つ目のエントリは、マルチキャストルートとして表示される変換アップデート ルートです。

```
Device# show ip route multicast vrf v1

B   +    10.1.1.0/24 [20/0] via 10.1.1.1 (v1), 00:00:08

B        10.1.1.0/24 [20/0] via 10.1.1.1 (v1), 00:00:42
```

次に、**show running-config** コマンドの出力例を示します。

（注） プロバイダー エッジ（PE）デバイスでは、BGP ネイバーがマルチキャスト ルーティングに対応していない場合でも、マルチキャストアドレス ファミリでそのネイバーをアクティブにする必要があります。ユニキャスト アドレス ファミリ識別子にルートマップが設定されており、マルチキャストアドレス ファミリ識別子にはルートマップが設定されていない場合、ユニキャストルートマップは、ユニキャストテーブルでのルートの制御は行いますが、マルチキャスト テーブルでのルートの制御は行いません。

```
Device# show running-config

address-family ipv4 vrf v1
redistribute connected
redistribute static
neighbor 10.1.1.1 remote-as 4
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 translate-update multicast unicast
neighbor 10.1.1.1 remote-as 4
neighbor 10.1.1.1 activate
exit-address-family
!
address-family ipv4 multicast vrf v1
redistribute connected
redistribute static
neighbor 10.1.1.1 remote-as 4
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 soft-reconfiguration inbound
neighbor 10.1.1.1 route-map x in
exit-address-family
```

（注） 出力の [neighbor 10.1.1.1 soft-reconfiguration inbound] フィールドおよび [neighbor 10.1.1.1 route-map x in] フィールドは、BGP マルチキャスト テーブル内のルートのみが影響を受けることを示しています。

次に、さまざまなアドレス ファミリでネイバーを設定する場合の **show running-config** コマンドの出力例を示します。

（注） さまざまなアドレス ファミリで BGP ネイバーを設定することで、ネイバーにアドバタイズされるユニキャスト ルートとマルチキャスト ルートを操作できます。

IPv4/IPv6 ユニキャスト アドレス ファミリの設定

```
Device# show running-config

address-family ipv4
neighbor 20.2.2.1 activate
neighbor 20.2.2.1 translate-update multicast unicast
exit-address-family
!
address-family ipv4 multicast
neighbor 20.2.2.1 activate
exit-address-family
!
```

IPv4/IPv6 VRF ユニキャスト アドレス ファミリの設定

```
Device# show running-config

address-family ipv4 vrf v1
neighbor 20.2.2.1 remote-as 4
neighbor 20.2.2.1 activate
neighbor 20.2.2.1 translate-update multicast unicast
exit-address-family
!
address-family ipv4 multicast vrf v1
neighbor 20.2.2.1 remote-as 4
neighbor 20.2.2.1 activate
exit-address-family
!
```

次に、旧バージョンのシスコ ソフトウェアを搭載したデバイスからの変換アップデート機能の設定例を示します。この場合は、**address-family** コマンドを実行せずに、IPv4/IPv6 ユニキャスト アドレス ファミリに対してネイバーが設定されています。

アドレス ファミリが設定されていない、古い形式の設定

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# neighbor 20.2.2.1 remote-as 4
Device(config-router)# neighbor 20.2.2.1 translate-update nlri ipv4 multicast unicast
Device(config-router-af)# end
```

アドレス ファミリが設定されていない、新しい形式の設定

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# neighbor 20.2.2.1 remote-as 4
Device(config-router)# neighbor 20.2.2.1 translate-update nlri multicast unicast
Device(config-router-af)# end
```

例：VRF 認識 BGP 変換アップデート設定の削除

次の例では、v1 という名前の IPv4 VRF アドレス ファミリおよび VRF 用の BGP ネイバー n2 ピアグループについて VRF 認識 BGP 変換アップデート機能を無効にする方法を示します。

（注） ネイバーの変換アップデート設定を無効にすると、マルチキャストセッションからネイバーを削除する場合と同様に、擬似マルチキャスト ネイバーが削除され、セッションのフラップが発生します。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf v1
Device(config-router-af)# no neighbor 10.1.1.1 translate-update multicast unicast
Device(config-router-af)# end
```

次の出力には、ネイバーの変換アップデート機能を無効にした後のデバッグ ログが表示されています。

```
*Nov 20 07:09:15.902: %BGP_SESSION-5-ADJCHANGE:
neighbor 2.2.2.1 IPv4 Multicast vpn vrf v1 topology base removed from session  Neighbor
 deleted
*Nov 20 07:09:15.902: %BGP-5-ADJCHANGE:
neighbor 2.2.2.1 vpn vrf v1 Down Neighbor deleted
*Nov 20 07:09:15.902: %BGP_SESSION-5-ADJCHANGE:
neighbor 2.2.2.1 IPv4 Unicast vpn vrf v1 topology base removed from session  Neighbor
deleted
*Nov 20 07:09:16.877: %BGP-5-ADJCHANGE:
neighbor 2.2.2.1 vpn vrf v1 Up
```

次に、**show running-config** コマンドの出力例を示します。

（注） 関連付けられたネイバー 10.1.1.1 は、そのネイバーで変換アップデートが無効になった後、不揮発性生成（NVGEN）からも削除されます。

```
Device# show running-config
```

```
address-family ipv4 vrf v1
redistribute connected
redistribute static
neighbor 10.1.1.1 remote-as 4
neighbor 10.1.1.1 activate
exit-address-family
!
address-family ipv4 multicast vrf v1
redistribute connected
redistribute static
exit-address-family
```

VRF 認識 BGP 変換アップデートの追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

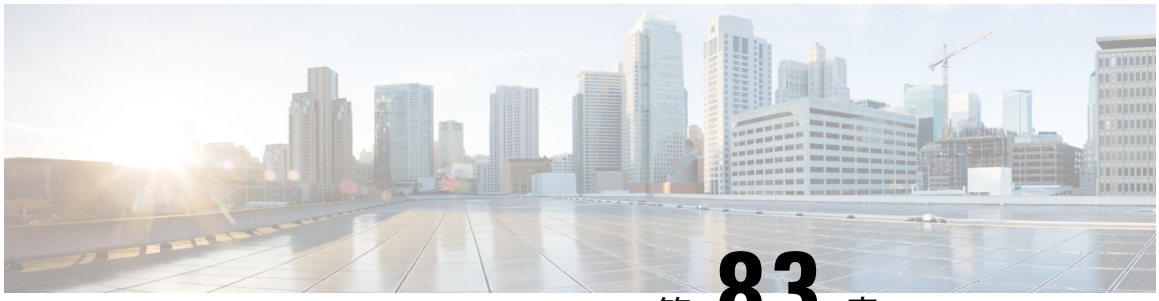
VRF 認識 BGP 変換アップデートの機能情報

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 *102 : VRF* 認識 *BGP* 変換アップデートの機能情報

機能名	リリース	機能情報
VRF 認識 BGP 変換アップデート		VRF 認識 BGP 変換アップデート機能を使用すると、マルチキャスト BGP（mBGP）ルーティングをサポートしない旧バージョンのシスコ ソフトウェアを搭載したカスタマーエッジ（CE）デバイスでのマルチキャスト転送が可能になります。 次のコマンドが導入されました。 **neighbor translate-update**



第 83 章

MTR に対する BGP サポート

MTR に対する BGP サポート機能により、単一の物理ネットワーク上の複数の論理トポロジに対するボーダー ゲートウェイ プロトコル（BGP）サポートが実現します。ここでは、マルチトポロジ ルーティング（MTR）に対して BGP を設定する方法について説明します。

- 機能情報の確認 （1277 ページ）
- MTR に対する BGP サポートの前提条件 （1277 ページ）
- MTR に対する BGP サポートの制約事項 （1278 ページ）
- MTR に対する BGP サポートに関する情報 （1278 ページ）
- MTR に対する BGP のサポートの設定方法 （1281 ページ）
- MTR に対する BGP サポートの設定例 （1289 ページ）
- その他の参考資料 （1291 ページ）
- MTR に対する BGP サポートに関する機能情報 （1292 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。

MTR に対する BGP サポートの前提条件

- 「MTR に対する BGP サポートに関する情報」に記載されているすべての概念について理解しておく必要があります。

- グローバルなマルチトポロジ ルーティング（MTR）トポロジ コンフィギュレーションを設定し、アクティブ化します。

MTR に対する BGP サポートの制約事項

- トポロジ内の再配布が許可されます。あるトポロジから別のトポロジへの再配布は許可されません。この制限は、ルーティング ループを防ぐために設計されています。トポロジ変換またはトポロジ インポート機能を使用して、あるトポロジから別のトポロジにルートを移動できます。
- 単一のマルチキャスト トポロジだけを設定でき、マルチキャスト トポロジが作成される場合は基本トポロジだけを指定できます。

MTR に対する BGP サポートに関する情報

MTR に対するルーティング プロトコル サポート

マルチトポロジ ルーティング（MTR）を動作させるには、デバイスで IP ルーティングをイネーブルにする必要があります。MTR は、シスコ ソフトウェアでのスタティック ルーティングおよびダイナミック ルーティングをサポートします。トポロジ単位のダイナミック ルーティングをイネーブルにすることで、ドメイン内およびドメイン間のルーティングをサポートできます。ルートの計算と転送は、各トポロジで個別に行われます。シスコ ソフトウェアには、次のプロトコルについて MTR のサポートが組み込まれています。

- Border Gateway Protocol（BGP）
- Integrated Intermediate System-to-Intermediate System（IS-IS）

グローバル ルーティング プロセス（ルータ コンフィギュレーション モード）のルータ アドレス ファミリ コンフィギュレーション モードでトポロジ単位のコンフィギュレーションを適用します。アドレス ファミリおよびサブアドレス ファミリは、デバイスがアドレス ファミリ コンフィギュレーション モードを開始するときに指定します。トポロジ名とトポロジ ID を指定するには、アドレス ファミリ コンフィギュレーション モードで **topology** コマンドを入力します。

各トポロジに、ルーティング プロトコル下で一意のトポロジ ID を設定します。トポロジ ID は、所定のプロトコルのアップデート時に各トポロジに対してネットワーク層到着可能性情報（NLRI）を識別してグループ化するために使用されます。OSPF、EIGRP、および IS-IS では、クラス固有のトポロジに対する **topology** コマンドの最初のコンフィギュレーションでトポロジ ID を入力します。BGP では、トポロジ コンフィギュレーションで **bgp tid** コマンドを入力することによってトポロジ ID を設定します。

クラス固有のトポロジには、基本トポロジとは異なるメトリックを設定できます。基本トポロジに設定されたインターフェイス メトリックをクラス固有のトポロジに継承することもできま

す。継承は、クラス固有のトポロジに明示的な継承メトリックが設定されていない場合に実行されます。

BGP サポートは、ルータ コンフィギュレーション モードだけで設定します。内部ゲートウェイ プロトコル（IGP）サポートは、ルータ コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで設定します。

デフォルトでは、インターフェイスには基本トポロジ以外のトポロジは含まれません。EIGRP、IS-IS、および OSPF のルーティング プロトコル サポートについては、インターフェイスに基本トポロジ以外のトポロジを明示的に設定する必要があります。アドレス ファミリ トポロジ コンフィギュレーション モードで **all-interfaces** コマンドを使用すると、デフォルト動作をオーバーライドできます。**all-interfaces** コマンドを入力すると、デフォルトのアドレス空間、またはトポロジが設定される Virtual Routing and Forwarding（VRF）インスタンスに属するデバイスのすべてのインターフェイスに、基本トポロジ以外のトポロジが設定されます。

BGP ネットワーク スコープ

マルチトポロジ ルーティング（MTR）用のボーダー ゲートウェイ プロトコル（BGP）サポートを実装するにはスコープ階層が必要ですが、スコープ階層はMTRの使用に制限されません。スコープ階層によって、ルータ スコープ コンフィギュレーション モードなどの新しいコンフィギュレーション モードが導入されています。デバイスは、ルータ コンフィギュレーション モードで **scope** コマンドを設定すると、ルータ スコープ コンフィギュレーション モードを開始します。このコマンドを入力すると、ルーティング テーブルの集合が作成されます。

BGP コマンドはスコープ階層で単一のネットワーク用に（グローバルに）設定するか、または仮想ルーティングおよび転送（VRF）単位で設定します。このようなコンフィギュレーションをスコープ コマンドと呼びます。スコープ階層には、1 つ以上のアドレス ファミリを含めることができます。

BGP 下の MTR コマンドライン インターフェイス（CLI）階層

ボーダー ゲートウェイ プロトコル（BGP）CLIは、事前マルチトポロジ ルーティング（MTR）の BGP コンフィギュレーションに対する下位互換性を提供し、MTR の階層化実装を可能にします。ルータ コンフィギュレーション モードには、事前アドレス ファミリおよび事前 MTR のコンフィギュレーション CLI との下位互換性があります。すべてのネットワークに影響を与えるグローバル コマンドはこのコンフィギュレーション モードで設定されます。アドレス ファミリおよびトポロジ コンフィギュレーション用に、アドレス ファミリ コンフィギュレーション モードまたはトポロジ コンフィギュレーション モードで使用する汎用のセッション コマンドとピア テンプレートを設定します。

グローバル コマンドの設定後に、スコープをグローバルに定義するか、特定の仮想ルーティングおよび転送（VRF）インスタンスに対して定義します。デバイスは、ルータ スコープ コンフィギュレーション モードまたはルータ コンフィギュレーション モードで **address-family** コマンドを設定すると、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。サブアドレス ファミリ識別子（SAFI）が指定されていない場合は、ユニキャストがデフォルトのアドレス ファミリです。MTR では、ユニキャストまたはマルチキャストの SAFI が指定された IPv4 アドレス ファミリだけがサポートされます。

デバイスがルータ コンフィギュレーション モードからアドレス ファミリ コンフィギュレーション モードに移行すると、ソフトウェアは BGP が事前 MTR ベースの CLI を使用するように設定します。このコンフィギュレーション モードには、既存のアドレス ファミリ コンフィギュレーションとの下位互換性があります。ルータ スコープ コンフィギュレーション モードからアドレス ファミリ コンフィギュレーション モードを開始すると、デバイスは MTR をサポートする階層 CLI を使用するよう設定されます。トポロジに固有ではないアドレス ファミリ コンフィギュレーション パラメータは、このアドレス ファミリ コンフィギュレーション モードで入力します。

デバイスは、アドレス ファミリ コンフィギュレーション モードで **topology** コマンドを設定すると、BGP トポロジ コンフィギュレーション モードを開始します。デバイスには、最大 32 個のトポロジ（基本トポロジを含む）を設定できます。トポロジ ID を設定するには、**bgp tid** コマンドを入力します。トポロジのすべてのアドレス ファミリ コンフィギュレーション パラメータとサブアドレス ファミリ コンフィギュレーション パラメータがここで設定されます。

（注） BGP ルーティング プロセスのスコープを設定すると、事前 MTR ベース設定に対する CLI サポートは削除されます。

次の例は、MTR の実装に対して BGP を設定するときに使用される階層レベルを示しています。

```
router bgp <autonomous-system-number>
 ! Global commands

 scope {global | vrf <vrf-name>}
  ! Scoped commands

  address-family {<afi>} [<safi>]
   ! Address family specific commands

   topology {<topology-name> | base}
    ! topology specific commands
```

クラス固有のトポロジの BGP セッション

マルチトポロジ ルーティング（MTR）は、セッション単位でボーダー ゲートウェイ プロトコル（BGP）下で設定されます。基本のユニキャスト トポロジとマルチキャスト トポロジは、グローバル（デフォルト）セッションで伝送されます。BGP ルーティング プロセス下で設定されるクラス固有のトポロジごとに別個のセッションが作成されます。各セッションは、トポロジ ID で識別されます。BGP は、クラス固有のトポロジごとにベストパスの計算を個別に実行します。セッションごとに別個のルーティング情報ベース（RIB）と転送情報ベース（FIB）が維持されます。

BGP を使用したトポロジの変換

ネットワークの設計とポリシー要件によっては、あるデバイス上のクラス固有のトポロジから、ネイバーデバイス上のクラス固有のトポロジにルートをインストールしなければならないことがあります。ボーダー ゲートウェイ プロトコル（BGP）を使用したトポロジ変換機能によって、この操作がサポートされます。トポロジ変換は、BGP ネイバー セッション ベースで行われます。**neighbor translate-topology** コマンドを設定するには、ネイバーの IP アドレスとトポロジ ID を使用します。

トポロジ ID は、ネイバーのクラス固有のトポロジを識別します。ネイバーのクラス固有のトポロジ内のルートは、ローカルのクラス固有のルーティング情報ベース（RIB）にインストールされます。BGP は、インストールされているすべてのルートでベストパスの計算を実行し、これらのルートをローカルのクラス固有の RIB にインストールします。重複するルートを変換すると、BGP は、標準の BGP ベストパスの計算ごとに、ルートのインスタンスを 1 つだけ選択してインストールします。

BGP を使用したトポロジのインポート

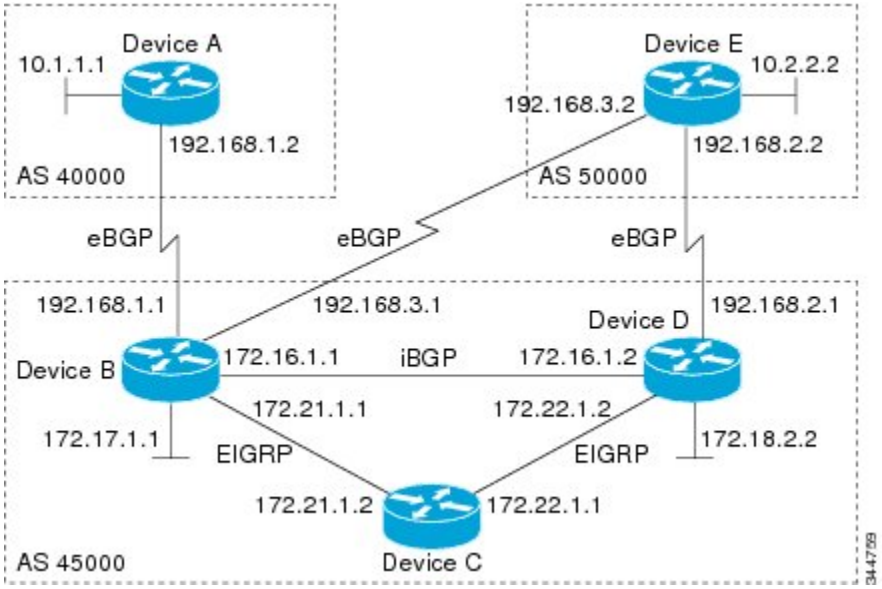
ボーダー ゲートウェイ プロトコル（BGP）を使用したトポロジのインポートはトポロジ変換と似ています。違いは、ルートが同一デバイス上のクラス固有のトポロジ間で移動されることです。この機能を設定するには、**import topology** コマンドを入力し、クラス固有のトポロジまたは基本トポロジの名前を指定します。ベストパスの計算は、インポート済みのルートがトポロジのルーティング情報ベース（RIB）にインストールされる前にこれらのルートで実行されます。この **import topology** コマンドには、クラス固有のトポロジ間で移動されるルートをフィルタ処理できるようにする **route-map** キーワードも含まれています。

MTR に対する BGP のサポートの設定方法

BGP を使用した MTR トポロジのアクティブ化

この作業は、ボーダー ゲートウェイ プロトコル（BGP）を使用してアドレス ファミリ内でマルチトポロジ ルーティング（MTR）トポロジをアクティブにする場合に実行します。この作業は下図のデバイス B で設定されますが、デバイス D およびデバイス E でも設定する必要があります。この作業ではスコープ階層がグローバルに適用するよう設定され、ネイバーがルータ スコープ コンフィギュレーション モードに設定されます。IPv4 ユニキャスト アドレス ファミリでは、ビデオ トラフィックに適用される MTR トポロジは、指定されたネイバーについてアクティブにされます。BGP トポロジのインターフェイス コンフィギュレーション モードはありません。

図 *95 : BGP* ネットワーク ダイアグラム



手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **scope** {**global** | **vrf** *vrf-name*}
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** | **multi-session** | **single-session**}
7. **address-family ipv4**[**mdt** |**multicast** |**unicast**]
8. **topology** {**base** | *topology-name*}
9. **bgp tid** *number*
10. **neighbor** *ip-address* **activate**
11. **neighbor** {*ip-address* | *peer-group-name*} **translate-topology** *number*
12. **end**
13. **clear ip bgp topology** {* | *topology-name*} {*as-number* | **dampening** [*network-address* [*network-mask*]] | **flap-statistics** [*network-address* [*network-mask*]] | **peer-group** *peer-group-name* | **table-map** | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **soft** [**in** [**prefix-filter**] | **out**]]
14. **show ip bgp topology** {* | *topology*} **summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 45000`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**scope** {**global** | **vrf** *vrf-name*} 例： `Device(config-router)# scope global`	BGP ルーティング プロセスに対してスコープを定義して、ルータ スコープ コンフィギュレーション モードを開始します。 • 単一のネットワークに適用される BGP の一般的なセッション コマンドまたは指定された仮想ルーティングおよび転送（VRF）が、このコンフィギュレーションモードで入力されます。 • BGP がグローバル ルーティング テーブルを使用することを指定するには、**global** キーワードを使用します。 • BGP が特定の VRF ルーティング テーブルを使用することを指定するには、**vrf** *vrf-name* キーワードおよび引数を使用します。VRF がすでに存在している必要があります。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* 例： `Device(config-router-scope)# neighbor 172.16.1.2 remote-as 45000`	指定された自律システムのネイバーの IP アドレスを、ローカル デバイスのマルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** | **multi-session** | **single-session**}	BGP セッションの TCP 転送セッション オプション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(config-router-scope)# neighbor 172.16.1.2 transport multi-session`	• 接続のタイプ（アクティブまたはパッシブのいずれか）を指定するには、**connection-mode** キーワードを使用します。 • TCP 転送パスの最大伝送ユニット（MTU）検出を有効にするには、**path-mtu-discovery** キーワードを使用します。 • アドレス ファミリごとに別個の TCP 転送セッションを指定するには、**multi-session** キーワードを使用します。 • すべてのアドレス ファミリで単一の TCP 転送セッションを使用するには、**single-session** キーワードを使用します。
ステップ 7	**address-family ipv4**[**mdt** |**multicast** |**unicast**] 例： `Device(config-router-scope)# address-family ipv4`	IPv4 アドレス ファミリを指定して、ルータ スコープ 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。 • IPv4 マルチキャスト配信ツリー（MDT）アドレス プレフィックスを指定するには、**mdt** キーワードを使用します。 • IPv4 マルチキャスト アドレス プレフィックスを指定するには、**multicast** キーワードを使用します。 • IPv4 ユニキャスト アドレス ファミリを指定するには、**unicast** キーワードを使用します。デフォルトでは、**address-family ipv4** コマンドに **unicast** キーワードが指定されていない場合、デバイスは IPv4 ユニキャスト アドレス ファミリのアドレス ファミリ コンフィギュレーション モードになります。 • トポロジに固有ではない設定パラメータは、このコンフィギュレーション モードで設定されます。
ステップ 8	**topology** {**base** | *topology-name*} 例： `Device(config-router-scope-af)# topology VIDEO`	BGP がクラス固有のトポロジまたは基本トポロジのトラフィックをルーティングするトポロジ インスタンスを設定し、ルータ スコープ アドレス ファミリ トポロジ 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 9	**bgp tid** *number* 例： `Device(config-router-scope-af-topo)# bgp tid 100`	BGP ルーティング プロセスを、指定されたトポロジ ID に関連付けます。 • それぞれのトポロジは、固有のトポロジ ID を使用して設定する必要があります。
ステップ 10	**neighbor** *ip-address* **activate** 例： `Device(config-router-scope-af-topo)# neighbor 172.16.1.2 activate`	BGP ネイバーが、ネットワーク サービス アクセス ポイント（NSAP）アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。 （注） ピア グループを BGP ネイバーとして設定した場合は、このコマンドを使用しないでください。これは、ピア グループ パラメータの設定時にピア グループが自動的にアクティブにされるためです。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **translate-topology** *number* 例： `Device(config-router-scope-af-topo)# neighbor 172.16.1.2 translate-topology 200`	（任意）別のデバイス上のトポロジからローカル デバイス上のトポロジへのルートをインストールするよう BGP を設定します。 • デバイス上のトポロジを識別するために、*number* 引数にトポロジ ID を入力します。
ステップ 12	**end** 例： `Device(config-router-scope-af-topo)# end`	（任意）ルータ スコープ アドレス ファミリ トポロジ 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 13	**clear ip bgp topology** {***** | *topology-name*} {*as-number* | **dampening** [*network-address* [*network-mask*]] | **flap-statistics** [*network-address* [*network-mask*]] | **peer-group** *peer-group-name* | **table-map** | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **soft** [**in** [**prefix-filter**] | **out**]] 例： `Device# clear ip bgp topology VIDEO 45000`	指定されたトポロジまたはすべてのトポロジ下で BGP ネイバー セッションをリセットします。
ステップ 14	**show ip bgp topology** {***** | *topology*} **summary** 例： `Device# show ip bgp topology VIDEO summary`	（任意）トポロジに関する BGP 情報を表示します。 • ほとんどの標準の BGP キーワードと引数を **topology** キーワードの後に入力できます。

	コマンドまたはアクション	目的
		（注） この作業に必要な構文だけが示されています。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

次の作業

イネーブルにするトポロジごとにこの作業を繰り返して、トポロジを使用するすべてのネイバー デバイスでこの設定を繰り返します。

同じルータ上のあるマルチトポロジ ルーティング（MTR）トポロジから別のトポロジにルートをインポートする場合は、「BGP を使用した MTR トポロジからのルートのインポート」セクションを参照してください。

BGP を使用した MTR トポロジからのルートのインポート

この作業は、複数のトポロジが同じデバイスで設定されている場合に、同じデバイス上のあるマルチトポロジ ルーティング（MTR）トポロジから別のトポロジにルートをインポートする場合に実行します。この作業では、10.2.2.0 ネットワークからのプレフィックスを許可するためにプレフィックス リストが定義されます。このプレフィックス リストは、インポートされたトポロジから移動したルートをフィルタリングするために、ルートマップとともに使用されます。グローバル スコープが設定され、アドレス ファミリ IPv4 が入力されて、VIDEO トポロジが指定されます。また、VOICE トポロジがインポートされ、10NET という名前のルートマップを使用してルートがフィルタリングされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *number*] {**deny** | **permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*]
4. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
5. **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...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **scope** {**global** | **vrf** *vrf-name*}
9. **address-family ipv4**[**mdt** |**multicast** |**unicast**]
10. **topology** {**base** | *topology-name*}
11. **import topology** {**base** | *topology-name*} [**route-map** *map-name*]
12. **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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 prefix-list** *list-name* [**seq** *number*] {**deny** | **permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*] 例： `Device(config)# ip prefix-list TEN permit 10.2.2.0/24`	IP プレフィックス リストを設定します。 • この例では、プレフィックス リスト TEN は、**match ip address** コマンドによって設定されたマッチングに応じて、10.2.2.0/24 プレフィックスのアドバタイズを許可します。
ステップ 4	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map 10NET`	ルート マップを作成し、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。 • この例では、10NET という名前のルート マップが作成されます。
ステップ 5	**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...*]} 例： `Device(config-route-map)# match ip address prefix-list TEN`	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 リストにより許可されているプレフィックスと一致するルート マップを作成します。 • この例では、ルート マップは、プレフィックス リスト TEN によって許可されるプレフィックスのマッチングを行うよう設定されます。
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-number* 例： `Device(config)# router bgp 50000`	ルータ コンフィギュレーションモードを開始して、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを作成または設定します。

	コマンドまたはアクション	目的
ステップ 8	**scope** {**global** | **vrf** *vrf-name*} 例： `Device(config-router)# scope global`	BGP ルーティング プロセスに対してスコープを定義して、ルータ スコープ コンフィギュレーション モードを開始します。 • 単一のネットワークに適用される BGP の一般的なセッション コマンドまたは指定された仮想ルーティングおよび転送（VRF）が、このコンフィギュレーションモードで入力されます。 • BGP がグローバル ルーティング テーブルを使用することを指定するには、**global** キーワードを使用します。 • BGP が特定の VRF ルーティング テーブルを使用することを指定するには、**vrf** *vrf-name* キーワードおよび引数を使用します。VRF がすでに存在している必要があります。
ステップ 9	**address-family ipv4**[**mdt** |**multicast** |**unicast**] 例： `Device(config-router-scope)# address-family ipv4`	ルータ スコープ 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、BGP 下でアドレス ファミリ セッションを設定します。 • トポロジに固有ではない設定パラメータは、このコンフィギュレーション モードで設定されます。
ステップ 10	**topology** {**base** | *topology-name*} 例： `Device(config-router-scope-af)# topology VIDEO`	BGP がクラス固有のトポロジまたは基本トポロジのトラフィックをルーティングするトポロジ インスタンスを設定し、ルータ スコープ アドレス ファミリ トポロジ 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	**import topology** {**base** | *topology-name*} [**route-map** *map-name*] 例： `Device(config-router-scope-af-topo)# import topology VOICE route-map 10NET`	（任意）同じデバイス上のあるトポロジから別のトポロジにルートを移動するよう BGP を設定します。 • トポロジ間で移動するルートをフィルタ処理するには、**route-map** キーワードを使用できます。
ステップ 12	**end** 例： `Device(config-router-scope-af-topo)# end`	（任意）ルータ スコープ アドレス ファミリ トポロジ 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。

MTR に対する BGP サポートの設定例

例：BGP トポロジ変換コンフィギュレーション

次に、VIDEO トポロジにボーダー ゲートウェイ プロトコル（BGP）を設定し、192.168.2.2 ネイバーを使用してトポロジ変換を設定する例を示します。

```
router bgp 45000
 scope global
  neighbor 172.16.1.1 remote-as 50000
  neighbor 192.168.2.2 remote-as 55000
  neighbor 172.16.1.1 transport multi-session
  neighbor 192.168.2.2 transport multi-session
   address-family ipv4
    topology VIDEO
     bgp tid 100
     neighbor 172.16.1.1 activate
     neighbor 192.168.2.2 activate
     neighbor 192.168.2.2 translate-topology 200
     end
clear ip bgp topology VIDEO 50000
```

例：BGP のグローバル スコープおよび VRF コンフィギュレーション

次に、ユニキャスト トポロジとマルチキャスト トポロジのグローバル スコープを設定する例を示します。ルータ スコープ コンフィギュレーション モードの終了後に、DATA という名前の仮想ルーティングおよび転送（VRF）インスタンスについてスコープが設定されます。

```
router bgp 45000
 scope global
  bgp default ipv4-unicast
  neighbor 172.16.1.2 remote-as 45000
  neighbor 192.168.3.2 remote-as 50000
  address-family ipv4 unicast
   topology VOICE
   bgp tid 100
   neighbor 172.16.1.2 activate
   exit
  address-family ipv4 multicast
   topology base
    neighbor 192.168.3.2 activate
    exit
   exit
  exit
 scope vrf DATA
  neighbor 192.168.1.2 remote-as 40000
  address-family ipv4
   neighbor 192.168.1.2 activate
   end
```

例：BGP トポロジの確認

次に、**show ip bgp topology** コマンドの出力例を示します。VIDEO という名前のマルチトポロジ ルーティング（MTR）トポロジを使用するよう設定されたボーダー ゲートウェイ プロトコル（BGP）ネイバーに関する情報が表示されます。

```
Device# show ip bgp topology VIDEO summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.2      4 45000     289     289        1    0    0 04:48:44        0
192.168.3.2     4 50000       3       3        1    0    0 00:00:27        0
```

次の部分的な出力には、VIDEO トポロジ下に BGP ネイバー情報が表示されます。

```
Device# show ip bgp topology VIDEO neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 04:56:30
  Last read 00:00:23, last write 00:00:21, hold time is 180, keepalive interval is 60
seconds
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
  Message statistics, state Established:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           296        296
    Route Refresh:          0          0
    Total:                297        297
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast topology VIDEO
  Session: 172.16.1.2 session 1
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
1 update-group member
  Topology identifier: 100
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Minimum incoming TTL 0, Outgoing TTL 255
Local host: 172.16.1.1, Local port: 11113
Foreign host: 172.16.1.2, Foreign port: 179
.
.
.
```

例：BGP を使用した MTR トポロジからのルートのインポート

次に、VOICE という名前のルート マップが VOICE という名前のマルチトポロジ ルーティング（MTR）トポロジからインポートされたルートをフィルタリングするために使用するアクセス リストを設定する例を示します。プレフィックス 192.168.1.0 が付いたルートだけがインポートされます。

```
access-list 1 permit 192.168.1.0 0.0.0.255
route-map BLUE
 match ip address 1
 exit
router bgp 50000
 scope global
  neighbor 10.1.1.2 remote-as 50000
  neighbor 172.16.1.1 remote-as 60000
   address-family ipv4
    topology VIDEO
     bgp tid 100
     neighbor 10.1.1.2 activate
     neighbor 172.16.1.1 activate
     import topology VOICE route-map VOICE
     end
clear ip bgp topology VIDEO 50000
```

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』
マルチトポロジ ルーティング（MTR）コマンド	『Cisco IOS Multitopology Routing Command Reference』
ボーダー ゲートウェイ プロトコル（BGP）コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概念と作業	『*IP Routing: BGP Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

MTR に対する BGP サポー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。

表 *103 : MTR* に対する *BGP* サポートに関する機能情報

機能名	リリース	機能情報
MTR に対する BGP サポート	12.2(33)SRB 15.0(1)S	この機能により、単一の物理ネットワーク上の複数の論理トポロジに対するボーダーゲートウェイ プロトコル（BGP）サポートが実現します。 Cisco IOS XE Release 2.5 では、Cisco ASR 1000 シリーズ ルータのサポートが追加されました。 次のコマンドが導入または変更されました。**address-family ipv4**、**bgp tid**、**clear ip bgp topology**、**import topology**、**neighbor translate-topology**、**neighbor transport**、**scope**、**show ip bgp topology**、**topology**

第 84 章

BGP 累積 IGP

BGP 累積 IGP 機能は、任意の非推移的なボーダー ゲートウェイ プロトコル（BGP）パス属性です。累積内部ゲートウェイ プロトコル（AIGP）属性の属性タイプ コードは、Internet Assigned Numbers Authority（IANA）によって割り当てられます。AIGP 属性の値フィールドは、タイプ、長さ、値（TLV）要素のセットとして定義されます。AIGP TLV には、AIGP メトリックが含まれます。

- 機能情報の確認 （1295 ページ）
- BGP 累積 IGP に関する情報 （1296 ページ）
- BGP 累積 IGP の設定方法 （1297 ページ）
- BGP 累積 IGP の設定例 （1301 ページ）
- BGP 累積 IGP の追加情報 （1302 ページ）
- BGP 累積 IGP の機能情報 （1302 ページ）

機能情報の確認

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

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

BGP 累積 IGP に関する情報

BGP 累積 IGP の概要

BGP 累積 IGP 機能は、パスに関連付けられた距離を計算する現在の Open Shortest Path First（OSPF）の動作をシミュレートするために必要です。OSPF または Label Distribution Protocol（LDP; ラベル配布プロトコル）は、ローカル エリアでのみプレフィックスまたはラベル情報を伝送します。次に、ボーダー ゲートウェイ プロトコル（BGP）では、エリア境界にある BGP にルートを再配布することにより、すべてのリモート エリアにプレフィックスまたはラベルを伝送します。その後、ルートまたはラベルは、ラベルスイッチドパス（LSP）を使用してアドバタイズされます。ルートのネクストホップはローカルデバイスに対する各エリア境界ルータ（ABR）で変更されます。これによって、エリア境界を越えて OSPF ルートをリークする必要がなくなります。各コア リンクで使用可能な帯域幅が OSPF コストにマップされます。したがって、BGP では、各プロバイダー エッジ（PE）デバイス間でこのコストを正しく伝送する必要があります。この機能は、BGP 累積 IGP 機能を使用して実現されます。

累積内部ゲートウェイ プロトコル（AIGP）属性を伝送するには、内部ボーダー ゲートウェイ プロトコル（iBGP）および外部ボーダー ゲートウェイ プロトコル（eBGP）ネイバーで AIGP 処理を有効にする必要があります。AIGP 属性を使用して設定されたネイバーは、他の iBGP ネイバーとは別のアップデート グループに配置されます。コスト コミュニティへの AIGP 値の送信が有効化されているネイバーには、個別のアップデート グループが必要です。BGP では、AIGP 属性をコスト コミュニティまたは Multi-Exit 識別子（MED）に変換し、ルートに付加してからレガシーにアドバタイズする必要があります。

BGP が AIGP 属性ルートをルーティング情報ベース（RIB）にインストールすると、AIGP コストとネクストホップ コストが加算されます。ネクストホップが非再帰 IGP ルートである場合、BGP は、AIGP メトリックを受信した AIGP 値に設定し、第 1 ホップ IGP メトリックをネクストホップに設定します。ネクストホップが AIGP メトリックを持つ再帰 IGP ルートである場合、受信した AIGP メトリックがネクストホップ AIGP メトリックに加算されます。

BGP 累積 IGP の送受信

累積内部ゲートウェイ プロトコル（AIGP）属性を持つプレフィックスをセッションが受信した場合に、そのセッションが AIGP 情報を受け取るように設定されていないときは、そのセッションでは、AIGP 属性を破棄し、アップデート メッセージの残りの部分を処理してから、AIGP 属性を他の BGP ピアに渡します。次に、ルートがルーティング情報ベース（RIB）にインストールされ、プレフィックスが、AIGP 属性とともに、AIGP が有効なすべてのネイバーに送信されます。ネイバーにアドバタイズする前にルートのネクストホップがデバイスによって変更されていない場合、AIGP 属性値は更新されません。ルートのネクストホップが変更された場合は、受信した AIGP 属性値にネクストホップ メトリックを加算することによって AIGP 属性値が再計算されます。

累積 IGP を使用したプレフィックスの生成

累積内部ゲートウェイ プロトコル（AIGP）メトリックを使用したルートの生成は設定により制御されます。次の条件を満たす再配布ルートに AIGP 属性が付加されます。

- AIGP でルートを再配布するプロトコルが有効化されている。
- ルートが、ボーダー ゲートウェイ プロトコル（BGP）に再配布される内部ゲートウェイ プロトコル（IGP）ルートである。AIGP 属性に割り当てられた値が、ルートの IGP ネクストホップの値であるか、ルート ポリシーによって設定された値である。
- このルートは BGP に再配布されたスタティック ルートです。割り当てられた値が、ルートのネクストホップの値であるか、ルート ポリシーによって設定された値である。
- network コマンドによってルートが BGP にインポートされる。割り当てられた値が、ルートのネクストホップの値であるか、ルート ポリシーによって設定された値である。
- 着信ルート マップまたは発信ルート マップで、**set aigp-metric** コマンドを使用して AIGP 属性ルート マップも作成している。

BGP 累積 IGP の設定方法

AIGP メトリック値の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **redistribute** *protocol autonomous-system-number* **route-map** *map-tag*
6. **network** *network-id* **route-map** *map-tag*
7. **exit**
8. **route-map rtmap**
9. **set aigp-metric [igp-metric** | *value***]**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute** *protocol autonomous-system-number* **route-map** *map-tag* 例： `Device(config-router-af)# redistribute bgp 100 route-map rtmap`	あるルーティング ドメインから別のルーティング ドメインへルートを再配布します。
ステップ 6	**network** *network-id* **route-map** *map-tag* 例： `Device(config-router-af)# network 10.1.1.1 route-map rtmap`	ボーダーゲートウェイ プロトコル（BGP）ルーティング プロセスによってアドバタイズされるネットワークを指定します。
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、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	**route-map rtmap** 例： `Device(config)# route-map rtmap`	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 9	**set aigp-metric** [**igp-metric** | *value*] 例： `Device(config-route-map)# set aigp-metric igp-metric`	累積内部ゲートウェイ プロトコル（AIGP）属性のメトリック値を指定します。手動によるメトリック値は、0 ～ 4294967295 の範囲で指定します。
ステップ 10	**end** 例：	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 モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-route-map)# end`	

AIGP 属性の送受信の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family {ipv4 | ipv6}** [**unicast**]
5. **neighbor** *ip-address* **aigp**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family {ipv4 | ipv6}** [**unicast**] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 または IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** *ip-address* **aigp** 例： `Device(config-router-af)# neighbor 192.168.1.1 aigp`	ネイバーごとに AIGP 属性の送受信を有効にします。
ステップ 6	**end** 例：	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-router-af)# end`	

BGP 累積 IGP の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family {ipv4 | ipv6}** [**unicast**]
5. **neighbor** *ip-address* **aigp [send {cost-community** *community-id* **poi {igp-cost | pre-bestpath} [transitive]} | med]**
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* 例： `Device(config)# router bgp 40000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family {ipv4 | ipv6}** [**unicast**] 例： `Device(config-router)# address-family ipv4 unicast`	IPv4 または IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** *ip-address* **aigp [send {cost-community** *community-id* **poi {igp-cost | pre-bestpath} [transitive]} | med]** 例： `Device(config-router-af)# neighbor 192.168.1.1 aigp send med`	AIGP 属性を MED に変換し、ルートに付加してから、レガシー プロバイダー エッジ（PE）デバイスにアドバタイズします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BGP 累積 IGP の設定例

例：AIGP メトリック値の設定

次に、累積内部ゲートウェイプロトコル（AIGP）メトリック属性を使用してプレフィックスを生成するための設定例を示します。

```
Device# configure terminal
Device(config)# router bgp 40000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# redistribute bgp 100 route-map rtmap
Device(config-router-af)# network 10.1.1.1 route-map rtmap
Device(config-router-af)# exit
Device(config)# route-map rtmap
Device(config-route-map)# set aigp-metric igp-metric
Device(config-route-map)# end
```

例：AIGP 属性の送受信の有効化

次の例では、アドレス ファミリ コンフィギュレーション モードで AIGP 送受信機能を有効にする方法を示します。

```
Device# configure terminal
Device(config)# router bgp 40000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# neighbor 192.168.1.1 aigp
Device(config-router-af)# exit
```

例：BGP 累積 IGP の設定

次の例では、デバイスは自律システム 65000 に属しており、IP アドレス 172.16.70.23 のネイバーにコスト コミュニティ（cost-community）属性を送信するように設定します。

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 multicast
Device(config-router-af)# neighbor 172.16.70.23 aigp send cost-community 100 poi igp-cost
 transitive
Device(config-router-af)# exit
```

次の例では、デバイスは自律システム 65000 に属しており、IP アドレス 172.16.70.23 のネイバーに MED 属性を送信するように設定します。

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 multicast
Device(config-router-af)# neighbor 172.16.70.23 aigp send med
Device(config-router-af)# exit
```

BGP 累積 IGP の追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

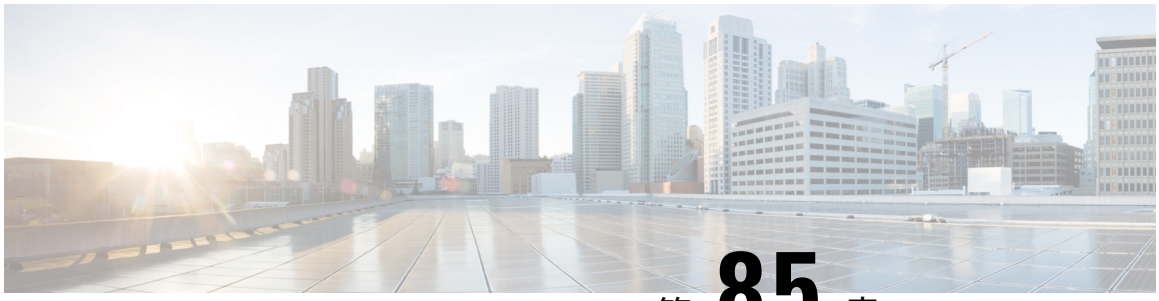
BGP 累積 IGP の機能情報

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 *104 : BGP* 累積 *IGP* の機能情報

機能名	リリース	機能情報
BGP 累積 IGP		BGP 累積 IGP 機能は、任意の非推移的なボーダー ゲートウェイ プロトコル（BGP）パス属性です。累積内部ゲートウェイ プロトコル（AIGP）属性の属性タイプ コードは、IANA によって割り当てられます。AIGP 属性の値フィールドは、タイプ、長さ、値（TLV）要素のセットとして定義されます。AIGP TLV には、AIGP メトリックが含まれます。 次のコマンドが導入されました。 **aigp**、**aigp send cost-community**、**aigp send med**、**bgp bestpath aigp ignore**、**set aigp-metric**



第 85 章

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング機能により、プロバイダー エッジ（PE）デバイスで、カスタマー エッジ（CE）デバイスから学習したルートまたは指定したネイバーの Virtual Routing and Forwarding（VRF）インスタンスで再配布されるルートへのマルチキャスト VPN（MVPN）関連拡張コミュニティの付加を抑制できます。

- 機能情報の確認 （1305 ページ）
- BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングに関する情報 （1306 ページ）
- BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定方法 （1306 ページ）
- BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定例 （1307 ページ）
- BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの追加情報 （1308 ページ）
- BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの機能情報 （1309 ページ）

機能情報の確認

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

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

BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングに関する情報

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの概要

VPN ルートは、マルチキャスト VPN（MVPN）をサポートするために、特別な拡張コミュニティ（送信元自律システム（AS）の拡張コミュニティおよび Virtual Routing and Forwarding（VRF）ルート インポート拡張コミュニティ）を伝送します。レガシー プロバイダー エッジ（PE）デバイスは、送信元 AS の拡張コミュニティを古いスタイルのマルチキャスト配信ツリー（MDT）として解釈します。拡張コミュニティは、プレフィックスの作成時に付加できます。BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング機能を有効にすると、PE デバイスでこれらの拡張コミュニティを抑制できます。この機能を使用すると、後続アドレス ファミリ識別子（SAFI）128 ルートについて拡張コミュニティが送信されないようにし、代わりに SAFI 129 を使用できます。SAFI 129 を使用するデバイスでは、送信元 AS の拡張コミュニティを正しく識別できる必要があります。

BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定方法

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **unicast-reachability** [**source-as** | **vrf-route-import**] [**disable**]
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 45000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **vrf** キーワードおよび *vrf-name* 引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**unicast-reachability** [**source-as** | **vrf-route-import**] [**disable**] 例： `Device(config-router-af)# unicast-reachability source-as disable`	非 MVPN プロファイルの拡張コミュニティのアドバタイズを無効にします。
ステップ 6	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

BGP MVPN 送信元 AS 拡張コミュニティ フィルタリングの設定例

例：BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの設定

次の例では、BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングを設定します。

```
Device# configure terminal
Device(config)# router bgp 45000
Device(config)# address-family ipv4 vrf vpn1
Device(config-router-af)# unicast-reachability source-as disable
Device(config-router-af)# exit
```

次に、 **show ip bgp vpnv4 vrf vpn1** コマンドの出力例を示します。

```
Device# show ip bgp vpnv4 vrf vpn1

BGP routing table entry for 10:10:1.1.1.1/32, version 25
Paths: (2 available, best #2, table red)
Multipath: eiBGP
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local, imported path from 10:11:1.1.1.1/32 (global)
    1.1.1.2 (metric 11) (via default) from 1.1.1.5 (1.1.1.5)
      Origin incomplete, metric 11, localpref 100, valid, internal
      Extended Community: RT:1:1 OSPF DOMAIN ID:0x0005:0x000000C80200
        MVPN AS:55:0.0.0.0 MVPN VRF:1.1.1.2:2 OSPF RT:0.0.0.0:2:0
        OSPF ROUTER ID:10.10.20.2:0
      Originator: 1.1.1.2, Cluster list: 1.1.1.5
      Connector Attribute: count=1
       type 1 len 12 value 10:11:1.1.1.2
      mpls labels in/out 20/21
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  Local
    10.10.10.100 (via vrf red) from 0.0.0.0 (1.1.1.1)
      Origin incomplete, metric 11, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:1:1 OSPF DOMAIN ID:0x0005:0x000000C80200
        MVPN VRF:1.1.1.1:1 OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:10.10.10.1:0
      mpls labels in/out 20/nolabel
      rx pathid: 0, tx pathid: 0x0
```

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』
BGP の概念と作業	『*IP Routing: BGP Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
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

BGP MVPN 送信元 AS の拡張コミュニティ フィルタリングの機能情報

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

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 *105 : BGP MVPN* 送信元 *AS* の拡張コミュニティ フィルタリングの機能情報

機能名	リリース	機能情報
BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング		BGP MVPN 送信元 AS の拡張コミュニティ フィルタリング機能により、プロバイダーエッジ（PE）デバイスで、カスタマーエッジ（CE）デバイスから学習したルートまたは指定したネイバーの Virtual Routing and Forwarding（VRF）インスタンスで再配布されるルートへのマルチキャスト VPN（MVPN）関連拡張コミュニティの付加を抑制できます。 次のコマンドが導入または変更されました。 **unicast-reachability**

第 86 章

BGP AS オーバーライド スプリットホライズン

BGP AS オーバーライド スプリットホライズン（as-override split-horizon）機能により、スプリットホライズンを使用するプロバイダーエッジ（PE）デバイスで、カスタマーエッジ（CE）デバイスから同じ CE デバイスに伝播されるルートをアドバタイズしないようにすることができます。また、BGP AS オーバーライド スプリットホライズン機能を使用すると、PE デバイスまたは CE デバイスで、同じレプリケーション グループ内の特定の PE デバイスまたは CE デバイスにルート アップデートを送信することもできます。

- 機能情報の確認 （1311 ページ）
- BGP AS オーバーライド スプリットホライズンに関する情報 （1312 ページ）
- BGP AS オーバーライド スプリットホライズンの設定方法 （1312 ページ）
- BGP AS オーバーライド スプリットホライズンの確認 （1314 ページ）
- BGP AS オーバーライドのスプリットホライズンの設定例 （1315 ページ）
- BGP AS オーバーライドのスプリットホライズンの追加情報 （1317 ページ）
- BGP AS オーバーライドのスプリットホライズンの機能情報 （1317 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 AS オーバーライド スプリットホライズンに関する情報

BGP AS オーバーライド スプリットホライズンの概要

スプリットホライズンをデバイスに設定すると、プロバイダー エッジ（PE）デバイスは、カスタマー エッジ（CE）デバイスから同じ CE デバイスに伝播されるルートをアドバタイズすることがあります。BGP AS オーバーライド スプリットホライズン機能では、すべての BGP ネイバーが同じアップデート グループに含まれている場合でも、それらのネイバーを個別のレプリケーション グループにグループ化して、CE デバイスから伝播されるルート アップデートが同じ CE デバイスに送信されないようにします。

BGP AS オーバーライド スプリットホライズン機能により、PE デバイスまたは CE デバイスは、同じアップデート グループ内の 1 つ以上の隣接する PE デバイスまたは CE デバイスに対してアップデートを選択的に送信およびブロックできます。PE デバイスまたは CE デバイスでは、メッセージのタイプ、およびメッセージの発信元が PE デバイスまたは CE デバイスのルータ ID と一致するかどうかに基づいて、隣接する PE デバイスまたは CE デバイスに対してメッセージを送信またはブロックします。

BGP AS オーバーライド スプリットホライズンの設定方法

BGP AS オーバーライド スプリットホライズンの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address family ipv4 vrf** *vrf-name*
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **activate**
7. **neighbor** *ip-address* **as-override split-horizon**
8. 手順 5 ～ 7 を繰り返して、Virtual Routing and Forwarding（VRF）インスタンスの各ネイバーについてスプリットホライズンを有効にします。
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 21`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address family ipv4 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv4 vrf vrf1`	後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VPN ルーティングおよび転送（VRF）インスタンスの名前を指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router-af)# neighbor 192.0.2.1 remote-as 1`	指定された自律システム内の BGP ネイバーとのピアリングを設定します。
ステップ 6	**neighbor** *ip-address* **activate** 例： `Device(config-router-af)# neighbor 192.0.2.1 activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 7	**neighbor** *ip-address* **as-override split-horizon** 例： `Device(config-router-af)# neighbor 192.0.2.1 as-override split-horizon`	VRF インスタンスのネイバーごとにスプリット ホライズンを有効にします。
ステップ 8	手順 5 ～ 7 を繰り返して、Virtual Routing and Forwarding（VRF）インスタンスの各ネイバーについてスプリット ホライズンを有効にします。	-

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-router-af)# end`	ルータ 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、特権 EXEC モードを開始します。

BGP AS オーバーライド スプリットホライズンの確認

手順の概要

1. **enable**
2. **show ip bgp vpn4 all update-group**
3. **show ip bgp vpnv4 all neighbors** *ip-address*
4. **show ip bgp vpnv4 all neighbors** *ip-address* **policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp vpn4 all update-group** 例： `Device# show ip bgp vpn4 all update-group`	アップデート グループの情報を表示します。
ステップ 3	**show ip bgp vpnv4 all neighbors** *ip-address* 例： `Device# show ip bgp vpnv4 all neighbors 192.0.2.1`	ネイバー接続の詳細を表示します。
ステップ 4	**show ip bgp vpnv4 all neighbors** *ip-address* **policy** 例： `Device# show ip bgp vpnv4 all neighbors 192.0.2.1 policy`	アドレス ファミリごとにネイバー ポリシーを表示します。

BGPASオーバーライドのスプリットホライズンの設定例

例：BGP AS オーバーライドのスプリットホライズンの設定

```
Device> enable
Device# configure terminal
Device(config)# router bgp 21
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# neighbor 192.0.2.1 remote-as 1
Device(config-router-af)# neighbor 192.0.2.1 activate
Device(config-router-af)# neighbor 192.0.2.1 as-override split-horizon
Device(config-router-af)# neighbor 198.51.100.1 remote-as 1
Device(config-router-af)# neighbor 198.51.100.1 activate
Device(config-router-af)# neighbor 198.51.100.1 as-override split-horizon
Device(config-router-af)# end
```

例：BGP AS オーバーライドのスプリットホライズンの確認

show ip bgp vpn4 all update-group コマンドの出力例

アップデート グループに関する情報を表示するには、特権 EXEC モードで **show ip bgp vpn4 all update-group** コマンドを使用します。

```
Device> enable
Device# show ip bgp vpn4 all update-group
BGP version 4 update-group 3, external, Address Family: VPNv4 Unicast
  BGP Update version : 5/0, messages 0 active RGs: 2 <<<<<<<<<<<<<
  Overrides the neighbor AS 1 with my AS before sending updates
  Topology: blue, highest version: 5, tail marker: 5
  Format state: Current working (OK, last not in list)
                Refresh blocked (not in list, last not in list)
  Update messages formatted 1, replicated 2, current 0, refresh 0, limit 1000
  Number of NLRIs in the update sent: max 4, min 0
  Minimum time between advertisement runs is 0 seconds
  Has 2 members:
   192.0.2.1         198.51.100.1
```

show ip bgp vpnv4 all neighbors *ip-address* コマンドの出力例

ネイバー接続に関する詳細を表示するには、特権EXECモードで **show ip bgp vpnv4 all neighbors** *ip-address* コマンドを使用します。

```
Device> enable
Device# show ip bgp vpnv4 all neighbors 209.165.200.228
BGP neighbor is 209.165.200.228,  vrf vrf1,  remote AS 1, external link
  BGP version 4, remote router ID 209.165.201.28
  BGP state = Established, up for 00:01:26
  Last read 00:00:35, last write 00:00:28, hold time is 180, keepalive interval is 60
seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
```

```
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                6          2
    Keepalives:             3          3
    Route Refresh:          0          0
    Total:                 12          6
  Default minimum time between advertisement runs is 0 seconds

 For address family: VPNv4 Unicast
  Translates address family IPv4 Unicast for VRF vrf1
  Session: 209.165.200.228
  BGP table version 40, neighbor version 40/0
  Output queue size : 0
  Index 1, Advertise bit 1
  1 update-group member
  Overrides the neighbor AS with my AS before sending updates
  Split horizon processing before sending updates
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:            10          2 (Consumes 160 bytes)
    Prefixes Total:              10          2
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          2
    Used as multipath:          n/a          0
Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 5, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Refresh Epoch: 1
  Last Sent Refresh Start-of-rib: 00:01:26
  Last Sent Refresh End-of-rib: 00:01:26
  Refresh-Out took 0 seconds
  Last Received Refresh Start-of-rib: never
  Last Received Refresh End-of-rib: never
                                     Sent       Rcvd
        Refresh activity:            ----       ----
          Refresh Start-of-RIB        1          0
          Refresh End-of-RIB          1          0

  Address tracking is enabled, the RIB does have a route to 209.165.200.228
  Connections established 3; dropped 2
  Last reset 00:01:35, due to split-horizon config change of session 1
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 1
Local host: 209.165.200.225, Local port: 22789
Foreign host: 209.165.200.228, Foreign port: 179
Connection tableid (VRF): 2
```

show ip bgp vpnv4 all neighbors *ip-address* policy コマンドの出力例

アドレス ファミリごとにネイバー ポリシーを表示するには、特権 EXEC モードで **show ip bgp vpnv4 all neighbors** *ip-address* **policy** コマンドを使用します。

```
Device> enable
Device# show ip bgp vpnv4 all neighbors 209.165.200.228
Neighbor: 209.165.200.228, Address-Family: VPNv4 Unicast (vrf1)
 Locally configured policies:
  as-override split-horizon
```

BGPASオーバーライドのスプリットホライズンの追加情報

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*』

シスコのテクニカル サポート

説明	リンク
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

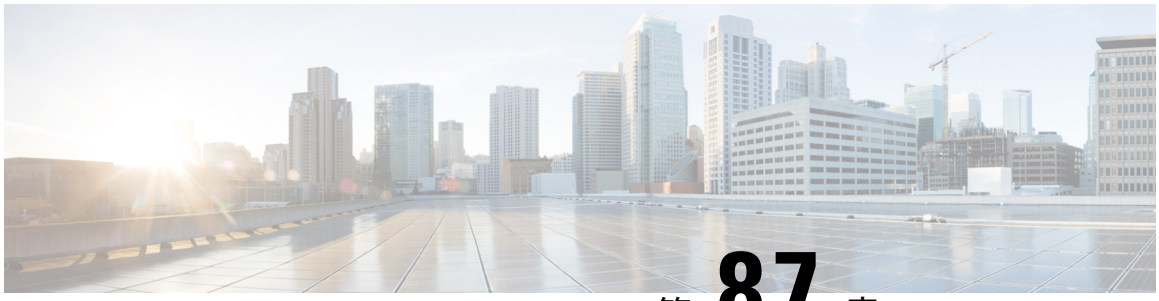
BGPASオーバーライドのスプリットホライズンの機能情報

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 *106* : *BGP AS* オーバーライドのスプリットホライズンの機能情報

機能名	リリース	機能情報
BGP AS オーバーライドのスプリットホライズン		BGP AS オーバーライドのスプリットホライズン（as-override split-horizon）機能により、スプリットホライズンを使用するプロバイダー エッジ（PE）デバイスで、カスタマー エッジ（CE）デバイスから同じ CE デバイスに伝播されるルートをアドバタイズしないようにすることができます。また、BGP AS オーバーライドのスプリットホライズン機能を使用すると、PE デバイスまたは CE デバイスで、同じレプリケーション グループ内の特定の PE デバイスまたは CE デバイスにルート アップデートを送信することもできます。 次のコマンドが導入または変更されました。**neighbor** *ip-address* **as-override split-horizon**



第 87 章

再配布ルートごとの複数送信元パスに対する BGP サポート

再配布ルートごとの複数送信元パスに対する BGP サポート機能は、BGP へのルート再配布またはその他のソーシングメカニズム（**network** コマンドなど）で複数のパスを使用できるようにします。この機能では、同じ送信元からの複数のパスを Virtual Routing and Forwarding（VRF）インスタンス間でインポートおよびエクスポートすることもできます。

このモジュールでは、機能の概要とその設定方法について説明します。

- 機能情報の確認 （1319 ページ）
- 再配布ルートごとの複数送信元パスに対する BGP サポートの制約事項 （1320 ページ）
- 再配布ルートごとの複数送信元パスに対する BGP サポートに関する情報 （1320 ページ）
- 再配布ルートごとの複数送信元パスに対する BGP サポートの設定方法 （1321 ページ）
- 再配布ルートごとの BGP 複数送信元パスの設定例 （1323 ページ）
- 再配布ルートごとの複数送信元パスに対する BGP サポートの追加情報 （1325 ページ）
- 再配布ルートごとの複数送信元パスに対する BGP サポートの機能情報 （1325 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。

再配布ルートごとの複数送信元パスに対するBGPサポートの制約事項

この機能には、次のような制約事項が適用されます。

- ゲートウェイ アドレスとして 0.0.0.0 を送信元とするパスでは、ボーダー ゲートウェイ プロトコル（BGP）に対して複数のパスが再配布されることはありません。そのため、すべての送信元パスには固有のゲートウェイがある必要があります。

再配布ルートごとの複数送信元パスに対するBGPサポートに関する情報

再配布ルートごとの複数送信元パスに対する BGP サポートの概要

再配布ルートごとの複数送信元パスに対する BGP サポート機能は、ボーダー ゲートウェイ プロトコル（BGP）へのルート再配布またはその他のソーシング メカニズム（**network** コマンドなど）で複数のパスを使用できるようにします。この機能が導入される前は、BGP では、再配布されるネットワークに対する単一の BGP 送信元パスを作成するために、同じネットワークに対するパスがルーティング情報ベース（RIB）に複数あったとしても、RIB から 1 つのパスしか受け入れませんでした。

この機能では、同じ送信元からの複数のパスを Virtual Routing and Forwarding（VRF）インスタンス間でインポートおよびエクスポートすることもできます。VRF インスタンスへのデフォルト パス以外のインポートは、以前から BGP でサポートされていました。ただし、これらの複数のパスは、同じ送信元からではなく、異なるネイバーまたは異なる送信元からのパスである必要がありました。

この機能を有効にすると、BGP を使用して、同じデバイス上で 1 つの VRF から数百の VRF に Equal Cost Multipath（ECMP; 等コスト マルチパス）の送信元パスまたはネクストホップをエクスポートできます。これらの各パスはマルチパスとして RIB にインストールされ、他の VRF でも ECMP パスを提供します。

BGP で RIB 内の再配布プロトコルからのルートごとのパスまたはネクストホップをすべて受け入れるようにするには、**bgp sourced-paths** コマンドを設定します。このコマンドを無効にした場合、または有効にしていない場合、BGP では、RIB からネットワークごとに 1 つの送信元パスしかインポートできません。

再配布ルートごとの複数送信元パスに対するBGPサポートの設定方法

複数発信元パスの設定

bgp sourced-paths コマンドを設定すると、ボーダー ゲートウェイ プロトコル（BGP）はルーティング情報ベース（RIB）からすべてのパスを受け入れます。**bgp sourced-paths** コマンドを削除すると、RIB から BGP へはネットワークごとに 1 つしか送信元パスが許可されないというデフォルトの動作に設定が戻ります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **bgp sourced-paths per-net static all**
6. **redistribute static**
7. **neighbor** *ip-address* **remote-as** *neighbor-as*
8. **neighbor** *ip-address***activate**
9. **neighbor** *ip-address***send-community both**
10. **end**

手順の詳細

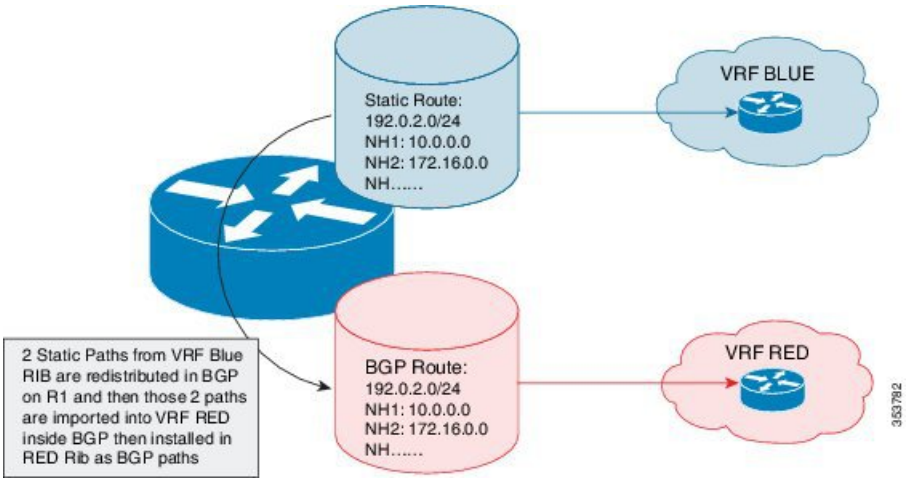
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、ルーティング 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 blue`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。 （注） また、ネットワーク設定に基づいて **address-family ipv6** コマンドを設定することもできます。
ステップ 5	**bgp sourced-paths per-net static all** 例： `Device(config-router-af)# bgp sourced-paths per-net static all`	ネットワークごとに RIB 内のすべてのスタティック パスを送信元とすることを許可します。
ステップ 6	**redistribute static** 例： `Device(config-router-af)# redistribute static`	別のルーティング プロトコルからスタティック ルートを再配布します。
ステップ 7	**neighbor** *ip-address* **remote-as** *neighbor-as* 例： `Device(config-router-af)# neighbor 204.0.0.3 remote-as 65000`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 8	**neighbor** *ip-address***activate** 例： `Device(config-router-af)# neighbor 204.0.0.3 activate`	BGP ネイバーとの情報交換を有効にします。
ステップ 9	**neighbor** *ip-address***send-community both** 例： `Device(config-router-af)# neighbor 204.0.0.3 send-community both`	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

再配布ルートごとの BGP 複数送信元パスの設定例

例：複数送信元パスの設定

図 *96 : BGP* 複数パス レプリケーションの展開シナリオ



上の図は、BGP で VRF BLUE から VRF RED に複数のパスを複製する展開シナリオを示しています。VRF RED では、VRF BLUE と VRF RED で同じルート ターゲット エクスポートを使用することで、ベストパスに加えて、他のパスもインポートできます。これにより、複数のパスを VRF RED に挿入できます。

```
Device# configure terminal
Device(config)# ip vrf blue
Device(config-vrf)# rd 100:200
Device(config-vrf)# route-target export 200:200
Device(config-vrf)# route-target import 200:200
Device(config-vrf)# exit

Device(config)# ip vrf red
Device(config-vrf)# rd 200:200
Device(config-vrf)# route-target export 300:200
Device(config-vrf)# route-target import 300:200
Device(config-vrf)# route-target import 200:200
Device(config-vrf)# exit

Device(config)# interface Loopback 0
Device(config-if)# ip address 198.51.100.1 255.255.255.255
Device(config-if)# exit

Device(config)# interface Ethernet 1/0
Device(config-if)# ip address 203.0.113.1 19.0.0.32 255.255.255.255
Device(config-if)# no shutdown
Device(config-if)# exit

Device(config)# interface Ethernet 1/2
Device(config-if)# ip address 209.165.200.225 255.255.255.240
Device(config-if)# no shutdown
```

```
Device(config-if)# exit

Device(config)# interface Ethernet 1/2.2
Device(config-subif)# encapsulation dot1Q 2
Device(config-subif)# ip vrf forwarding blue
Device(config-subif)# ip address 192.168.0.1 255.255.255.240
Device(config-subif)# no shutdown
Device(config-subif)# exit

Device(config)# interface Ethernet 1/2.3
Device(config-subif)# encapsulation dot1Q 3
Device(config-subif)# ip vrf forwarding blue
Device(config-subif)# ip address 1922.168.0.17 255.255.255.240
Device(config-subif)# no shutdown
Device(config-subif)# exit

Device(config)# router ospf 2 vrf blue
Device(config-router)# network 192.68.0.0 0.0.0.255 area 0
Device(config-router)# network 192.68.1.16 0.0.0.255 area 0
Device(config-router)# exit
!
Device(config)# router ospf 1
Device(config-router)# network 209.165.200.224 0.0.255.255 area 0
Device(config-router)# exit

Device(config)# router bgp 65000
Device(config-router)# no bgp default ipv4-unicast
Device(config-router)# neighbor 10.0.0.2 remote-as 65000
Device(config-router)# neighbor 10.0.0.2 update-source Loopback0
Device(config-router)# address-family ipv4
Device(config-router-af)# exit-address-family

Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor 10.0.0.2 activate
Device(config-router-af)# neighbor 10.0.0.2 send-community extended
Device(config-router-af)# exit-address-family

Device(config-router)# address-family ipv4 vrf blue
Device(config-router-af)# bgp sourced-paths per-net static all
Device(config-router-af)# bgp sourced-paths per-net ospf all
Device(config-router-af)# redistribute static
Device(config-router-af)# redistribute ospf 2
Device(config-router-af)# exit-address-family

Device(config-router)# address-family ipv4 vrf red
Device(config-router-af)# import path selection all
Device(config-router-af)# import path limit 2
Device(config-router-af)# maximum-paths 2
Device(config-router-af)# exit-address-family
Device(config-router)# exit

Device(config)# ip route vrf blue 192.0.2.2 255.255.255.255 10.0.0.2 global
Device(config)# ip route vrf blue 192.0.2.2 255.255.255.255 172.16.0.2 global
Device(config)# end
```

再配布ルートごとの複数送信元パスに対するBGPサポートの追加情報

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』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

シスコのテクニカル サポート

説明	リンク
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

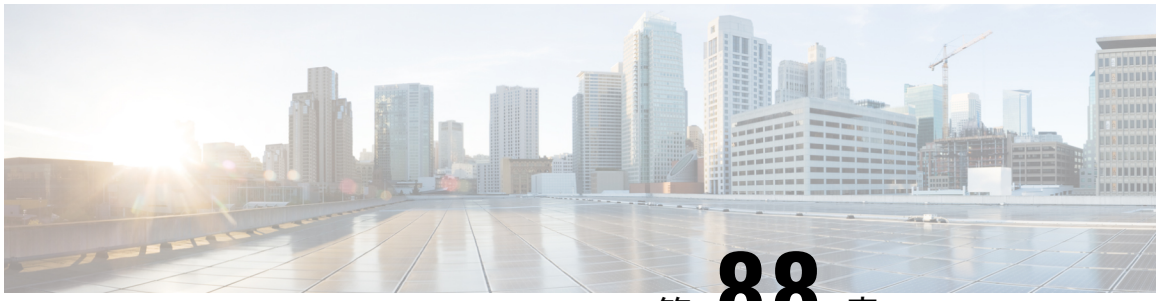
再配布ルートごとの複数送信元パスに対するBGPサポートの機能情報

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 *107 :* 再配布ルートごとの複数送信元パスに対する *BGP* サポートの機能情報

機能名	リリース	機能情報
再配布ルートごとの複数送信元パスに対する BGP サポート	Cisco IOS XE Release 3.15S	再配布ルートごとの複数送信元パスに対する BGP サポート機能は、BGP へのルート再配布またはその他のソーシング メカニズム（**network** コマンドなど）で複数のパスを使用できるようにします。この機能では、同じ送信元からの複数のパスを Virtual Routing and Forwarding（VRF）インスタンス間でインポートおよびエクスポートすることもできます。 この機能は、Cisco IOS XE Release 3.15S で、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。 **bgp sourced-paths** コマンドが導入されました。



第 88 章

メンテナンス機能：BGP ルーティング プロトコル

Cisco IOS XE Everest 16.4.1 リリースから、BGP でイベント トレース機能がサポートされています。イベント トレース機能では、コマンドを使用してイベント トレースを有効にすることで、BGP トレースをキャプチャできます。トレースをログに記録しない場合は、コマンドを無効にすることができます。コンバージェンスが発生して接続状態が変更されると、BGP トレースがイベント トレース インフラストラクチャに記録されます。

- 機能情報の確認 （1327 ページ）
- メンテナンス機能：BGP ルーティング プロトコルに関する情報 （1328 ページ）
- グローバル コンフィギュレーション モードでの BGP イベント トレースの設定 （1328 ページ）
- EXEC モードでの BGP イベント トレースの設定 （1329 ページ）
- BGP イベント トレースの確認 （1330 ページ）
- メンテナンス機能：BGP ルーティング プロトコルの機能情報 （1331 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。

メンテナンス機能：BGP ルーティング プロトコルに関する情報

BGP イベント トレースは、次の機能をサポートしています。

- BGP イベント トレースは、ピア接続状態の変更用のバッファを作成し、イベント ロギングを更新します。バッファのサイズは 100,000 で、100,000 のトレース エントリが一度に格納されることを意味します。バッファのサイズはコンフィギュレーション コマンドを使用して変更でき、バッファの最大サイズは 1,000,000 まで拡張できます。
- このバッファは循環式であるため、バッファの最後に到達すると、最初からログ記録が開始されます。「ワンショット（one-shot）」が設定されていない場合は、最初からログ記録が継続されます。
- パフォーマンスに若干の影響があることを考慮して、BGP イベント トレースはデフォルトでは無効になっています。これは、EXEC モードで **enable** コマンドを実行することによって有効化できます。
- BGP イベント トレース：
  - ネイバー：状態変更、エラー処理、認識できないパケットや不正なパケットの処理など、すべてのピア イベントがこのバッファにキャプチャされます。
- BGP では、実行時にバイナリ形式のトレースが対応するバッファに記録されるため、トレースを効率的にログ記録できます。**monitor event-trace bgp neighbor** コマンドを使用すると、人間が判読できる形式でトレースがコンソールに出力されます。このコマンドでは、イベント トレースをバイナリ形式または人間が判読できる形式でファイルにダンプすることもできます。
- show コマンドには、イベント ログを表示するための afi/safi/vrf/neighbor アドレス フィルタリング オプションが用意されています。異なる afi/safi/vrf でのイベント トレース ロギングは、完全に異なるトレースに基づきます。

グローバル コンフィギュレーション モードでの BGP イベント トレースの設定

BGP イベント トレースでは、接続状態のイベント トレース用にグローバル コンフィギュレーション モードおよび特権 EXEC モードのコマンドが用意されています。BGP のイベント トレースを有効にするには、次の設定手順を使用します。この設定では、アクティブ/スタンバイ ルータがクラッシュやスイッチオーバーにより再起動されると、BGP トレースが有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **monitor event-trace bgp neighbor** {**dump-file** *filename* | **size** *entries*}
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**monitor event-trace bgp neighbor** {**dump-file** *filename*	**size** *entries*} 例： `Device(config)# monitor event-trace bgp neighbor size 10`	BGP のイベント トレースを有効にします。 イベント トレースを無効にするには、**no monitor event-trace bgp neighbor** コマンドを使用します。 • **dump-file**：トレース ダンプ ファイルの名前を設定します。 • **size**：トレースのサイズを設定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

EXEC モードでの BGP イベント トレースの設定

手順の概要

1. **enable**
2. **monitor event-trace bgp neighbor** {**clear** | **continuous** | **destroy-buffer** | **disable** | **dump** *filename* | **enable** | **one-shot**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor event-trace bgp neighbor** {**clear** | **continuous** | **destroy-buffer** | **disable** | **dump** *filename* | **enable** | **one-shot**} 例： `Device# monitor event-trace bgp neighbor enable`	BGP のイベント トレースを有効にします。 イベント トレースを無効にするには、**no monitor event-trace bgp neighbor** コマンドを使用します。 • **clear**：イベント トレース バッファをクリアします。 • **continuous**：ログ記録されているイベント トレースをコンソールに継続的に表示します。 • **destroy-buffer**：トレース用に割り当てられたバッファを破棄します。 • **disable**：イベント トレース機能を無効にします。アクティブ ノードとスタンバイ ノードの両方を無効にするには、このコマンドを両方のノードに対して指定する必要があります。 • **dump** *filename*：すべてのネイバー イベント トレースをバイナリ形式または ASCII 形式でファイルにダンプします。 • **enable**：イベント トレース機能を有効にします。アクティブ ノードとスタンバイ ノードの両方を有効にするには、このコマンドを両方のノードに対して指定する必要があります。 • **one-shot**：イベント トレースを 1 回だけログに記録します。バッファがいっぱいになると、イベント トレース ロギングは停止します。
ステップ 3	**exit** 例： `Device# exit`	特権 EXEC コンフィギュレーション モードを終了します。

BGP イベント トレースの確認

次の **show** コマンドを使用して、キャプチャされたイベント トレースを参照できます。これらの **show** コマンドは、AFI/SAFI/VRF/neighbor アドレスおよびさまざまな組み合わせに基づいてトレースをフィルタ処理します。

- **show monitor event-trace bgp all**
- **show monitor event-trace bgp back**
- **show monitor event-trace bgp clock**
- **show monitor event-trace bgp from-boot**
- **show monitor event-trace bgp ipv4** {**all** | **back** | **clock** | **flowspec** | **from-boot** | **latest** | **mdt** | **multicast** | **mvpn** | **unicast**}
- **show monitor event-trace bgp ipv4 flowspec neighbors**
- **show monitor event-trace bgp ipv4 mdt vrf**
- **show monitor event-trace bgp ipv6** {**all** | **back** | **clock** | **flowspec** | **from-boot** | **latest** | **multicast** | **mvpn** | **unicast**}
- **show monitor event-trace bgp l2vpn** {**all** | **back** | **clock** | **evpn** | **from-boot** | **latest** | **vpls**}
- **show monitor event-trace bgp latest**
- **show monitor event-trace bgp neighbors**
- **show monitor event-trace bgp nsap**
- **show monitor event-trace bgp parameters**
- **show monitor event-trace bgp rtfilter**
- **show monitor event-trace bgp vpnv4** {**all** | **back** | **clock** | **from-boot** | **latest** | **vrf**}
- **show monitor event-trace bgp vpnv6** {**all** | **back** | **clock** | **flowspec** | **from-boot** | **latest** | **multicast** | **unicast**}

メンテナンス機能：BGP ルーティング プロトコルの機能情報

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 *108 :* メンテナンス機能：*BGP* ルーティング プロトコルの機能情報

機能名	リリース	機能情報
メンテナンス機能：BGP ルーティング プロトコル	Cisco IOS XE Everest 16.4.1 リリース	Cisco IOS XE Everest 16.4.1 リリースから、BGP でイベント トレース機能がサポートされています。イベント トレース機能では、コマンドを使用してイベント トレースを有効にすることで、BGP トレースをキャプチャできます。トレースをログに記録しない場合は、コマンドを無効にすることができます。コンバージェンスが発生して接続状態が変更されると、BGP トレースがイベント トレース インフラストラクチャに記録されます。