IP ルーティング：BGP コンフィギュレーション ガイド、Cisco IOS Release 15.1S

IP Routing: BGP Configuration Guide, Cisco IOS Release 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

IP ルーティング : BGP コンフィギュレーション ガイド、Cisco IOS Release 15.1S

BGP 機能のロードマップ

この機能のロードマップでは、『*Cisco IOS IP ルーティング：BGP コンフィギュレーション ガイド*』に記載されている Cisco IOS の機能をリストし、各機能の説明があるドキュメントにマッピングします。ロードマップは、ご使用のリリース群を選択し、該当リリースでの機能を確認できるよう構成されています。お探しの機能名を検索し、「参照先」列に記載されている URL をクリックして、機能の記載を含むドキュメントにアクセスしてください。

機能およびリリースでのサポート

表 1 に、次の Cisco IOS ソフトウェア リリース群の Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）機能のサポートを示します。

- 「Cisco IOS Release 12.0S」
- 「Cisco IOS Release 12.2S」
- 「Cisco IOS Release 12.2SB」
- 「Cisco IOS Release 12.2SR」
- 「Cisco IOS Release 12.2SX」
- 「Cisco IOS Release 12.2T、12.3、12.3T、12.4 および 12.4T」
- 「Cisco IOS Release 15.1T」
- 「Cisco IOS Release 15.0S」
- 「Cisco IOS Release 15.1S」

プラットフォームのサポートおよびソフトウェア 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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1 に、各ソフトウェア群の最新のリリースを最初に、また、リリース内の機能をアルファベット順で示します。

表 1　サポートする BGP 機能

リリース	機能名	機能の説明	参照先
Cisco IOS Release 12.0S			
12.0(32)S12	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。自律システム番号の要求の増加に伴い、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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す。	『Cisco BGP Overview』 『Configuring a Basic BGP Network』
12.0(31)S	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。	『Connecting to a Service Provider Using External BGP』
12.0(31)S	BFD に対する BGP サポート	Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。	『Configuring Advanced BGP Features』
12.0(29)S	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。	『Configuring BGP Neighbor Session Options』
12.0(29)S	グローバル テーブルから Virtual private network Routing and Forwarding（VRF; VPN ルーティング/転送）テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.0(29)S	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、Routing Information Base（RIB; ルーティング情報ベース）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 サイクル間での最良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。	『Configuring Advanced BGP Features』
12.0(27)S	EIGRP MPLS VPN PE-CE に対する BGP コスト コミュニティ サポート	EIGRP Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）PE-CE に対する BGP コスト コミュニティ サポート機能は、バックドア ルータを含む多様な EIGRP MPLS VPN ネットワーク トポロジに対して BGP コスト コミュニティ サポートを提供します。	『BGP Cost Community』
12.0(27)S	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。	『Configuring BGP Neighbor Session Options』
12.0(27)S	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、external Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）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。	『Configuring BGP Neighbor Session Options』
12.0(26)S	BGP MIB サポート拡張機能	BGP MIB サポート拡張機能によって、新しい Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知用に CISCO-BGP4-MIB のサポートが導入されました。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.0(26)S	Regex エンジン パフォーマンス拡張機能	Regex エンジン パフォーマンス拡張機能により、複雑な正規表現を処理するよう設計された新しい正規表現エンジンが導入されます。この新しい正規表現エンジンは既存のエンジンを置き換えません。既存のエンジンは単純な正規表現に適しており、これは Cisco IOS ソフトウェアでのデフォルトのエンジンです。いずれかのエンジンを Command-Line Interface（CLI; コマンドライン インターフェイス）から選択できます。	『Regex Engine Performance Enhancement』
12.0(24)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	ピア テンプレートを使用したボーダー ゲートウェイ プロトコル（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。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。	『Configuring a Basic BGP Network』
12.0(24)S	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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、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、最良パス選択プロセスに反映させることができます。	『BGP Cost Community』
12.0(24)S	BGP ダイナミック アップデート ピア グループ	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。	『Configuring a Basic BGP Network』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.0(24)S	BGP リンク帯域幅	ボーダー ゲートウェイ プロトコル（BGP）Link Bandwidth 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 アトリビュートは、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。	『BGP Link Bandwidth』
12.0(24)S	MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能によって、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を使用するように設定されたボーダー ゲートウェイ プロトコル（BGP）ネットワークで、外部 BGP（eBGP）パスおよび内部 BGP（iBGP）パスの両方を使用してマルチパス ロード バランシングを設定できます。この機能によって、ロード バランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホーム ネットワークおよびスタブ ネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよび Provider Edge（PE; プロバイダー エッジ）ルータのために役立ちます。	『BGP Multipath Load Sharing for eBGP and iBGP in an MPLs VPN』
12.0(24)S	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 マップ設定に導入されます。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。	『Connecting to a Service Provider Using External BGP』
12.0(22)S	BGP 条件付きルートの挿入	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クスよりも、より具体的なプレフィクスを 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。	『Configuring a Basic BGP Network』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.0(22)S	BGP ハイブリッド CLI	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 Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）形式から Address Family Identifier（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。	『Configuring a Basic BGP Network』
12.0(22)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	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。	『Connecting to a Service Provider Using External BGP』
12.0(22)S	BGP ネクストホップ伝播	BGP ネクストホップ伝播機能により、ネットワークの設計およびマイグレーションを行うときの柔軟性が高まります。BGP ネクストホップ伝播機能では、反映されたルートのネクストホップ アトリビュートをルート リフレクタによって変更でき、ネクストホップ アトリビュートを変更せずに BGP によって外部 BGP（eBGP）マルチホップ ピアにアップデートを送信できます。	『BGP Next Hop Propagation』
12.0(22)S	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。	『BGP Policy Accounting Output Interface Accounting』
12.0(22)S	BGP プレフィクスベース アウトバウンド ルート フィルタリング	BGP プレフィクスベース アウトバウンド ルート フィルタリング機能は、BGP Outbound Route Filtering（ORF; アウトバウンド ルート フィルタリング）送受信機能を使用して、BGP ピアの間で送られる BGP アップデートの数を最小化します。この機能を設定すると、不要なルーティング アップデートをソースでフィルタリングできるため、ルーティング アップデートの生成や処理に必要なシステム リソースの数を減らす助けになります。たとえば、この機能を使用して、サービス プロバイダー ネットワークからのルート全体を受け付けるのではないルータで、ルータに要求される処理の量を減らすことができます。	『Connecting to a Service Provider Using External BGP』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.0(22)S	最大プレフィクス制限後の BGP 再起動セッション	最大プレフィクス制限後の BGP 再起動セッション機能により、**restart** キーワードが導入されて、**neighbor maximum-prefix** コマンドの機能が拡張されます。この機能拡張により、ネットワーク オペレータは、ピアから受信したプレフィクス数が最大プレフィクス制限を超えたときに、ピアリング セッションが別のルータによって再確立される時間間隔を設定できます。	『Configuring BGP Neighbor Session Options』
12.0(22)S	BGP ルート マップ ポリシー リスト サポート	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。	『Connecting to a Service Provider Using External BGP』
12.0(21)S	ピアごとの受信ルートに対する BGP 4 MIB サポート	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タを（Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コマンドを使用して）照会する機能を提供する CISCO-BGP4-MIB で新しいテーブルを導入します。	『BGP 4 MIB Support for per-Peer Received Routes』
12.0(9)S	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 Internet Protocol（IP; インターネット プロトコル）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 Policy Accounting』
Cisco IOS Release 12.2S			
12.2(25)S	EIGRP MPLS VPN PE-CE に対する BGP コスト コミュニティ サポート	EIGRP MPLS VPN PE-CE に対する BGP コスト コミュニティ サポート機能は、バックドア ルータを含む多様な EIGRP MPLS VPN ネットワーク トポロジに対して BGP コスト コミュニティ サポートを提供します。	『BGP Cost Community』
12.2(25)S	BGP MIB サポート拡張機能	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。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(25)S	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。	『Configuring BGP Neighbor Session Options』
12.2(25)S	グローバル テーブルから VRF テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』
12.2(25)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	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。	『Connecting to a Service Provider Using External BGP』
12.2(25)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	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。	『Connecting to a Service Provider Using External BGP』
12.2(25)S	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。	『Configuring BGP Neighbor Session Options』
12.2(25)S	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	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、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。	『Loadsharing IP Packets Over More Than Six Parallel Paths』
12.2(25)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	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。	『Configuring a Basic BGP Network』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(22)S	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。	『BGP Policy Accounting Output Interface Accounting』
12.2(22)S	Regex エンジン パフォーマンス拡張	Regex エンジン パフォーマンス拡張機能により、複雑な正規表現を処理するよう設計された新しい正規表現エンジンが導入されます。この新しい正規表現エンジンは既存のエンジンを置き換えません。既存のエンジンは単純な正規表現に適しており、これは Cisco IOS ソフトウェアでのデフォルトのエンジンです。いずれかのエンジンをコマンドライン インターフェイス（CLI）から選択できます。	『Regex Engine Performance Enhancement』
12.2(18)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	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。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。	『Configuring a Basic BGP Network』
12.2(18)S	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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、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、最良パス選択プロセスに反映させることができます。	『BGP Cost Community』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(18)S	BGP ダイナミック アップデート ピア グループ	BGP ダイナミック アップデート ピア グループ機能により、アウトバウンド ポリシーを共有し、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。	『Configuring a Basic BGP Network』
12.2(18)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	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。	『Connecting to a Service Provider Using External BGP』
12.2(18)S	最大プレフィクス制限後の BGP 再起動セッション	最大プレフィクス制限後の BGP 再起動セッション機能により、**restart** キーワードが導入されて、**neighbor maximum-prefix** コマンドの機能が拡張されます。この機能拡張により、ネットワーク オペレータは、ピアから受信したプレフィクス数が最大プレフィクス制限を超えたときに、ピアリング セッションが別のルータによって再確立される時間間隔を設定できます。	『Configuring BGP Neighbor Session Options』
12.2(18)S	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 マップ設定に導入されます。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。 アウトバウンド ルート マップの continue 句は、Cisco IOS Release 12.0(31)S 以降のリリースだけでサポートされています。	『Connecting to a Service Provider Using External BGP』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(18)S	BGP ルート マップ ポリシー リスト サポート	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。	『Connecting to a Service Provider Using External BGP』
12.2(14)S	ピアごとの受信ルートに対する BGP 4 MIB サポート	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タを（Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コマンドを使用して）照会する機能を提供する CISCO-BGP4-MIB で新しいテーブルを導入します。	『BGP 4 MIB Support for per-Peer Received Routes』
12.2(14)S	BGP 条件付きルートの挿入	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クスよりも、より具体的なプレフィクスを 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。	『Configuring a Basic BGP Network』
12.2(14)S	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 アトリビュートは、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。	『BGP Link Bandwidth』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(14)S	MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能によって、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を使用するように設定されたボーダー ゲートウェイ プロトコル（BGP）ネットワークで、外部 BGP（eBGP）パスおよび内部 BGP（iBGP）パスの両方を使用してマルチパス ロード バランシングを設定できます。この機能によって、ロード バランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホーム ネットワークおよびスタブ ネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよびプロバイダー エッジ（PE）ルータのために役立ちます。	『BGP Multipath Load Sharing for eBGP and iBGP in an MPLs VPN』
12.2(14)S	BGP 名前付きコミュニティ リスト	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 アトリビュート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。	『Connecting to a Service Provider Using External BGP』
12.2(14)S	BGP ネクストホップ伝播	BGP ネクストホップ伝播機能により、ネットワークの設計およびマイグレーションを行うときの柔軟性が高まります。BGP ネクストホップ伝播機能では、反映されたルートのネクストホップ アトリビュートをルート リフレクタによって変更でき、ネクストホップ アトリビュートを変更せずに BGP によって外部 BGP（eBGP）マルチホップ ピアにアップデートを送信できます。	『BGP Next Hop Propagation』
12.2(14)S	BGP プレフィクスベース アウトバウンド ルート フィルタリング	BGP プレフィクスベース アウトバウンド ルート フィルタリング機能は、BGP ORF 送受信機能を使用して、BGP ピアの間で送られる BGP アップデートの数を最小化します。この機能を設定すると、不要なルーティング アップデートをソースでフィルタリングできるため、ルーティング アップデートの生成や処理に必要なシステム リソースの数を減らす助けになります。たとえば、この機能を使用して、サービス プロバイダー ネットワークからのルート全体を受け付けるのではないルータで、ルータに要求される処理の量を減らすことができます。	『Connecting to a Service Provider Using External BGP』
12.2(14)S	iBGP のマルチパス ロード シェアリング	iBGP のマルチパス ロード シェアリング機能を使用すると、BGP 対応ルータがイネーブルになり、複数の iBGP パスを宛先への最良パスとして選択できます。この最良パスまたはマルチパスは、次にこのルータの IP ルーティング テーブルにインストールされます。	『iBGP Multipath Load Sharing』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
Cisco IOS Release 12.2SB			
12.2(33)SB	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。	『Configuring Advanced BGP Features』
12.2(33)SB	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。	『Configuring a Basic BGP Network』
12.2(33)SB	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SB	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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。	『Configuring Advanced BGP Features』
12.2(31)SB2	BGP ルータ ID の VRF 単位の割り当て	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。	『Per-VRF Assignment of BGP Router ID』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(31)SB	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。	『Configuring BGP Neighbor Session Options』
12.2(31)SB	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。	『Configuring Advanced BGP Features』 『Configuring BGP Neighbor Session Options』
12.2(31)SB	セッションごとの TCP の PMTUD に対する BGP サポート	Transmission Control Protocol（TCP; 伝送制御プロトコル）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、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。	『Configuring BGP Neighbor Session Options』
12.2(28)SB	ピアごとの受信ルートに対する BGP 4 MIB サポート	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タを（Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コマンドを使用して）照会する機能を提供する CISCO-BGP4-MIB で新しいテーブルを導入します。	『BGP 4 MIB Support for per-Peer Received Routes』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	Nonstop Routing（NSR; ノンストップ ルーティング）with Stateful Switchover（SSO; ステートフル スイッチオーバー）に対する BGP サポート	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 サポート機能により、プロバイダー エッジ（PE）ルータは Customer Edge（CE; カスタマー エッジ）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、Route Processor（RP; ルート プロセッサ）スイッチオーバー中または PE ルータに対する定期的な In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）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 NonStop Forwarding（NSF; ノンストップ フォワーディング）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。	『BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)』
12.2(27)SBC	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	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。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。	『Configuring a Basic BGP Network』
12.2(27)SBC	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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、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、最良パス選択プロセスに反映させることができます。	『BGP Cost Community』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(27)SBC	BGP ダイナミック アップデート ピア グループ	BGP ダイナミック アップデート ピア グループ機能により、アウトバウンド ポリシーを共有し、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。	『Configuring a Basic BGP Network』
12.2(27)SBC	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	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。	『Connecting to a Service Provider Using External BGP』
12.2(27)SBC	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 マップ設定に導入されます。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。 アウトバウンド ルート マップの continue 句は、Cisco IOS Release 12.0(31)S 以降のリリースだけでサポートされています。	『Connecting to a Service Provider Using External BGP』
12.2(27)SBC	BGP ルート マップ ポリシー リスト サポート	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。	『Connecting to a Service Provider Using External BGP』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(27)SBC	グローバル テーブルから VRF テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』
12.2(27)SBC	名前付き拡張コミュニティ リストに対する BGP サポート	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。	『Connecting to a Service Provider Using External BGP』
12.2(27)SBC	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	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。	『Connecting to a Service Provider Using External BGP』
Cisco IOS Release 12.2SR			
12.2(33)SRE	IP および MPLS-VPN 向け BGP PIC エッジ	IP および MPLS-VPN 向け BGP PIC エッジ機能は、障害が生じた場合すぐにバックアップ パスが引き継ぎ、サブセカンド フェールオーバーがイネーブル化されるように、ルーティング情報ベース（RIB）および Cisco Express Forwarding にバックアップ パスを作成、保存します。	『BGP PIC Edge for IP and MPLS-VPN』
12.2(33)SRE	BGP 最良外部	IP および MPLS-VPN 向け BGP PIC エッジ機能は、障害が生じた場合すぐにバックアップ パスが引き継ぎ、サブセカンド フェールオーバーがイネーブル化されるように、ルーティング情報ベースおよび Cisco Express Forwarding にバックアップ パスを作成、保存します。	『BGP Best External』
12.2(33)SRE	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。自律システム番号の要求の増加に伴い、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す。	『Cisco BGP Overview』 『Configuring a Basic BGP Network』 『Connecting to a Service Provider Using External BGP』 『BGP per Neighbor SoO Configuration』
12.2(33)SRC	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。	『Configuring Advanced BGP Features』
12.2(33)SRC	BGP MIB サポート拡張機能	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。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRB	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。	『Configuring a Basic BGP Network』
12.2(33)SRB	BGP のネイバーごとの SoO 設定	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。以前のリリースでは、SoO パラメータは、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。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。	『BGP per Neighbor SoO Configuration』
12.2(33)SRB	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SRB	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。	『Configuring Advanced BGP Features』 『Configuring BGP Neighbor Session Options』
12.2(33)SRB	MTR に対する BGP サポート	Multi-Topology Routing（MTR）に対する BGP サポートによって、MTR トポロジをサポートするために新しい設定階層とコマンドライン インターフェイス（CLI）コマンドが導入されました。新しい設定階層、つまりスコープは、MTR とは関係なく BGP によって実装できます。MTR によって、クラスベースの転送によってサービスの区別化を設定できます。MTR では、複数のユニキャスト トポロジと別個のマルチキャスト トポロジがサポートされます。トポロジは、一連の独立したネットワーク レイヤ到着可能性情報（NLRI）によって特徴付けられる、基礎となるネットワーク（または基本トポロジ）のサブセットです。 12.2(33)SRB では、この機能が Cisco 7600 シリーズ ルータで追加されました。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRB	L2VPN アドレス ファミリに対する BGP サポート	Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）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。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 Support for the L2VPN Address Family』
12.2(33)SRB	Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）に対する Multiprotocol BGP（MP-BGP; マルチプロトコル BGP）サポート	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 Open System Interconnection（OSI; 開放型システム間相互接続）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。	『Multiprotocol BGP (MP-BGP) Support for the CLNS』
12.2(33)SRA	BGP MIB サポート拡張機能	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。	『Configuring Advanced BGP Features』
12.2(33)SRA	BFD に対する BGP サポート	Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRA	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。	『Configuring BGP Neighbor Session Options』
12.2(33)SRA	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。	『Configuring BGP Neighbor Session Options』
12.2(33)SRA	グローバル テーブルから VRF テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』
12.2(33)SRA	名前付き拡張コミュニティ リストに対する BGP サポート	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SRA	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	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SRA	セッションごとの TCP の PMTUD に対する BGP サポート	Transmission Control Protocol（TCP; 伝送制御プロトコル）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、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。	『Configuring BGP Neighbor Session Options』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRA	BGP ルータ ID の VRF 単位の割り当て	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。	『Per-VRF Assignment of BGP Router ID』
Cisco IOS Release 12.2SX			
12.2(33)SXI1	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。自律システム番号の要求の増加に伴い、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す。	『Cisco BGP Overview』 『Configuring a Basic BGP Network』
12.2(33)SXI	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SXH	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。3 つの **show** コマンドの出力は、ダイナミック ネイバーに関する情報を表示するようにアップデートされています。	『Configuring BGP Neighbor Session Options』
12.2(33)SXH	BGP MIB サポート拡張機能	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。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SXH	BFD に対する BGP サポート	Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。	『Configuring Advanced BGP Features』
12.2(33)SXH	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。	『Configuring BGP Neighbor Session Options』
12.2(33)SXH	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。	『Configuring BGP Neighbor Session Options』
12.2(33)SXH	グローバル テーブルから VRF テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』
12.2(33)SXH	名前付き拡張コミュニティ リストに対する BGP サポート	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。	『Connecting to a Service Provider Using External BGP』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SXH	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 サイクル間での最良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。	『Configuring Advanced BGP Features』
12.2(33)SXH	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	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。	『Connecting to a Service Provider Using External BGP』
12.2(33)SXH	セッションごとの TCP の PMTUD に対する BGP サポート	Transmission Control Protocol（TCP; 伝送制御プロトコル）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、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。	『Configuring BGP Neighbor Session Options』
12.2(33)SXH	BGP ルータ ID の VRF 単位の割り当て	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。	『Per-VRF Assignment of BGP Router ID』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SXH	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	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。	『Configuring a Basic BGP Network』
12.2(18)SXE	MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能によって、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を使用するように設定されたボーダー ゲートウェイ プロトコル（BGP）ネットワークで、外部 BGP（eBGP）パスおよび内部 BGP（iBGP）パスの両方を使用してマルチパス ロード バランシングを設定できます。この機能によって、ロード バランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホーム ネットワークおよびスタブ ネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよびプロバイダー エッジ（PE）ルータのために役立ちます。	『BGP Multipath Load Sharing for eBGP and iBGP in an MPLs VPN』
12.2(18)SXE	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。	『Configuring BGP Neighbor Session Options』
Cisco IOS Release 12.2T、12.3、12.3T、12.4 および 12.4T			
12.4(24)T	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。自律システム番号の要求の増加に伴い、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す。	『Cisco BGP Overview』 『Configuring a Basic BGP Network』
12.4(20)T	セッションごとの TCP の PMTUD に対する BGP サポート	Transmission Control Protocol（TCP; 伝送制御プロトコル）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、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。	『Configuring BGP Neighbor Session Options』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.4(20)T	BGP ルータ ID の VRF 単位の割り当て	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。	『Per-VRF Assignment of BGP Router ID』
12.4(11)T	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。	『Configuring a Basic BGP Network』
12.4(11)T	BGP のネイバーごとの SoO 設定	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。Cisco IOS Release 12.4(9)T、12.2(33)SRA、およびこれら以前のリリースでは、SoO パラメータは、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。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。	『BGP per Neighbor SoO Configuration』
12.4(4)T	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。	『Connecting to a Service Provider Using External BGP』
12.4(4)T	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。	『Configuring Advanced BGP Features』 『Configuring BGP Neighbor Session Options』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.4(4)T	BFD に対する BGP サポート	Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。	『Configuring Advanced BGP Features』
12.3(14)T	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。	『Configuring BGP Neighbor Session Options』
12.3(14)T	グローバル テーブルから VRF テーブルへの IP プレフィ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。	『BGP Support for IP Prefix Import from Global Table into a VRF Table』
12.3(14)T	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 サイクル間での最良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。	『Configuring Advanced BGP Features』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.3(11)T	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。	『Configuring BGP Neighbor Session Options』
12.3(11)T	名前付き拡張コミュニティ リストに対する BGP サポート	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。	『Connecting to a Service Provider Using External BGP』
12.3(11)T	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	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。	『Connecting to a Service Provider Using External BGP』
12.3(8)T	EIGRP MPLS VPN PE-CE に対する BGP コスト コミュニティ サポート	EIGRP MPLS VPN PE-CE に対する BGP コスト コミュニティ サポート機能は、バックドア ルータを含む多様な EIGRP MPLS VPN ネットワーク トポロジに対して BGP コスト コミュニティ サポートを提供します。	『BGP Cost Community』
12.3(7)T	BGP MIB サポート拡張機能	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。	『Configuring Advanced BGP Features』
12.3(7)T	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。	『Configuring BGP Neighbor Session Options』
12.3(4)T	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	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。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。	『Configuring a Basic BGP Network』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.3(4)T	BGP ダイナミック アップデート ピア グループ	BGP ダイナミック アップデート ピア グループ機能により、アウトバウンド ポリシーを共有し、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。	『Configuring a Basic BGP Network』
12.3(4)T	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。	『BGP Policy Accounting Output Interface Accounting』
12.3(4)T	Regex エンジン パフォーマンス拡張	Regex エンジン パフォーマンス拡張機能により、複雑な正規表現を処理するよう設計された新しい正規表現エンジンが導入されます。この新しい正規表現エンジンは既存のエンジンを置き換えません。既存のエンジンは単純な正規表現に適しており、これは Cisco IOS ソフトウェアでのデフォルトのエンジンです。いずれかのエンジンを Command-Line Interface（CLI; コマンドライン インターフェイス）から選択できます。	『Regex Engine Performance Enhancement』
12.3(2)T	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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、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、最良パス選択プロセスに反映させることができます。	『BGP Cost Community』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.3(2)T	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 マップ設定に導入されます。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。	『Connecting to a Service Provider Using External BGP』
12.3(2)T	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	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、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。	『Loadsharing IP Packets Over More Than Six Parallel Paths』
12.2(15)T	BGP ハイブリッド CLI	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。	『Configuring a Basic BGP Network』
12.2(15)T	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	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。	『Connecting to a Service Provider Using External BGP』
12.2(15)T	BGP ノンストップ フォワーディング（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。	『Configuring Advanced BGP Features』
12.2(15)T	最大プレフィクス制限後の BGP 再起動セッション	最大プレフィクス制限後の BGP 再起動セッション機能により、**restart** キーワードが導入されて、**neighbor maximum-prefix** コマンドの機能が拡張されます。この機能拡張により、ネットワーク オペレータは、ピアから受信したプレフィクス数が最大プレフィクス制限を超えたときに、ピアリング セッションが別のルータによって再確立される時間間隔を設定できます。	『Configuring BGP Neighbor Session Options』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(15)T	BGP ルート マップ ポリシー リスト サポート	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。	『Connecting to a Service Provider Using External BGP』
12.2(13)T	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。	『BGP Policy Accounting』
12.2(8)T	BGP 名前付きコミュニティ リスト	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 アトリビュート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。	『Connecting to a Service Provider Using External BGP』
12.2(8)T	CLNS に対するマルチプロトコル BGP（MP-BGP）サポート	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。	『Multiprotocol BGP (MP-BGP) Support for the CLNS』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(4)T	BGP 条件付きルートの挿入	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クスよりも、より具体的なプレフィクスを 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。	『Configuring a Basic BGP Network』
12.2(4)T	MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング	eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能によって、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）を使用するように設定されたボーダー ゲートウェイ プロトコル（BGP）ネットワークで、外部 BGP（eBGP）パスおよび内部 BGP（iBGP）パスの両方を使用してマルチパス ロード バランシングを設定できます。この機能によって、ロード バランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホーム ネットワークおよびスタブ ネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよびプロバイダー エッジ（PE）ルータのために役立ちます。	『BGP Multipath Load Sharing for eBGP and iBGP in an MPLs VPN』
12.2(4)T	BGP プレフィクスベース アウトバウンド ルート フィルタリング	BGP プレフィクスベース アウトバウンド ルート フィルタリング機能は、BGP ORF 送受信機能を使用して、BGP ピアの間で送られる BGP アップデートの数を最小化します。この機能を設定すると、不要なルーティング アップデートをソースでフィルタリングできるため、ルーティング アップデートの生成や処理に必要なシステム リソースの数を減らす助けになります。たとえば、この機能を使用して、サービス プロバイダー ネットワークからのルート全体を受け付けるのではないルータで、ルータに要求される処理の量を減らすことができます。	『Connecting to a Service Provider Using External BGP』
12.2(2)T	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 アトリビュートは、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。	『BGP Link Bandwidth』
12.2(2)T	iBGP のマルチパス ロード シェアリング	iBGP のマルチパス ロード シェアリング機能を使用すると、BGP 対応ルータがイネーブルになり、複数の iBGP パスを宛先への最良パスとして選択できます。この最良パスまたはマルチパスは、次にこのルータの IP ルーティング テーブルにインストールされます。	『iBGP Multipath Load Sharing』
Cisco IOS Release 15.1T			

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
15.1(2)T	BGP - プライベート AS の削除および交換	プライベート Autonomous System Number（ASN; 自律システム番号）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 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 ASN を削除することが必要です。	『Removing Private AS Numbers from the AS Path in BGP』
Cisco IOS Release 15.0S			
15.0(1)S	BGP - プライベート AS の削除および交換	プライベート Autonomous System Number（ASN; 自律システム番号）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 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 ASN を削除することが必要です。	『Removing Private AS Numbers from the AS Path in BGP』
15.0(1)S	BGP 低速ピア	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。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。	『Detecting and Mitigating a BGP Slow Peer』
15.0(1)S	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。	『Configuring BGP Neighbor Session Options』

表 1　サポートする BGP 機能 （続き）

リリース	機能名	機能の説明	参照先
15.0(1)S	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 サポートと In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）	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 サポート機能により、プロバイダー エッジ（PE）ルータは Customer Edge（CE; カスタマー エッジ）ルータとともに BGP の状態を維持でき、Route Processor（RP; ルート プロセッサ）スイッチオーバー中または PE ルータに対する定期的な In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）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 Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)』
Cisco IOS Release 15.1S			
15.1(1)S	BGP：RT 制約ルート配布	BGP：ルート ターゲット（RT）制約ルート配布は、ルート リフレクタ（RR）が RR および 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ために、サービス プロバイダが MPLS L3VPN で使用する機能です。アップデートを減らすことにより、リソースを節約できます。	『BGP: RT Constrained Route Distribution』

Cisco BGP の概要

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。Cisco IOS に実装された BGP バージョン 4 のソフトウェアでは、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 version 4（IPv4; IP バージョン 4）、IP version 6（IPv6; IP バージョン 6）、Virtual Private Networks version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、Connectionless Network Service（CLNS; コネクションレス型ネットワークサービス）、Layer 2 VPN（L2VPN; レイヤ 2 VPN）を含む Internet Protocol（IP; インターネット プロトコル）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 Cisco IOS 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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「Cisco BGP 概要の機能情報」（P.19）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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 Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）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

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 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。Transmission Control Protocol（TCP; 伝送制御プロトコル）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

TCP ポートは 179 に割り当てられており、ローカル ポートはランダムなポート番号に割り当てられています。Cisco IOS 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 プロバイダーがインターネットを構築するために使用されています。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、external BGP（eBGP; 外部 BGP）ピアリング セッションが作成されます。BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）と呼ばれてはいますが、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。同一組織内の BGP ピアは、internal BGP（iBGP; 内部 BGP）ピアリング セッションによってルーティング情報を交換します。BGP ピア セッションの設定および基本的な BGP ネットワークを構築するその他の作業の詳細については、「Configuring a Basic BGP Network」モジュールを参照してください。

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、パス固有のアトリビュート、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、Autonomous System（AS; 自律システム）アトリビュートに含まれます。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、ループが作成され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 ネイバーのピア セッションに関連するさまざまなオプションを設定する設定作業の詳細については、「Configuring BGP Neighbor Session Options」モジュールを参照してください。

デフォルトでは、BGP は宛先ホストまたはネットワークへの最良パスとして 1 つのパスを選択します。最良パス選択アルゴリズムによりパス アトリビュートが分析され、BGP ルーティング テーブル内でどのルートが最良パスとしてインストールされているかが判断されます。各パスでは、BGP 最良パス分析で使用されるウェルノウンの必須の遷移アトリビュート、ウェルノウンの任意の遷移アトリビュート、およびオプションの遷移アトリビュートが伝送されます。Cisco IOS ソフトウェアには、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用してこれらのアトリビュートの一部を変更し BGP パス選択に反映させる機能があります。BGP パス選択は、BGP 標準ポリシーの設定にも影響されます。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リングすることの詳細については、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。

BGP では、最良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、許可される最大数よりも多くの全体的に良好なマルチパスが存在する場合、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。iBGP ピアリング セッションの設定作業を含む BGP の拡張機能の設定に関する詳細は、「Configuring Advanced BGP Features」モジュールを参照してください。

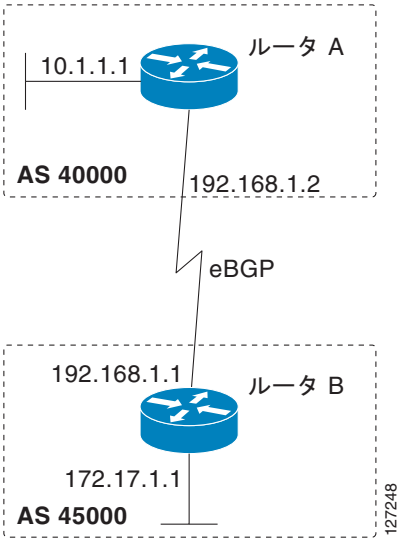
BGP 自律システム

自律システムは、単一のテクニカル アドミニストレーション エンティティによって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。この設定により、ルーティング ドメインの管理および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。

図 1 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、Internet Service Provider（ISP; インターネット サービス プロバイダー）のルータです。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

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、RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述された、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、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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。表 1 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

形式	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 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、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。表 2 および 表 3 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るとはいえ、**show** コマンド出力と正規表現を用いた 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** コマンドをイネーブルにした後で、**clear ip bgp *** コマンドを入力し、すべての BGP セッションについて、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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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、Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）がサポートされています。

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 スペース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。Cisco IOS 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 はデフォルトでイネーブルになっています。CIDR をイネーブル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

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 レイヤ 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 レイヤ 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 レイヤ 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 レイヤ 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 レイヤ 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、Protocol Independent Multicast（PIM; プロトコル独立型マルチキャスト）機能で使用され、データ分散ツリーが構築されます。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 トラフィックへの専用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 Network Access Point（NAP; ネットワーク アクセス ポイント）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、Reverse Path Forwarding（RPF; リバース パス フォワーディング）によるマルチキャスト対応ソースの検索、および Multicast Distribution Tree（MDT; マルチキャスト分散ツリー）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 Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）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。

図 2 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

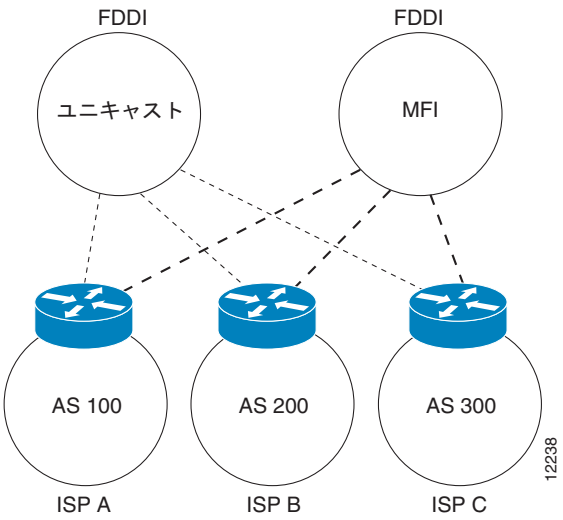
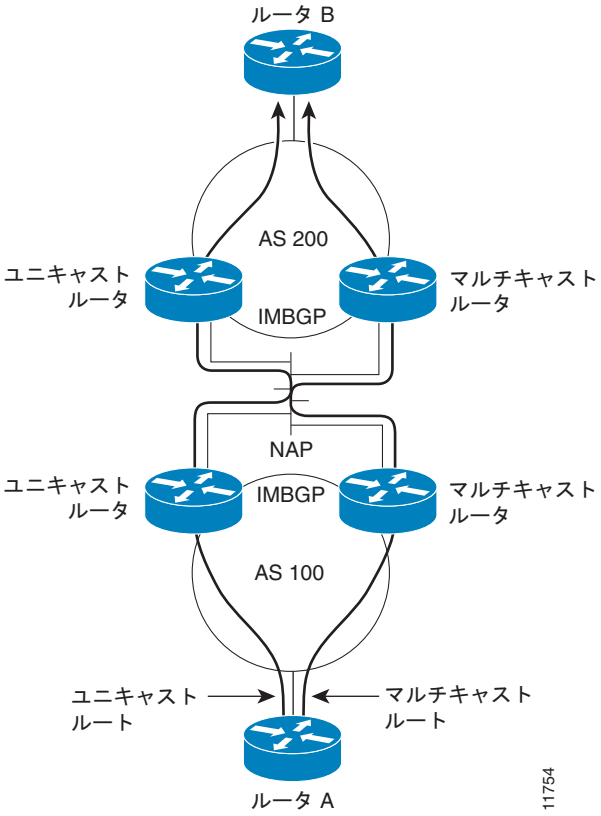


図 3 は、ユニキャストだけに対応したルータおよびマルチキャストだけに対応したルータのトポロジです。左側にある 2 つのルータはユニキャストだけに対応しています（マルチキャスト ルーティングをサポートしていないか、マルチキャスト ルーティングを実行するよう設定されていない）。右側にある 2 つのルータはマルチキャストだけに対応したルータです。ルータ A および B は、ユニキャストおよびマルチキャスト ルーティングの両方をサポートしています。ユニキャストだけに対応したルータおよびマルチキャストだけに対応したルータは、1 つの NAP に接続されています。

図 3 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 に移動し、その逆の経路で戻ります。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 ルートがイネーブル化され、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 トラフィックには、ルータ A からマルチキャスト ルータを経由しルータ B に移動し、その逆の経路で戻るパスが使用されます。

図 3 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 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、「Configuring Basic IP Multicast」モジュールを参照してください。

NLRI コンフィギュレーション CLI

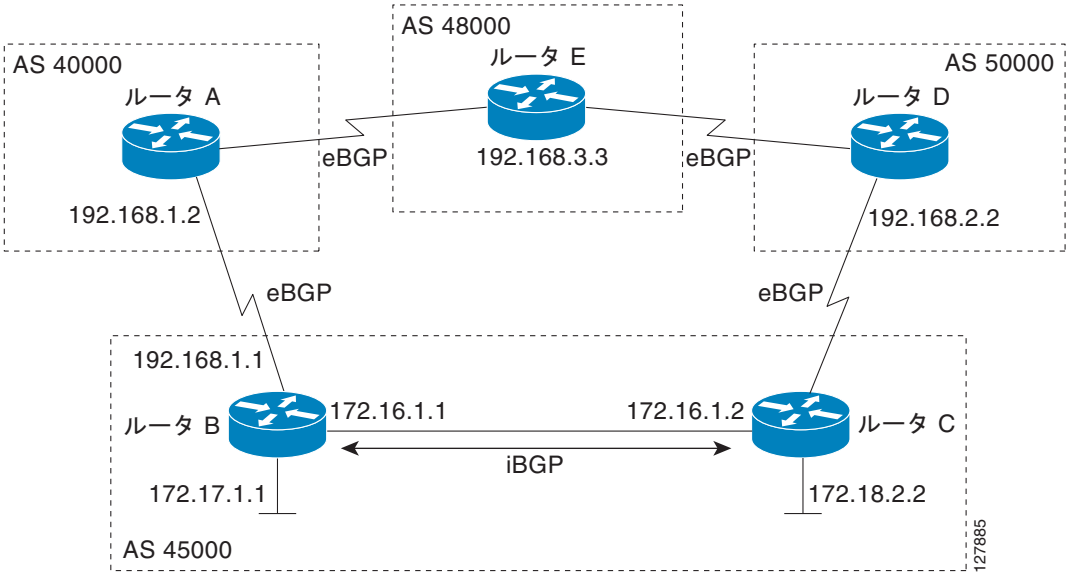
BGP は、ユニキャストの IPv4 ルーティング情報だけを伝送するように設計されました。Cisco IOS ソフトウェアの BGP 設定では、ネットワーク レイヤ到着可能性情報（NLRI）形式 CLI が使用されました。NLRI 形式では、マルチキャスト ルーティング情報のサポートは限られており、複数のネットワーク レイヤ プロトコルはサポートされません。BGP 設定に NLRI 形式 CLI を使用することは推奨できません。BGP ハイブリッド CLI 機能を使用すれば、アドレス ファミリ VPNv4 形式でコマンドを設定し、既存の NLRI でフォーマットされた構成を変更することなく、これらのコマンド 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 コマンド使用の詳細については、「Configuring a Basic BGP Network」モジュールを参照してください。アドレス ファミリ設定形式について、および NLRI CLI 形式の制限についての詳細は、「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」の概念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更に増してお

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図 4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。図 4 に示されている個別の各自律システムでは、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）および IPv6 などのいくつかのルーティング プロトコルを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 レイヤ 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 アトリビュート（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 レイヤ 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 Routing and Forwarding（VRF; VPN ルーティング/転送）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 Virtual Private LAN Service（VPLS; バーチャル プライベート LAN サービス）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。表 4 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	参考資料
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

表 4　Cisco IOS ソフトウェアでサポートされる SAFI （続き）

SAFI フィールド値	説明	参考資料
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 固有アトリビュートおよびトンネル 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遷移コネクタ アトリビュートで、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、Provider Edge（PE; プロバイダー エッジ）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 Customer Edge（CE; カスタマーエッジ）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 Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレス プレフィクスを使用する 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 プレフィクスが設定されたとき、ユニキャスト アドレス プレフィ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 Data Communications Network（DCN; データ通信ネットワーク）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 サポートの詳細については、「Configuring Multiprotocol BGP (MP-BGP) support for CLNS」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 プレフィクスが設定されたとき、ユニキャスト アドレス プレフィ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クスのレプリケーションを許可する Route Descriptor（RD; ルート ディスクリプタ）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、Electronic Data Interchange（EDI; 電子データ交換）、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 スペースは、設計によりグローバル アドレス スペースから隔離されます。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

Cisco IOS Release 12.2(33)SRB およびそれ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。L2VPN は、IP Security（IPsec; IP セキュリティ）または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）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 Routing Information Base（RIB; ルーティング情報ベース）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。プレフィクスおよびパス情報は L2VPN データベースに保存され、最良パスが 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 バーチャル プライベート LAN サービス（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、Cisco IOS Release 12.2(33)SRB の「BGP Support for the L2VPN Address Family」機能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。多くの BGP CLI コマンドは、CLI コンフィギュレーションのその他の部分に影響します。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 Enhanced Interior Gateway Routing Protocol（EIGRP; 拡張内部ゲートウェイ ルーティング プロトコル）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リングされて 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** 形式は機能をディセーブルにします。しかし、この CLI コンフィギュレーションの例では、単にルート マップをディセーブルにしただけではルート再配布は停止しません。フィルタリングまたはルート マップからの一致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に予期しない結果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 マップなどの他のコマンド タイプが含まれたコンフィギュレーション コマンドは、組み込まれているコマンドの削除により生じる影響を軽減するために、コンフィギュレーション コマンド自体も削除または変更する必要があるか検討する必要があります。

次の CLI 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の削除設定についての詳細は、「Configuring a Basic BGP Network」モジュールを参照してください。

次の作業

「Configuring a Basic BGP Network」モジュールに進みます。

参考資料

関連資料

関連項目	参照先
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 基本作業の設定	「Configuring a Basic BGP Network」モジュール
BGP ネイバー セッション オプションの設定	「Configuring BGP Neighbor Session Options」モジュール
サービス プロバイダー接続の BGP 設定	「Connecting to a Service Provider Using External BGP」モジュール
内部 BGP（iBGP）設定作業	「Configuring Internal BGP Features」モジュール
BGP の拡張機能の設定	「Configuring Advanced BGP Features」モジュール
マルチプロトコル BGP と CLNS の設定	「Configuring Multiprotocol BGP (MP-BGP) Support for CLNS」モジュール
基本 IP マルチキャスト 設定作業	「Configuring Basic IP Multicast」モジュール

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 5 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 5 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 5　Cisco BGP 概要の機能情報

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	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 15.0(1)S Cisco IOS XE 3.1.0SG	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、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す。 Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、および 12.2(33)SXI1 では、シスコは 4 バイト自律システム番号の実装時に、asplain 形式を正規表現マッチングのデフォルト、また自律システム番号の出力表示形式として使用しています。しかし、RFC 5396 が記述する asplain と asdot 形式のどちらでも、4 バイト自律システム番号を設定できます。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** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 自律システム番号の形式」（P.4） この機能により、次の各コマンドが追加または変更されています。**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**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 5　Cisco BGP 概要の機能情報 （続き）

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	12.2(33)SRB	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ました。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。 次のセクションで、この機能に関する情報を参照できます。 • 「Cisco BGP アドレス ファミリ モデル」（P.10） • 「L2VPN アドレス ファミリ」（P.15） この機能により、次の各コマンドが追加または変更されています。**address-family l2vpn**、**show ip bgp l2vpn**。
CLNS に対するマルチプロトコル BGP サポート設定	12.2(33)SRB	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 Open System Interconnection（OSI; 開放型システム間相互接続）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。 次のセクションで、この機能に関する情報を参照できます。 • 「Cisco BGP アドレス ファミリ モデル」（P.10） • 「CLNS アドレス ファミリ」（P.14） この機能により、次のコマンドが導入または変更されています。**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 およびマルチプロトコル BGP)**、**redistribute (BGP から ISO ISIS)**、**redistribute (ISO ISIS から 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**、**show bgp nsap summary**。

表 5　Cisco BGP 概要の機能情報 （続き）

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 レイヤ 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 レイヤ 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。 この機能に関する詳細については、次の各項を参照してください。 • 「マルチプロトコル BGP」（P.7） • 「BGP に対しマルチプロトコル BGP を使用する利点」（P.7） • 「IP マルチキャストのマルチプロトコル BGP 拡張」（P.8）

基本 BGP ネットワーク設定

このモジュールでは、基本的な Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「基本 BGP ネットワーク設定の機能情報」（P.93）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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

基本 BGP ネットワーク設定の前提条件

基本 BGP 作業を設定する前に、「Cisco BGP Overview」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

- 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。

基本 BGP ネットワーク設定の概要

基本 BGP ネットワークを設定するには、次の概念について理解する必要があります。

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 Cisco IOS ソフトウェア実装には、BGP が 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できるようにするマルチプロトコル拡張機能と、IP Version 4（IPv4; IP バージョン 4）、IP Version 6（IPv6; IP バージョン 6）、Virtual Private Networks Version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、および Connectionless Network Services（CLNS; コネクションレス型ネットワーク サービス）を含む複数のレイヤ 3 プロトコル アドレス ファミリが組み込まれています。

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、external BGP（eBGP; 外部 BGP）ピアリング セッションが作成されます。BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）と呼ばれますが、組織内のネットワークの多くが複雑になってきているため、BGP を使用して、組織内で使用される内部ネットワークを簡略化することができます。同一組織内の BGP ピアは、internal BGP（iBGP; 内部 BGP）ピアリング セッションによっ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 スピーカーとピア関係

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。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 対応ルータです。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、その間に他のルータ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 ルータのことで、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、またはルーティング 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 ルータは、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。

外部 BGP ピアの詳細については、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。内部 BGP ピアの詳細については、「Configuring Internal BGP Features」モジュールを参照してください。

BGP 自律システム番号の形式

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、RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述された、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、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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。表 1 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

形式	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 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、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。表 2 および 表 3 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るとはいえ、**show** コマンド出力と正規表現を用いた 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** コマンドをイネーブルにした後で、**clear ip bgp *** コマンドを入力し、すべての BGP セッションについて、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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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。RFC 4893 では新たに 23456 が予約済み（プライベート）自律システム番号に指定され、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なくなっています。

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 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 プロセスがイネーブルになったとき、またはルータ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、ルータはリモート 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、ルータはリモート 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。ルータがリセットされ、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 ルータとの 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、Finite State Machine（FSM; 有限状態マシン）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。

シスコシステムズが採用している 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。たとえば、**network**、**redistribute**、**bgp bestpath** などのコマンド。
- 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表 4 に示します。

表 4　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
```

Cisco IOS Release 12.0(22)S、12.2(15)T、およびそれ以降のリリースでは、**bgp upgrade-cli** コマンドにより、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）形式からアドレス ファミリ形式への BGP ネットワークおよび既存のコンフィギュレーションの移行が簡単になっています。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 Command-Line Interface（CLI; コマンドライン インターフェイス）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、「NLRI から AFI へのコンフィギュレーション：例」（P.82）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。Cisco IOS ソフトウェアは、BGP ピアリング セッションをリセットするために、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 ルータがインバウンド 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。中断を伴わないポリシー変更については、ルート リフレッシュ機能がアップデート情報をローカルに保存することはありません。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.
  ```

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 ソフト再構成を実行するように BGP を設定するための **bgp soft-reconfig-backup** コマンドが導入されました。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アトリビュートを合成し、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。集約プレフィクスは、Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）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。

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、Routing Information Database（RIB; ルーティング情報データベース）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 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。

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

Cisco IOS Release 12.0(24)S、12.2(18)S、12.3(4)T、または 12.2(27)SBC への 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。

ピア 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 ピア テンプレートのコンフィギュレーションは、ピア グループ コンフィギュレーションと競合したり、これを制約したりすることはありません。また、ピア グループは引き続き、BGP ピア テンプレートをサポートする Cisco IOS リリースでもサポートされます。ただし、ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。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。

基本 BGP ネットワークの設定方法

基本 BGP ネットワーク設定は、いくつかの必須作業と、多数の任意の作業から構成されます。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。

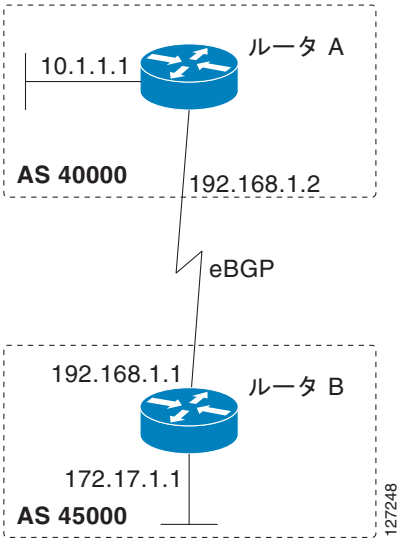
BGP ルーティング プロセスの設定

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 をイネーブルにするには、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イネーブルにされていますが、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） 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。

図 1 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 つのルータの間で 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 1　　2 つの自律システムを持つ BGP トポロジ



BGP ルータ ID

BGP はルータ ID を使用して、BGP 対応ピアを識別します。BGP ルータ ID は 32 ビット値です。この値は、IPv4 アドレスで表現されることがよくあります。デフォルトでは、Cisco IOS ソフトウェアは、ルータのループバック インターフェイスの IPv4 アドレスにこのルータ ID を設定します。ルータでループバック インターフェイスが設定されていない場合、BGP ルータ ID を表現するために、ルータの物理インターフェイスで設定されている最大の IPv4 アドレスが選択されます。BGP ルータ ID は、ネットワークの BGP ピア固有のものでなければなりません。

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：** `Router> enable`	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。
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`	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。 • *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 スピーカーへのルータを表します。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] **例：** `Router(config-router)# network 10.1.1.0 mask 255.255.255.0`	（任意）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判断します。
ステップ 5	**bgp router-id** *ip-address* **例：** `Router(config-router)# bgp router-id 10.1.1.99`	（任意）BGP を実行しているローカル ルータの ID として、32 ビットの固定ルータ ID を設定します。 • *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 セッションすべてがリセットされます。
ステップ 6	**timers bgp** *keepalive holdtime* **例：** `Router(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。
ステップ 7	**bgp fast-external-fallover** **例：** `Router(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。

	コマンドまたはアクション	目的
ステップ 8	**bgp log-neighbor-changes** **例：** `Router(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。予期しないネイバーのリセットは、ネットワークでのエラー率が高いことまたはパケット損失が高いことを示す場合があり、調査する必要があります。
ステップ 9	**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 10	**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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を図 1 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、設定は図 1（P.12）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。

前提条件

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。

制約事項

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されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

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. **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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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。

	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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、それ以降の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドと関連付けられる Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスの名前を表します。
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、この作業に適用される構文だけが使用されます。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 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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業を図 1（P.12）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、この作業を図 1（P.12）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」（P.25）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」（P.29）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

BGP ピアが 4 バイト自律システム番号に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、設定は図 2（P.19）のルータ B で行われています。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、図 2（P.19）にあるルータ B の自律システム番号は 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。

シスコシステムズが採用している 4 バイト自律システム番号

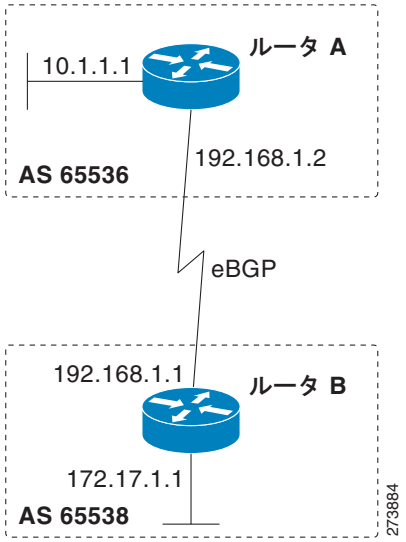
Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、およびそれ以降のリリースでは、シスコシステムズが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**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」（P.3）を参照してください。

Cisco IOS Release 12.0(32)S12、および 12.4(24)T では、シスコシステムズが採用している 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。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、「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：例」（P.78）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の自律システム番号 23456 は RFC 4893 により作成されたもので、この番号を Cisco IOS CLI で自律システム番号として設定することはできません。

図 2　　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



前提条件

この作業を行うには、ルータで、Cisco IOS Release 12.0(32)SY8、12.2(33)SXI1、またはそれ以降のリリースが実行されている必要があります。

制約事項

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されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス 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、ネイバーをアクティブ化することも必要です。

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. 必要に応じて、ステップ 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、ステップ 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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 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：** `Router(config-router)# neighbor 192.168.1.2 remote-as 65536`	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。 • この例では、4 バイト自律システム番号 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、ステップ 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：** `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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、それ以降の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドと関連付けられる Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスの名前を表します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** *ip-address* **activate** **例：** `Router(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	必要に応じて、ステップ 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：** `Router(config-router)# network 172.17.1.0 mask 255.255.255.0`	（任意）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判断します。
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 モードに戻ります。
ステップ 11	**show ip bgp** [*network*] [*network-mask*] **例：** `Router# 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、この作業に適用される構文だけが使用されます。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 12	**show ip bgp summary** **例：** `Router# show ip bgp summary`	（任意）BGP 接続すべての状況を表示します。

例

次の例は、図 2（P.19）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 バイト自律システム番号 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、図 2（P.19）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 バイト自律システム番号が 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 バイト自律システム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。

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」（P.3）を参照してください。

前提条件

この例では、ルータで、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1、またはそれ以降のリリースが実行されている必要があります。

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：** `Router> enable`	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。
ステップ 2	**show ip bgp summary** **例：** `Router# show ip bgp summary`	BGP 接続すべての状況を表示します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65538`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 65538 は asplain 表記法で定義されています。
ステップ 5	**bgp asnotation dot** **例：** `Router(config-router)# bgp asnotation dot`	BGP 4 バイト自律システム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。 **（注）** 4 バイト自律システム番号は、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：** `Router(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：** `Router# 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 バイト自律システム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、この作業に適用される構文だけが使用されます。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 8	**show ip bgp summary** **例：** `Router# 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：** `Router# show ip bgp regexp ^1\.0$`	自律システム 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 バイトの自律システム 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。

	コマンドまたはアクション	目的
ステップ 10	**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 11	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65538`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。 • この例では、4 バイト自律システム番号 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：** `Router(config-router)# no bgp asnotation dot`	BGP 4 バイト自律システム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 バイト自律システム番号は、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：** `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。
ステップ 14	**clear ip bgp *** **例：** `Router# 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 バイト自律システム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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp summary** コマンドの出力は、4 バイト自律システム番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト自律システム番号 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 バイト自律システム番号 1.0 および 1.14 に注意してください。これらは自律システム番号 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 バイトの自律システム 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 バイト自律システム番号は、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 バイト自律システム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 バイト自律システム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 バイトの自律システム 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。

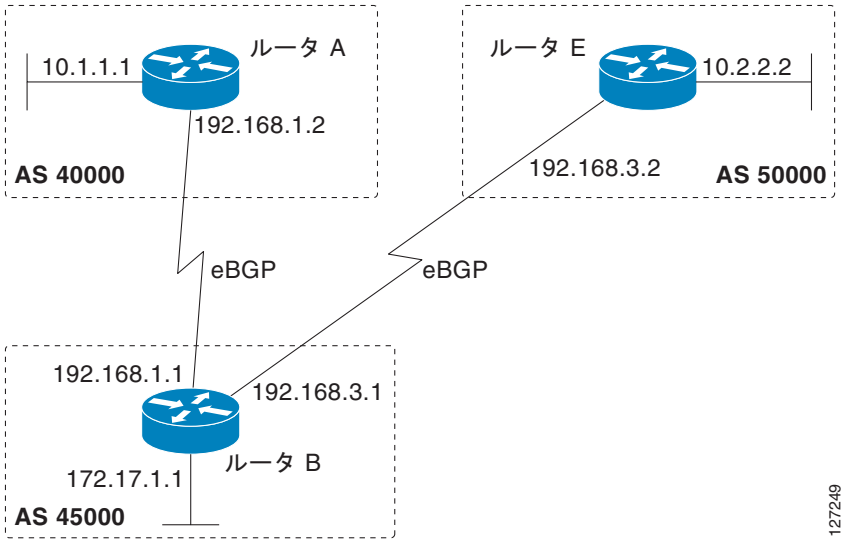
```
Router# show ip bgp regexp ^65536$


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、設定は図 3 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。

（注） 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、「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：例」（P.81）を参照してください。

図 3　IPv4 VRF アドレス ファミリ用 BGP トポロジ



前提条件

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. **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。
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 プレフィクスを作成するために、IPv4 プレフィクスに 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 拡張コミュニティへ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 アトリビュートを 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	**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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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、キーワード **unicast** 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 プレフィクスを指定するには、**multicast** キーワードを使用します。 • 後続する 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 インスタンス名を指定するには、**vrf** キーワードと *vrf-name* 引数を使用します。
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クス数を制限するものは、ルータ上で使用可能なシステム リソースだけです。 • プレフィ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`	ネイバーが IPv4 VRF アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。
ステップ 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

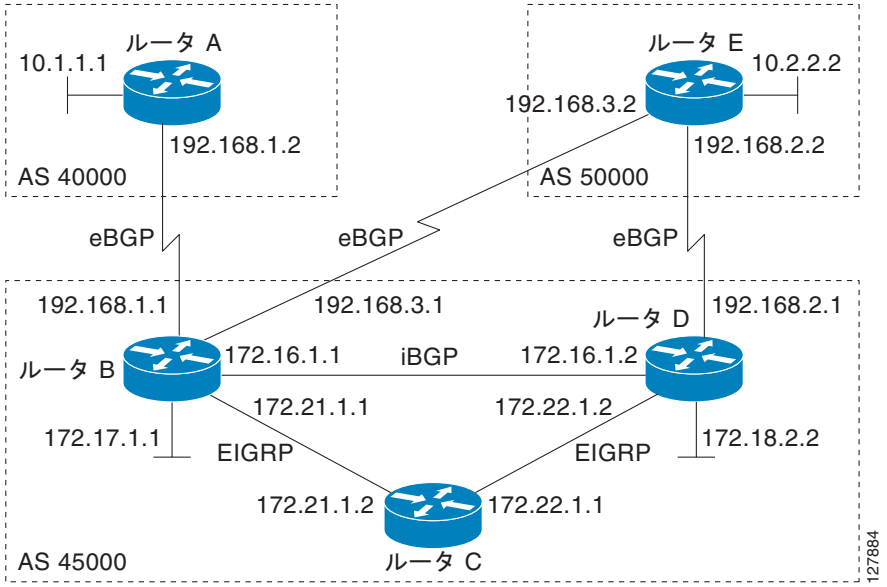
BGP ルータ間の基本的なネットワーク接続を検証するには **ping** コマンドを使用します。また、VRF インスタンスが作成されたことを確認するには **show ip vrf** コマンドを使用します。

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して、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、ネイバーをディセーブルにする方法を示しています。

図 4 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 つのルータの間で 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 4　　BGP ピア トポロジ



制約事項

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されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、アドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用し、ネイバーをアクティブ化することも必要です。

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： `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 ファミリをディセーブルにします。 （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： `Router(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 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* | *peer-group-name*} **description** *text* **例：** `Router(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：** `Router(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、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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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：** `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）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判断します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.3.2 activate`	BGP ネイバーとの情報の交換をイネーブルにします。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds* **例：** `Router(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：** `Router(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 ルータ）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：** `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 モードを終了して、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 13	**neighbor** {*ip-address* | *peer-group-name*} **shutdown** **例：** `Router(config-router)# neighbor 192.168.3.2 shutdown`	（任意）BGP ピア、またはピア グループをディセーブルにします。 **（注）** このステップを実行すると、ネイバーがディセーブルにされるため、この後の **show** コマンドを使ったステップをいずれも実行できなくなります。
ステップ 14	**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 15	**show ip bgp ipv4 multicast** [*command*] **例：** `Router# 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：** `Router# 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、この作業を図 4（P.29）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 ファミリの下に設定されている各ルータ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、図 4（P.29）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

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、またはディセーブルにしてください。この例では、**route-map** CLI を削除しても、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。単に **redistribute** CLI を削除するだけでは、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の CLI が残ります。

BGP CLI の削除の詳細については、「Cisco BGP Overview」モジュールの「BGP CLI Removal Considerations」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、「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：例」（P.84）を参照してください。

手順の概要

1. **enable**

2. **configure terminal**
3. **no route-map** *map-tag*
4. **router eigrp** *autonomous-system-number*
5. **no redistribute** *protocol* [*as-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：** `Router> enable`	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。
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	**no route-map** *map-name* **例：** `Router(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：** `Router(config)# router eigrp 100`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 5	**no redistribute** *protocol* [*as-number*] **例：** `Router(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、この作業例のステップ 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、この作業に適用される構文だけが使用されます。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 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。
ステップ 7	**show running-config** **例：** `Router# 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」（P.37）
- 「基本 BGP 情報のリセットと表示」（P.40）

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、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。表 5 は、これらの利点と欠点をまとめたものです。

表 5　ハード リセットとソフト リセットの長所と短所

リセットのタイプ	長所	短所
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 Forwarding Information Base（FIB; 転送情報ベース）テーブル内のプレフィクスが失われる。推奨されない。
アウトバウンド 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。

表 5　　ハード リセットとソフト リセットの長所と短所 （続き）

リセットのタイプ	長所	短所
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。

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 ソフトコンフィギュレーションを設定するには、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。

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. soft-reconfiguration inbound を使って設定される各ピアについて、ステップ 6 ～ 8 を繰り返します。
10. **exit**
11. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
12. **set local-preference** *number-value*
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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**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イネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**bgp soft-reconfig-backup** **例：** `Router(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：** `Router(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 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* | *peer-group-name*} **soft-reconfiguration** [**inbound**] **例：** `Router(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、Cisco IOS ソフトウェアを設定します。 • このネイバーから受信したアップデートは、インバウンド ポリシーに関係なく、すべ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。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router)# neighbor 192.168.1.2 route-map LOCAL in`	受信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	soft-reconfiguration inbound を使って設定される各ピアについて、ステップ 6 ～ 8 を繰り返します。	—
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-name* [**permit** | **deny**] [**sequence-number**] **例：** `Router(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 local-preference** *number-value* **例：** `Router(config-route-map)# set local-preference 200`	自律システム パスのプリファレンス値を指定します。 • この例では、ローカル プリファレンス値は 200 に設定されています。

	コマンドまたはアクション	目的
ステップ 13	**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 14	**show ip bgp neighbors** [*neighbor-address*] **例：** `Router(config-router-af)# 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、この作業に適用される構文だけが使用されます。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 15	**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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

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

ステップ 1 **enable**

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。

```
Router> enable
```

ステップ 2 **clear ip bgp** {***** | *autonomous-system-number* | *neighbor-address*}} [**soft** [**in** | **out**]

BGP ネイバー セッションをクリアおよびリセットするにはこのコマンドを使用します。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。

次に、BGP ネイバー セッションをすべてクリアし、リセットする例を示します。Cisco IOS Release 12.2(25)S 以降の構文では **clear ip bgp all** です。

```
Router# clear ip bgp *
```

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*]

BGP ルーティング テーブル内のエントリをすべて表示するには、このコマンドを使用します。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
```

ステップ 4 **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]

TCP および BGP 接続に関する情報をネイバーに表示するには、このコマンドを使用します。

次の例は、図 3（P.26）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
```

ステップ 5 **show ip bgp paths**

データベースにある BGP パスをすべて表示するには、このコマンドを使用します。次に、図 4（P.29）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
```

ステップ 6 **show ip bgp summary**

BGP パスすべてのステータスを表示するには、このコマンドを使用します。次に、図 4（P.29）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)
```

BGP を使用したルート プレフィクスの集約

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（*supernets*）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ルータは、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：** `Router> enable`	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。
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 route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*] **例：** `Router(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：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute static** **例：** `Router(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：** `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 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。

AS-SET 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 アトリビュートは、AS-SET には追加されません。

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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**aggregate-address** *address mask* [**as-set**] **例：** `Router(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：** `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。

BGP を使用した集約されたルートのアドバタイズ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. **aggregate-address** *address mask* [**summary-only**]
   または
   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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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	**aggregate-address** *address mask* [**summary-only**] または **aggregate-address** *address mask* [**suppress-map** *map-name*] **例：** `Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 summary-only` または `Router(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、集約ルートのうち、より具体的なものを選択的に抑制し、その他のルートを抑制せずにそのまま残すことができます。IP アクセス リスト、および自律システム パス アクセス リストの **match** 句は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。

	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*} **unsuppress-map** *map-name* **例：** `Router(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：** `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。

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。

前提条件

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。

制約事項

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。
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：** `Router(config-router-af)# bgp suppress-inactive`	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。 • 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イネーブルにするには、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、より都合のよい管理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クスは、アドバタイズ マップと存在マップまたは不在マップの 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クスを指定します。

- 存在マップが設定されている場合、プレフィクスがアドバタイズ マップと存在マップの両方に存在するときに条件が満たされます。
- 不在マップが設定されている場合、プレフィクスがアドバタイズ マップには存在するが、不在マップには存在しないときに条件が満たされます。

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. トラッキングの対象となる各プレフィクスについて、ステップ 7 と 8 を繰り返します。
10. **exit**
11. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
12. 作成される各アクセス リストについて、ステップ 11 を繰り返します。
13. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	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。
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 45000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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	**neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} **例：** `Router(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 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、**アドバタイズ マップ** map1 に関連付けられているルート マップで、**存在マップ** map2 にも同じプレフィクスが存在する場合に、指定されたネイバーにアドバタイズされるプレフィクスを指定します。 • この例では、プレフィクス 172.17.0.0（ステップ 11 より）が map1 および map2 に存在する場合に、ネイバー 192.168.1.2 にアドバタイズされます。
ステップ 6	**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 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：** `Router(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、またはプレフィクス リストにより許可されているプレフィ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クスとマッチングされます。
ステップ 9	トラッキングの対象となる各プレフィクスについて、ステップ 7 と 8 を繰り返します。	—
ステップ 10	**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 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **例：** `Router(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 プレフィクスのアドバタイズが許可されます。

	コマンドまたはアクション	目的
ステップ 12	作成される各アクセス リストについて、ステップ 11 を繰り返します。	—
ステップ 13	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了して、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」（P.11）の説明のとおり **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従って、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」（P.50）
- 「BGP ルートの条件付き挿入」（P.52）
- 「バックドア ルートを使用した BGP ルートの開始」（P.56）

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。コンフィギュレーションを簡素化する、またはルータがシステム リソースを過剰にしないように防ぐには、デフォルト ルートが便利です。ルータが Internet Service Provider（ISP; インターネット サービス プロバイダー）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 ルータ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：** `Router> enable`	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。
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 DEFAULT permit 10.1.1.0/24`	IP プレフィクス リストを設定します。 • この例では、プレフィクス リスト DEFAULT は、**match ip address** コマンドで設定されたマッチングに基づいて、10.1.1.0/24 プレフィクスのアドバタイジングを許可しています。
ステップ 4	**route-map** *map-tag* [**permit** | **deny**] [**sequence-number**] **例：** `Router(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：** `Router(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、またはプレフィクス リストにより許可されているプレフィ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、プレフィクス リスト DEFAULT で許可されているプレフィクスとマッチングされます。
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 40000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] **例：** `Router(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 ルータ）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：** `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。

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クスではなく、より具体的なプレフィクスを 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。

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。Cisco IOS ソフトウェアには、プレフィクスを BGP にする方法がいくつか用意されています。現在使用されている方法には、再配布する方法や、**network** または **aggregate-address** コマンドを使った方法などがあります。これらの方法は、ルーティング テーブル、または BGP テーブルのいずれかに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クスにより具体的なプレフィ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。元のプレフィクスと同じ、またはより具体的なプレフィクスだけが挿入されます。BGP 条件付きルート挿入をイネーブルにするには、**bgp inject-map exist-map** コマンドを使用します。また、BGP 条件付きルート挿入では、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クスが BGP ルーティング テーブルに挿入されます。exist-map は、BGP スピーカーにより追跡されるプレフィクスを表します。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クスを定義します。

前提条件

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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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アトリビュート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 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。
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 アトリビュートを設定します。
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。

	コマンドまたはアクション	目的
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`	プレフィクス リストを作成します。 • この例では、プレフィクス 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 モードを終了して、特権 EXEC モードに戻ります。
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クスが、集約プレフィ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。

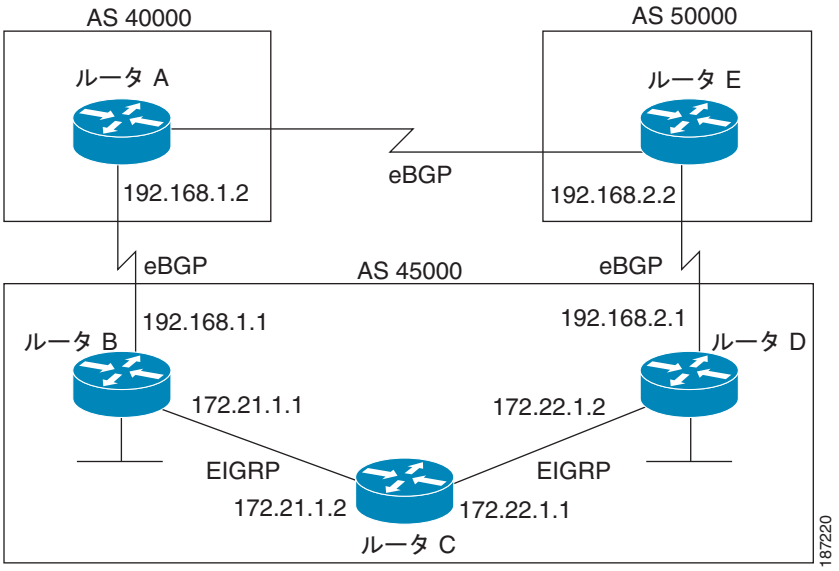
バックドア ルートを使用した BGP ルートの開始

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。

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 を使用する境界ルータを 2 つ使った BGP ネットワーク トポロジでは、2 つの境界ルータ間の通信で、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。図 5 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、図 5 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



前提条件

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。この設定は図 5 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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(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 ルータ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：** `Router(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：** `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 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。

制約事項

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されたネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなど、その他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス 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、ネイバーをアクティブ化することも必要です。

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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** **例：** `Router(config-router)# neighbor fingroup 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* **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：** `Router(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：** `Router(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：** `Router(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されたネイバーは、ユニキャスト アドレス プレフィ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 プレフィクス タイプを BGP が交換できるようにするには、ネイバーのアクティブ化にも **neighbor activate** コマンドを使用する必要があります。
ステップ 9	**neighbor** *ip-address* **peer-group** *peer-group-name* **例：** `Router(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：** `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。

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」（P.60）
- 「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」（P.63）
- 「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」（P.65）

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。Cisco IOS 12.0(25)S、12.4(11)T、12.2(33)SRB、12.2(33)SB 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。

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。

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、異なる値を使って、一般セッション コマンドを再度適用した場合、それ以降の値が優先され、間接継承されたテンプレートで設定された直前の値が上書きされます。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。

制約事項

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。
- ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。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。
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	**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リストについては、「ピア セッション テンプレート」（P.60）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	**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リストについては、「ピア セッション テンプレート」（P.60）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。

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。
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	**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リストについては、「ピア セッション テンプレート」（P.60）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リストについては、「ピア セッション テンプレート」（P.60）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	**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。
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。 • ステップ 5 のネイバー継承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、ステップ 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。
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」（P.67）を参照してください。

ピア ポリシー テンプレートの設定

次に説明する作業では、ピア ポリシー テンプレートを作成し、設定します。

- 「基本的なピア ポリシー テンプレートの設定」（P.67）
- 「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」（P.70）
- 「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」（P.73）

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。

制約事項

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。
- ピア グループおよびピア テンプレートの両方で機能するように BGP ネイバーを設定することはできません。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 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。継承されたピア ポリシー テンプレートは、ルート マップのように、シーケンス番号付きで設定されます。ルート マップ同様、継承されたピア ポリシー テンプレートは、継承文のシーケンス番号の小さい順に評価されます。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継承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。

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. **exit-peer-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：** `Router> enable`	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。
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 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：** `Router(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リストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。
ステップ 6	**weight** *weight-value* **例：** `Router(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リストについては、「ピア ポリシー テンプレート」（P.67）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：** `Router(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クスをフィルタします。 • この例のプレフィクス 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リストについては、「ピア ポリシー テンプレート」（P.67）を参照してください。
ステップ 8	**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。

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」（P.70）、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」（P.73）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。
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」（P.67）を参照してください。
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。

	コマンドまたはアクション	目的
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** キーワードをつけた場合の出力で、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。
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。 • ステップ 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、ステップ 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。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*] **例：** `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。
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の詳細については、「ピア セッション テンプレートの設定」（P.59）、および「ピア ポリシー テンプレートの設定」（P.67）を参照してください。

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 リセットを手動でイネーブルにするには、**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。

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

ステップ 1 **enable**

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。

```
Router> enable
```

ステップ 2　**clear ip bgp update-group** [*index-group* | *ip-address*]

BGP アップデート メンバシップをクリアし、BGP アップデート グループを再計算するには、このコマンドを使用します。特定のアップデート グループをクリアするには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のネイバーをクリアするには、*ip-address* 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 アップデート グループをすべてクリアし、再計算します。

次の例は、アップデート グループから、ネイバー 192.168.2.2 のメンバシップをクリアします。

```
Router# clear ip bgp update-group 192.168.2.2
```

ステップ 3　**show ip bgp replication** [*index-group* | *ip-address*]

このコマンドは、BGP アップデート グループ レプリケーションの統計情報を表示します。特定のアップデート グループ レプリケーションの統計情報を表示するには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のアップデート グループ レプリケーションの統計情報を表示するには、*ip-address* 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、すべてのアップデート グループのレプリケーション統計情報を表示します。

次の例は、すべての BGP ネイバーのアップデート グループ レプリケーション情報を表示します。

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1     192.168.1.2        0        0      0      0
         2 internal        2     192.168.3.2        0        0      0      0
```

ステップ 4　**show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

BGP アップデート グループに関する情報を表示するには、このコマンドを使用します。特定のアップデート グループの統計情報を表示するには、*index-group* 引数を使用します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。特定のアップデート グループの情報を表示するには、*ip-address* 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、すべてのアップデート グループの統計情報を表示します。概要を表示するには、**summary** キーワードを使用します。

次の例は、すべてのネイバーのアップデート グループ情報を表示します。

```
Router# show ip bgp update-group

BGP version 4 update-group 1, external, Address Family: IPv4 Unicast
  BGP Update version : 8/0, messages 0
  Update messages formatted 11, replicated 3
  Number of NLRIs in the update sent: max 1, min 0
  Minimum time between advertisement runs is 30 seconds
  Has 2 members (* indicates the members currently being sent updates):
   192.168.1.2      192.168.3.2
```

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 ネットワーク設定のコンフィギュレーション例

ここでは、次の例について説明します。

BGP プロセスの設定とピアのカスタマイズ：例

次の例は、図 4（P.29）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

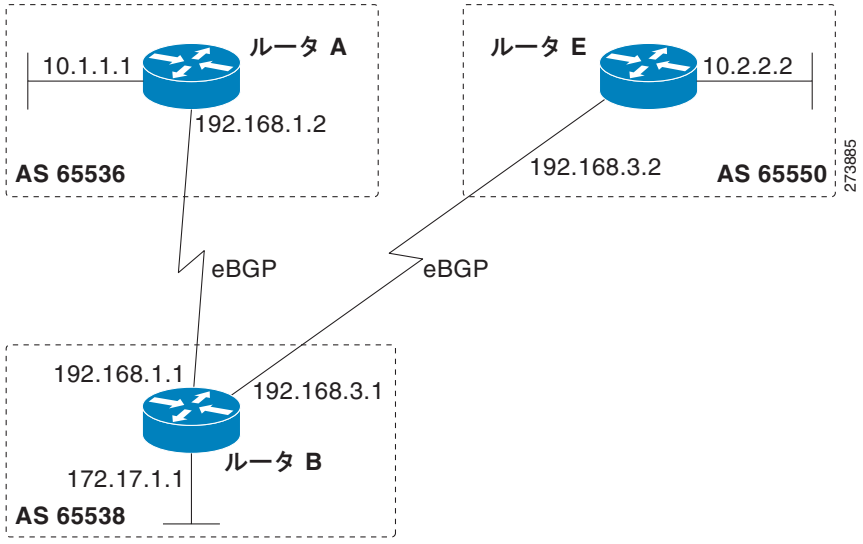
```
router bgp 45000
 bgp router-id 172.17.1.99
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 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
```

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：例

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、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な例を示します。これは、図 6 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の例で、このプロセスは、asplain 表記法を使用して設定された 4 バイトの自律システムのルータ A、B、および 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 6　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
```

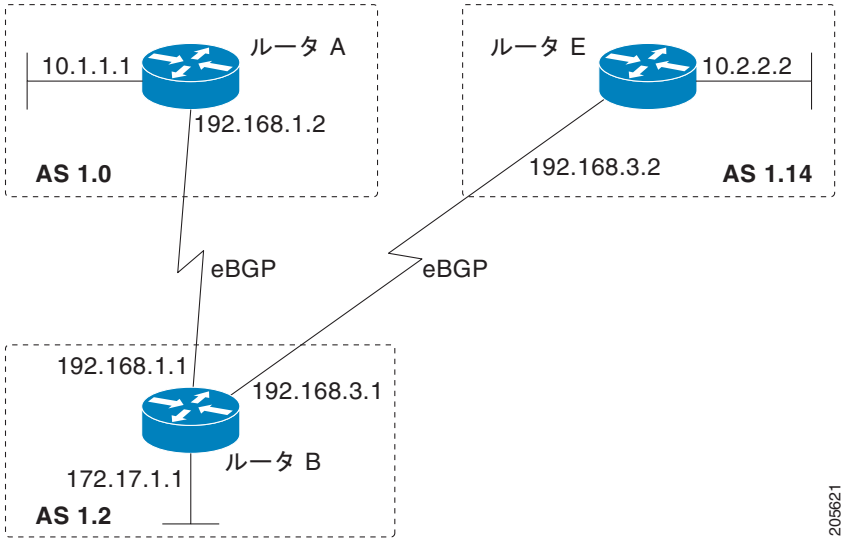
ルータ E

```
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
```

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、Cisco IOS Release 12.0(32)S12 および 12.4(24)T で使用可能な例を示します。これは、図 6 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 4 バイトの自律システムのルータ A、B、および 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 7　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
```

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：例

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
```

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
```

NLRI から AFI へのコンフィギュレーション：例

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。次のセクションでは、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。

- 次の「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」
- 「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」（P.83）

（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
```

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：例

次の例は、ルート マップを使用して、EIGRP への BGP ルートの再配布をイネーブルにする 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の両方を示しています。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 ルート再配布をイネーブルにする 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** コマンドの両方がディセーブルにされています。route-map コマンドだけを削除した場合、再配布が自動的にディセーブルにされ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** コマンドもディセーブル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
```

BGP ソフト リセット：例

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。

ダイナミック インバウンド ソフト リセットの例

次の例では、**clear ip bgp 192.168.1.1 soft in** EXEC コマンドを使用して、BGP ピア 192.168.1.1 でダイナミック ソフト再構成を開始します。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
```

格納された情報を使用したインバウンド ソフト リセットの例

次の例では、ネイバー 192.168.1.1 に対してインバウンド ソフト再構成をイネーブルにする方法を示しています。このネイバーから受信したアップデートは、インバウンド ポリシーに関係なく、すべ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
```

4 バイト自律システム番号を使用する BGP ピアのリセット：例

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。この例では、ルータで、Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、12.2(33)SXI1 またはそれ以降のリリースが実行されている必要があります。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 ピアが稼動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
```

BGP を使用したプレフィクスの集約：例

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 アトリビュート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
```

グローバル コンフィギュレーション モードで始まる次の例は、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。

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

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

BGP ピア グループの設定：例

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
```

ピア セッション テンプレートの設定：例

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。ネイバー継承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
```

ピア ポリシー テンプレートの設定：例

次の例は、ポリシー テンプレート コンフィギュレーション モードで、GLOBAL という名前のピア ポリシー テンプレートを作成します。

```
router bgp 45000
 template peer-policy GLOBAL
 weight 1000
 maximum-prefix 5000
 prefix-list NO_SALES in
 exit-peer-policy
```

次の例は、ポリシー テンプレート コンフィギュレーション モードで、PRIMARY-IN という名前のピア ポリシー テンプレートを作成します。

```
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。

```
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 テンプレート名 CUSTOMER-A を継承するように、192.168.2.2 ネイバーを設定します。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
```

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とメンテナンス：例

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。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からは、**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 プロバイダーへの接続については、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。
- BGP ネイバー セッション オプションの設定については、「Configuring BGP Neighbor Session Options」モジュールを参照してください。
- iBGP 機能の設定については、「Configuring Internal BGP Features」モジュールを参照してください。

参考資料

ここでは、基本的な BGP 作業の設定に関連する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands 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*』
IPv6 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 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	「Cisco BGP Overview」モジュール
IPv4 VRF アドレス ファミリを使った Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）および BGP コンフィギュレーションの例	「Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels」モジュール
基本的な MPLS VPN および BGP コンフィギュレーションの例	「*Configuring MPLS Layer 3 VPNs*」モジュール

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 6 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 6 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 6　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 バージョン 4	Cisco IOS XE 3.1.0SG	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 Cisco IOS ソフトウェア実装には、BGP が 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できるようにするマルチプロトコル拡張機能と、IP Version 4（IPv4; IP バージョン 4）、IP Version 6（IPv6; IP バージョン 6）、Virtual Private Networks Version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、および Connectionless Network Services（CLNS; コネクションレス型ネットワーク サービス）を含む複数のレイヤ 3 プロトコル アドレス ファミリが組み込まれています。 この機能については、次の項に説明があります。 • 「BGP バージョン 4」（P.2）
BGP 条件付きルートの挿入	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クスよりも、より具体的なプレフィクスを 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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ルート集約」（P.8） • 「BGP ルートの条件付き挿入」（P.52）

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
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	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。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア テンプレート」（P.10） • 「ピア セッション テンプレートの設定」（P.59） • 「ピア ポリシー テンプレートの設定」（P.67）
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。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア グループおよび BGP アップデート メッセージ」（P.9） • 「BGP アップデート グループ」（P.10） • 「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」（P.75）

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
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。 次のセクションで、この機能に関する情報を参照できます。 • 「シスコシステムズが採用している 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」（P.6） • 「NLRI から AFI へのコンフィギュレーション：例」（P.82）
BGP ネイバー ポリシー	12.2(33)SB 12.2(33)SRB 12.4(11)T Cisco IOS XE 3.1.0SG	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。 次のセクションで、この機能に関する情報を参照できます。 • 「ピア ポリシー テンプレートの設定」（P.67） • 「ピア ポリシー テンプレートの設定：例」（P.88） この機能では、**show ip bgp neighbors**、および **show ip bgp template peer-policy** 機能が変更されました。

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
4 バイト ASN に対する BGP サポート	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 15.0(1)S Cisco IOS XE 3.1.0SG	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、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、シスコシステムズが採用している 4 バイト自律システム番号は、自律システム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 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** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 自律システム番号の形式」（P.3） • 「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」（P.18） • 「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」（P.22） • 「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：例」（P.78） • 「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：例」（P.81） • 「4 バイト自律システム番号を使用する BGP ピアのリセット：例」（P.85） この機能により、次の各コマンドが追加または変更されています。**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**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 6　基本 BGP ネットワーク設定の機能情報 （続き）

機能名	リリース	機能の設定情報
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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ルート集約」（P.8） • 「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」（P.46） • 「BGP を使用したプレフィクスの集約：例」（P.86）

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、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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、External BGP（eBGP; 外部 BGP）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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「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」（P.81）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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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。詳しくは、「Cisco BGP Overview」および「Configuring a Basic BGP Network」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、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）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。

サービス プロバイダーとの外部 BGP を使用した接続の制約事項

- 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 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

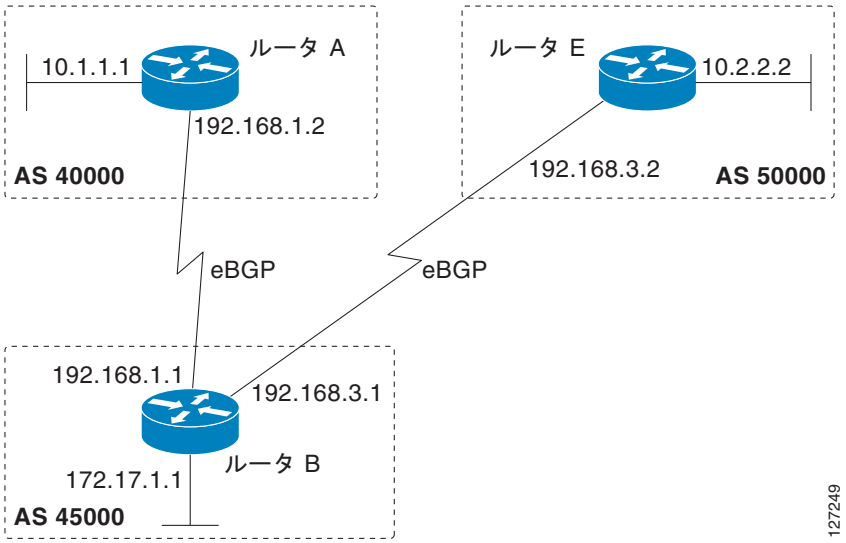
外部 BGP を使用して ISP への接続作業を行うには、次の概念を理解しておく必要があります。

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。図 1 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、図 1 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** コマンドが使用できます。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 アトリビュート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 1　　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、先に **neighbor disable-connected-check** コマンドを設定しなければ、eBGP ピアリング セッションは確立できません。

外部ネットワークとの接続により、使用するネットワークからのトラフィックを別のネットワークへ、インターネットを通じて転送することができるようになります。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 アトリビュートを使用します。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 アトリビュート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 アトリビュートによるタギングを 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

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、RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述された、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。表 1 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

形式	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 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、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。表 2 および 表 3 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るとはいえ、**show** コマンド出力と正規表現を用いた 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** コマンドをイネーブルにした後で、**clear ip bgp *** コマンドを入力し、すべての BGP セッションについて、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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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

形式	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 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 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。RFC 4893 では新たに 23456 が予約済み（プライベート）自律システム番号に指定され、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なくなっています。

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 アトリビュート

デフォルトでは、BGP は宛先ホストまたはネットワークへの最良パスとして 1 つのパスを選択します。どのルートを最良パスとして 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、最良パス選択アルゴリズムはパスのアトリビュートを分析します。それぞれのパスには、BGP 最良パス分析で使用されるさまざまなアトリビュートがついています。Cisco IOS ソフトウェアは、Command-Line Interface（CLI; コマンドライン インターフェイス）を通してそのようなアトリビュートを変更することで、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、最良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、許可される最大数よりも多くの全体的に良好なマルチパスが存在する場合、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 アトリビュート情報を含めることができます。BGP アトリビュートはルートの特徴を記述するもので、ソフトウェアはアトリビュートをどのルートをアドバタイズするか決定を下すのを助けるのに使用します。一部のアトリビュート情報は、BGP 対応のネットワーキング デバイスでも設定できます。アトリビュートには、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 アトリビュートが設定可能です。

- AS-path
- Community
- Local_Pref
- Multi_Exit_Discriminator（MED）
- Next_Hop
- Origin

AS-path

このアトリビュートは、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 アトリビュートを使えば、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 アトリビュートは 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 アトリビュートは、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 アトリビュートは、（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 アトリビュートだけを比較します。**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 Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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。Cisco IOS ソフトウェアが稼動する BGP ルータでは、MED アトリビュートのないルートを値 0 を持つ MED として扱い、MED 変数の欠落したルートが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 アトリビュートは、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 アトリビュートは変更されません。

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

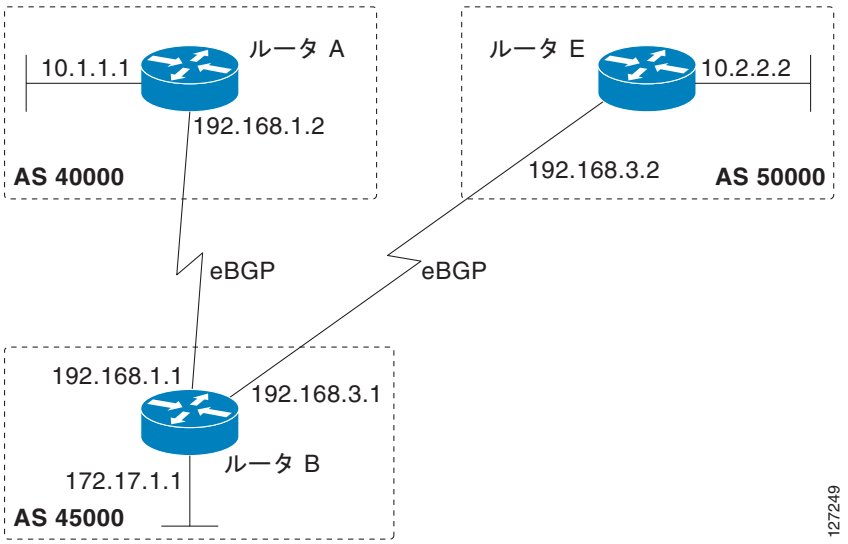
このアトリビュートは、ルートがどのように BGP ルーティング テーブルに含まれたかを示します。Cisco IOS ソフトウェアにおいて、BGP **network** コマンドを使用して定義されたルートには、Interior Gateway Protocol（IGP）の送信コードが与えられています。Exterior Gateway Protocol（EGP）から配信されたルートは、EGP の送信元を使用してコーディングされ、その他のプロトコルから再配布されたルートは「不完全」と定義されます。BGP の送信元決定ポリシーでは、「不完全」よりも EGP が、EGP よりも IGP が優先されます。

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もっと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。図 2 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 2　　マルチホーミング トポロジ



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。プレフィクス処理は、BGP タイマーの調整、BGP によるパス アトリビュートの扱いの変更、ルーティング プロセスが受け入れるプレフィクスの数の制限、および BGP プレフィクス 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。表 4 に、BGP ポリシー フィルタの処理順序を示します。

表 4　　BGP ポリシー処理順序

インバウンド	アウトバウンド
ルート マップ	配信リスト
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 プレフィクス リスト
IP プレフィクス 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
配信リスト	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 リセットでは、指定されたピアリング セッションは TCP 接続を含めて破棄され、指定されたピアからのルートが削除されます。
- 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 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 ルータがインバウンド 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 コミュニティ

BGP コミュニティは、ネットワーク、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ルートをグループ化する（カラー ルートとも呼ばれる）のに使用されます。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 アトリビュートを使えば、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。

標準コミュニティ リストは、よく知られたコミュニティと特定のコミュニティ番号を設定するために使用されます。拡張コミュニティ リストは、正規表現を使用してコミュニティをフィルタリングするために使用されます。正規表現は、コミュニティ アトリビュートのマッチング パターン設定に使用されます。

コミュニティ アトリビュートはオプションです。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、アトリビュートは無視されます。

4 つの定義済みコミュニティがあります。

- no-export：外部 BGP ピアへアドバタイズしない。
- 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にアドバタイズする。BGP 対応のネットワーキング デバイスはすべてその所属となります。
- local-as：ローカルの自律システムの外には送らない。

Cisco IOS Release 12.2(8)T では、BGP 名前付きコミュニティ リストが導入されました。BGP 名前付きコミュニティ リストによって、わかりやすい名前をコミュニティ リストに割り当てられるようになりました。設定可能なコミュニティ リスト数の制限はありません。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、設定可能なコミュニティ リスト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。

（注） 標準および拡張コミュニティ リストには、いずれも各タイプのリスト内で設定可能なコミュニティ グループ数に 100 という上限がありました。名前付きコミュニティ リストでは、この制限がありません。

拡張コミュニティ

拡張コミュニティ アトリビュートは、Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスおよび Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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。Route Target（RT; ルート ターゲット）および Site of Origin（SoO）拡張コミュニティ アトリビュートは、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 アトリビュート

RT 拡張コミュニティ アトリビュートは、**ip extcommunity-list** コマンドの **rt** キーワードで設定されます。このアトリビュートは、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 アトリビュートにより、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 アトリビュート

SoO 拡張コミュニティ アトリビュートは、**ip extcommunity-list** コマンドの **soo** キーワードで設定されます。このアトリビュートは、Provider Edge（PE; プロバイダー エッジ）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 アトリビュート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、このアトリビュート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 アトリビュート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 アトリビュートは、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 アトリビュート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。

管理ディスタンス

管理ディスタンスは、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 タイプの管理ディスタンスを、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 も管理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、処理される。
- 1 つのルート マップに 2 つ以上のポリシー リストを設定できる。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 マップ内にあるがポリシー リストの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。
- 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、ポリシー リストすべては受信アトリビュートだけでマッチング。

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

ここでは、次の作業について説明します。

- 「インバウンド パス選択の変更」（P.13）
- 「アウトバウンド パス選択への影響」（P.20）
- 「ISP との BGP ピアリングの設定」（P.27）
- 「BGP ポリシーの設定」（P.41）

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。明らかに最適な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 アトリビュート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
- 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 アトリビュートの変更によるインバウンド パス選択の変化」（P.13）
- 「MED アトリビュートの設定によるインバウンド パス選択の変化」（P.17）

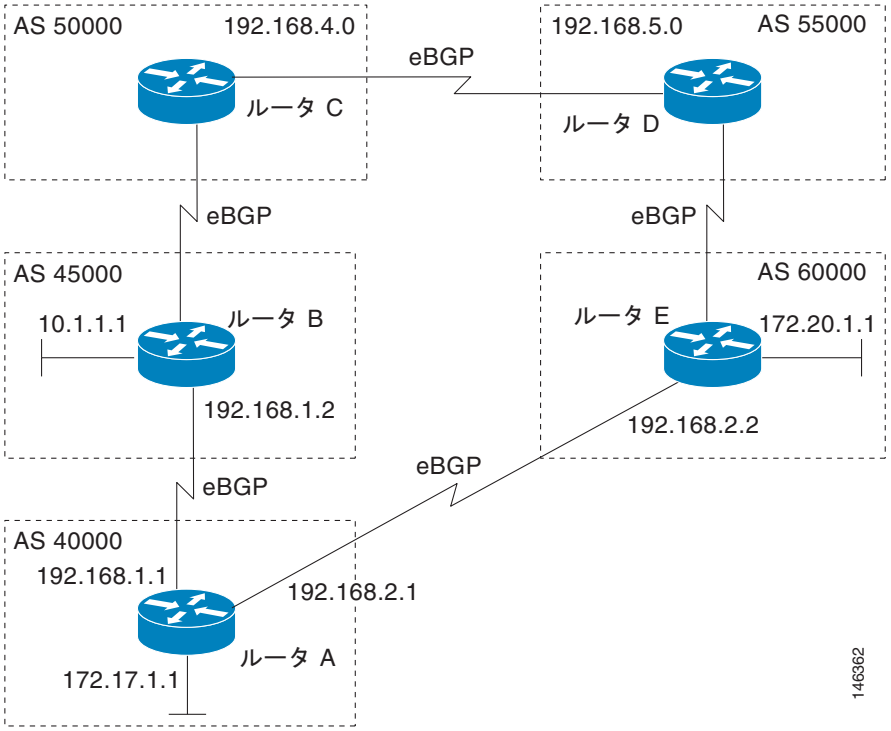
AS-path アトリビュートの変更によるインバウンド パス選択の変化

AS-path アトリビュートを変更して 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、図 3 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、「4 バイト自律システム番号を使用した AS-path アトリビュートの変更によるインバウンド パス選択の変更：例」（P.68）を参照してください。

AS-path アトリビュートの変更は、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、図 3 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 アトリビュート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。図 3 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 アトリビュート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 3　AS-path アトリビュート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*} **route-map** *map-name* {**in** | **out**}
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 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：** `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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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 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判断します。
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 PREPEND out`	受信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。

	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*} **activate** **例：** `Router(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イネーブルにします。
ステップ 9	**exit-address-family** **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	**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-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(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 マップが作成され、後続の条件一致があれば
ステップ 12	**set as-path** {**tag** | **prepend** *as-path-string*} **例：** `Router(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 ストリングを BGP ルートに「プリペンド」するには、**prepend** キーワードを使用します。通常、ローカルの自律システム番号は複数回プリペンドされ、自律システム パスの長さは増加します。 • 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。
ステップ 13	**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、特権 EXEC モードに戻ります。
ステップ 14	**show running-config** **例：** `Router# show running-config`	実行中のコンフィギュレーション ファイルを表示します。

例

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。

ルータ A

```
Router# 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
```

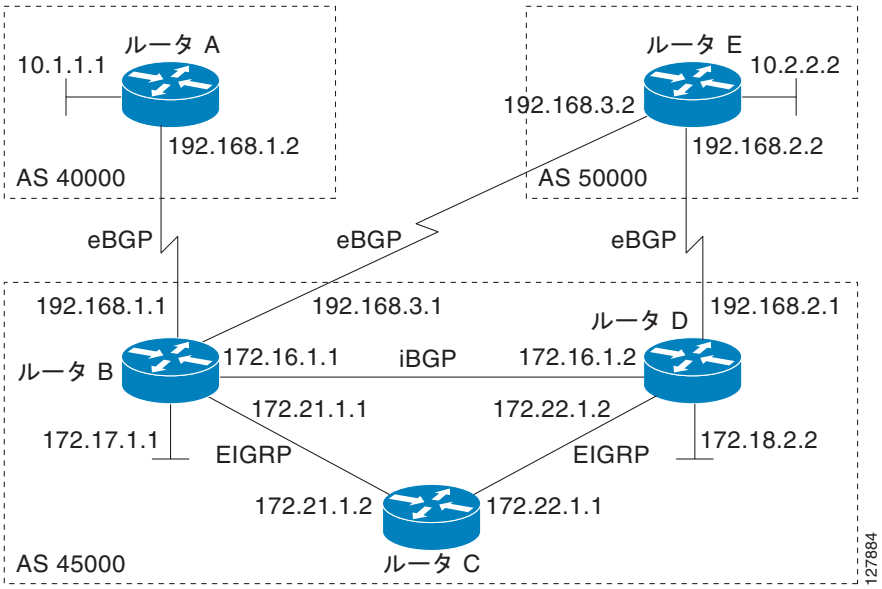
```
 no auto-summary
 no synchronization
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
!
route-map PREPEND permit 10
 set as-path prepend 40000 40000
.
.
.
```

MED アトリビュートの設定によるインバウンド パス選択の変化

MED アトリビュートの設定は、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 アトリビュートは、（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、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 アトリビュート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。図 4 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アトリビュートを比較します（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 4　　MED アトリビュート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 アトリビュートを比較するには、**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. ステップ 1 から ステップ 12 をルータ D で繰り返します。
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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**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。

	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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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 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判断します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router-af)# neighbor 192.168.3.2 route-map MED out`	受信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：** `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	**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-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(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：** `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 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。

	コマンドまたはアクション	目的
ステップ 13	ステップ 1 から ステップ 12 をルータ D で繰り返します。	—
ステップ 14	**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。 • 図 4 で、ルータ B とルータ D の両方が MED アトリビュート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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力は、この作業が図 4 のルータ B とルータ D の両方で実行された後の、ルータ E からのものです。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。

```
Router# 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 アトリビュートの使用
- 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。

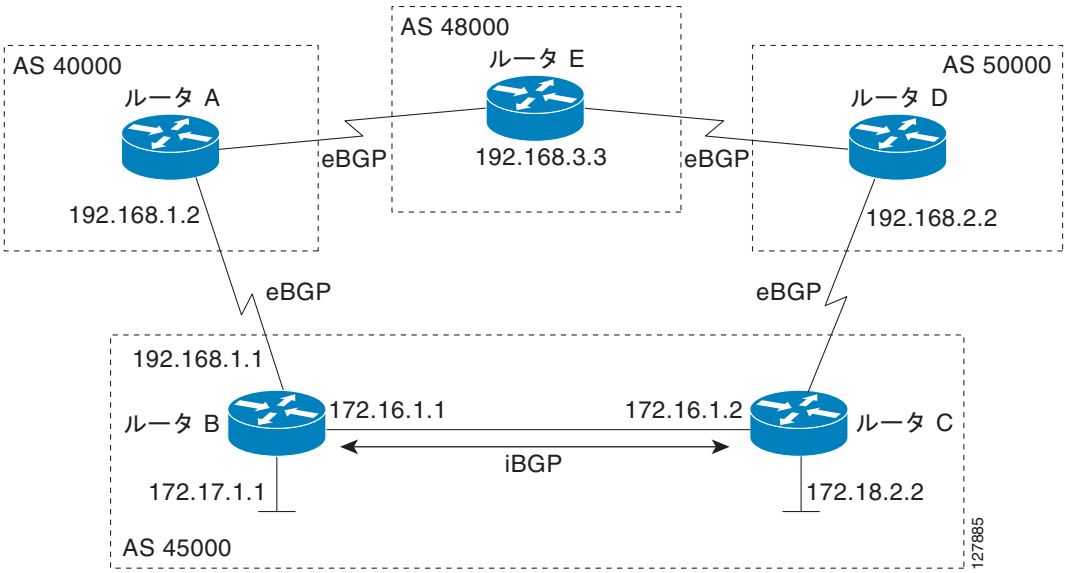
- 「Local_Pref アトリビュートを使用したアウトバウンド パス選択の変更」（P.21）
- 「アウトバウンド BGP ルート プレフィクスのフィルタリング」（P.23）

Local_Pref アトリビュート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 アトリビュートの使用です。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 アトリビュート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 アトリビュート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、図 5 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 5　　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. ステップ 1 から ステップ 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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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*] [**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判断します。
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	ステップ 1 から ステップ 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。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

アウトバウンド BGP ルート プレフィクスのフィルタリング

BGP プレフィクスベース 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。

BGP プレフィクスベース アウトバウンド ルート フィルタリング

BGP プレフィクスベース アウトバウンド ルート フィルタリングは、BGP ORF 送受信機能を使用して、BGP ピアの間で送られる BGP アップデートの数を最小化します。BGP ORF を設定すると、不要なルーティング アップデートをソースでフィルタリングできるため、ルーティング アップデートの生成や処理に必要なシステム リソースの量を減らす助けになります。たとえば、BGP ORF を使用して、サービス プロバイダー ネットワークからのルート全体を受け付けるのではないルータで、ルータに要求される処理の量を減らすことができます。

BGP プレフィクスベース アウトバウンド ルート フィルタリングはピア ルータへの ORF 機能のアドバタイズメントを通してイネーブルになります。ORF 機能のアドバタイズメントは、ある BGP ピアがネイバーからのプレフィクス リストを受け付け、そのプレフィクス リストをローカルで設定された ORF

に適用する（存在する場合）ことを示します。この機能がイネーブルの場合、BGP スピーカーはインバウンド プレフィクス リスト フィルタをアウトバウンド フィルタとしてリモート ピアにインストールでき、これにより不要なルーティング アップデートを減少させることができます。

BGP プレフィクスベース アウトバウンド ルート フィルタリングは、ORF 送受信機能を使用して設定できます。ローカル ピアは ORF 機能を send モードでアドバタイズします。リモート ピアは ORF 機能を受信モードで受信し、そのフィルタをアウトバウンド ポリシーとして適用します。ローカルとリモートのピアは、それぞれのルータの ORF を維持するために、アップデートを交換します。アップデートは、アドバタイズされた ORF プレフィクス リスト機能に依存するアドレス ファミリによってピア ルータの間で交換されます。リモート ピアは、**clear ip bgp in prefix-filter** コマンドで要求されたルート リフレッシュの後か、immediate ステータスの ORF プレフィクス リストが処理された後に、ローカル ピアにアップデートを送信し始めます。BGP ピアは、ローカル ピアがインバウンド プレフィクス リストをリモート ピアにプッシュした後、インバウンド プレフィクス リストを受信したアップデートに適用し続けます。

前提条件

プレフィクスベース ORF BGP の配信を受信できるようになる前に、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イネーブルになっている必要があります。

制約事項

- BGP プレフィクスベース 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。
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、プレフィクス長のマッチング、ワイルドカードベースのプレフィクス 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。 • 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。

	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：** `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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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 機能をイネーブルにし、*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イネーブルにします。 • **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。

	コマンドまたはアクション	目的
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」（P.27）
- 「単一 ISP とのマルチホーミング」（P.31）
- 「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」（P.37）

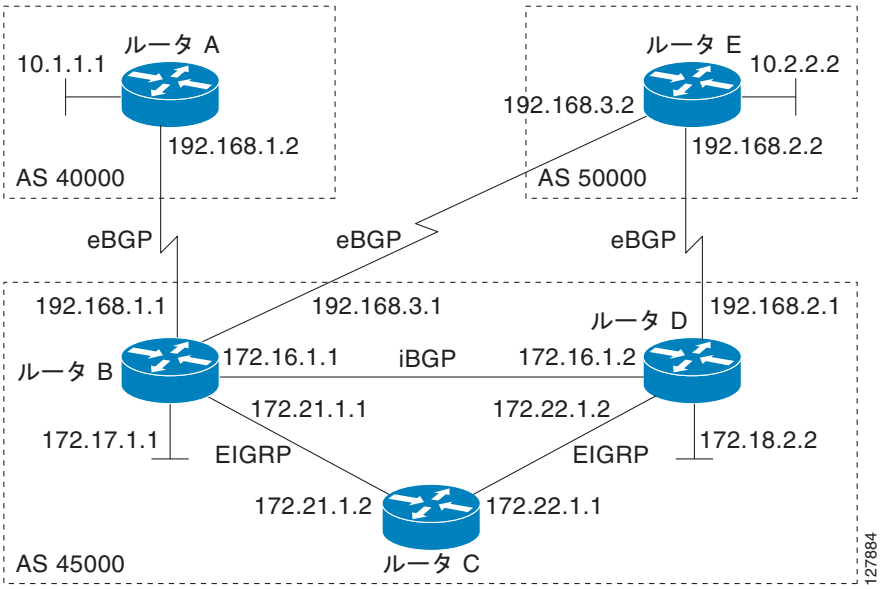
2 つの ISP とのマルチホーミングの設定

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。図 6 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 6　　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-address*] [*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。
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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判断します。
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 アトリビュートが 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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 **vrf** キーワードと *vrf-name* 引数は、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*} **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 アトリビュートが 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 アトリビュートを見るには、このコマンドをルータ B に入力します。weight アトリビュートが最大のルートが、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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の例は、ルートに weight アトリビュートが割り当てられた、ルータ B の BGP ルーティング テーブルを示しています。192.168.3.2 を通るルート（図 6 のルータ E）は最大の weight アトリビュートを持っているため、ネットワーク 172.17.1.0 への優先ルートとなります。

```
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           100 40000 i
*> 10.2.2.0/24      192.168.3.2              0           150 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。図 6 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、図 6 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。

MED アトリビュート

MED アトリビュートの設定は、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 アトリビュートは、（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、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。

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. 別のルート マップを設定するには、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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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判断します。
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`	受信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。	—
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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 **vrf** キーワードと *vrf-name* 引数は、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` および **例：** `Router(config-router-af)# neighbor 192.168.3.1 route-map SETMETRIC2 out`	受信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。
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 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` および **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、管理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、管理ディスタンスとして 40 が設定されます。管理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。
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。

	コマンドまたはアクション	目的
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。 • 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 図 6 のルータ E で使用します。 • この例では、この作業に適用される構文だけが使用されます。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 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。 • 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 図 6 のルータ E で使用します。 • この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

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、図 6 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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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判断します。
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`	受信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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 **vrf** キーワードと *vrf-name* 引数は、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`	受信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 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 リストのマッチングを行います。 • 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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に、この作業設定が完了した後の、図 6 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

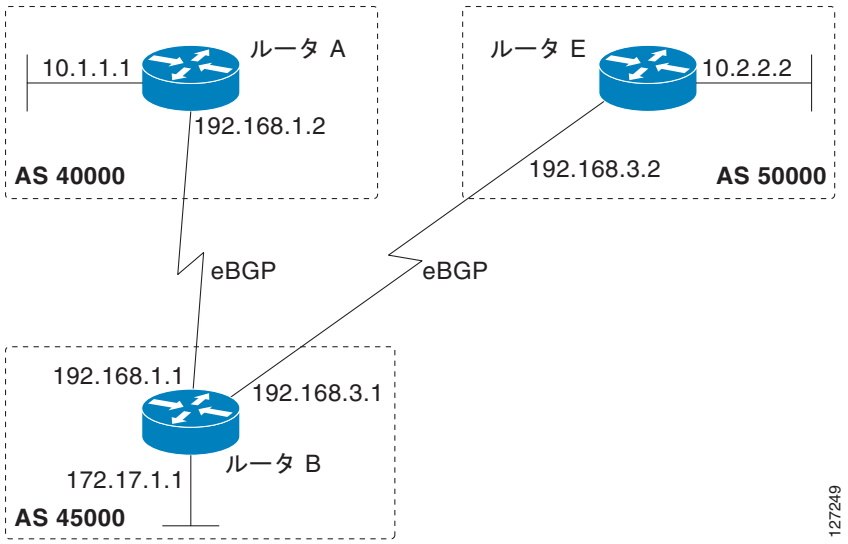
このセクションの作業は、BGP ネットワーク内でトラフィックをフィルタリングする BGP ポリシーの設定に役立ちます。次に示すオプション作業は、BGP ネットワークでトラフィックをフィルタリングするさまざまな方法の一部を示すものです。

- 「プレフィクス リストによる BGP プレフィクスのフィルタリング」（P.41）
- 「AS-path フィルタを使用した BGP プレフィクスのフィルタリング」（P.45）
- 「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 プレフィクスのフィルタリング」（P.48）
- 「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」（P.52）
- 「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」（P.55）
- 「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」（P.59）
- 「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」（P.62）

プレフィクス リストによる BGP プレフィクスのフィルタリング

プレフィクス 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、図 7 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。実際には、ルータ A への転送のためルータ E から受信した情報がこれにより制限されます。プレフィクス リスト情報を表示し、ヒット カウントをリセットするためのオプション ステップが含まれます。

図 7　　BGP ポリシー設定作業の BGP トポロジ



制約事項

neighbor prefix-list コマンドおよび **neighbor distribute-list** コマンドは、BGP ピアに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. **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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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`	指定された自律システム内のネイバーの 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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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）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判断します。

	コマンドまたはアクション	目的
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	**ip prefix-list** *list-name* [**seq** *seq-number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] [**eq** *eq-value*] **例：** `Router(config)# ip prefix-list super172 permit 172.0.0.0/8`	BGP 関連のプレフィクス 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。 • 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クス リストが定義されます。 • すべてのプレフィクス 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 プレフィクスのフィルタリング

フィルタ ルート情報への AS-path アトリビュート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 プレフィクスをフィルタリングするには、次の作業を実行します。図 7 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。フィルタリングがイネーブルにされた後、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何かあった場合、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ことから、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。

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 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. **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、ステップ 9 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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 5	すべての BGP ピアについて 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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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）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判断します。 **（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 100 out`	プレフィクス 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 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：** `Router(config)# ip as-path access-list 100 deny ^50000$` および **例：** `Router(config)# ip as-path access-list 100 permit .*`	BGP 関連のアクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 • 1 番目の例では、アクセス リスト番号 100 は 50000 で始まり 50000 で終わる AS-path はすべて拒否するように定義されています。 • 2 番目の例では、AS-path アクセス リストの 1 番目の例での基準に一致しないルートは、すべて許可されます。ピリオドとアスタリスク記号は AS-path 内のすべての文字が一致することを示しているため、ルータ B はそれらのアップデートをルータ A に転送することになります。 **（注）** 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。
ステップ 12	AS-path アクセス リストで要求されているすべてのエントリについて、ステップ 11 を繰り返します。	—
ステップ 13	**end** **例：** `Router(config-access-list)# end`	アクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp regexp** *as-regular-expression* **例：** `Router# show ip bgp regexp ^50000$`	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。

```
Router# 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
```

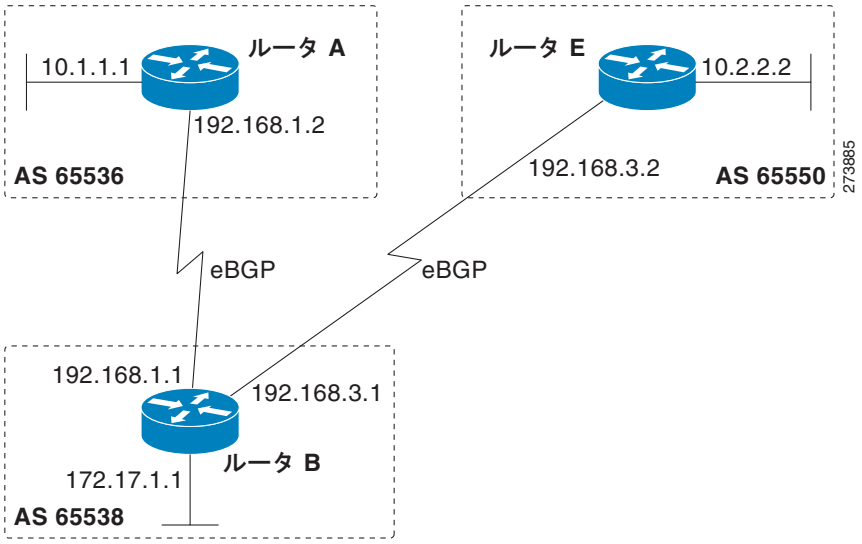
4 バイト自律システム番号を使用した AS-path フィルタによる BGP プレフィクスのフィルタリング

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。この作業の 4 バイト自律システム番号は、デフォルトの asplain（10 進数）形式です。たとえば、図 8（P.49）において、ルータ B は自律システム番号 65538 にあります。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」（P.4）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 アトリビュート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 プレフィクスをフィルタリングするには、次の作業を実行します。図 8 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。フィルタリングがイネーブルにされた後、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何かあった場合、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ことから、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 8　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 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. **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、ステップ 10 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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 ピアについて 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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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）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判断します。 **（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。

	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*} **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：** `Router(config)# ip as-path access-list 99 deny ^65550$` および **例：** `Router(config)# ip as-path access-list 99 permit .*`	BGP 関連のアクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 • 1 番目の例では、アクセス リスト番号 99 は 65550 で始まり 65550 で終わる AS-path はすべて拒否するように定義されています。 • 2 番目の例では、AS-path アクセス リストの 1 番目の例での基準に一致しないルートは、すべて許可されます。ピリオドとアスタリスク記号は AS-path 内のすべての文字が一致することを示しているため、ルータ B はそれらアップデートをルータ A に転送することになります。 **（注）** 作業例ではこれらの文の双方を設定する必要があるため、2 つの例を示しています。
ステップ 12	AS-path アクセス リストで要求されているすべてのエントリについて、ステップ 11 を繰り返します。	—
ステップ 13	**end** **例：** `Router(config-access-list)# end`	アクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 14	**show ip bgp regexp** *as-regular-expression* **例：** `Router# show ip bgp regexp ^65550$`	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、受信ルートの制御のためにルート マップ内で参照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。BGP コミュニティは、複雑で規模の大きなネットワークでインバウンドとアウトバウンドのルートをフィルタリングする手段を提供します。個別のピアについて長大なアクセス リストやプレフィクス リストを編集する代わりに、BGP では同一のルーティングポリシーを持つピアを、たとえそれらが異なる自律システムやネットワークに分散していたとしても、グループ化することができます。

この作業では、受信ルートを制御するために、図 7 のルータ B を、いくつかのルート マップとコミュニティ リストを使用して設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *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 15 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. **end**
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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**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 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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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：** `Router(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：** `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 8	**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 9	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(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：** `Router(config-route-map)# match community 1`	BGP コミュニティ リストのマッチングを行います。 • この例では、コミュニティ アトリビュートがコミュニティ リスト 1 と一致しています。
ステップ 11	**set weight** *weight* **例：** `Router(config-route-map)# set weight 30`	ルーティング テーブルの BGP weight を指定します。 • 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が、30 に設定された BGP weight を持つことになります。
ステップ 12	**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 13	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(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：** `Router(config-route-map)# match community 2`	BGP コミュニティ リストのマッチングを行います。 • この例では、コミュニティ アトリビュートがコミュニティ リスト 2 と一致しています。
ステップ 15	**set community** *community-number* **例：** `Router(config-route-map)# set community 99`	BGP コミュニティ アトリビュートを設定します。 • 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 BGP コミュニティ アトリビュートを持つことになります。
ステップ 16	**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。

	コマンドまたはアクション	目的
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：** `Router(config)# ip community-list 1 permit 100` および **例：** `Router(config)# ip community-list 2 permit internet`	BGP のコミュニティ リストを作成して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 はコミュニティ アトリビュートが 100 のルートを許可しています。ルータ C のルートはすべてコミュニティ アトリビュートが 100 であるため、weight 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** キーワードを使用することで、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、route アトリビュート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。
ステップ 18	ステップ 15 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：** `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：** `Router# 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 アトリビュートが 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。

```
Router# 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、**internet** キーワードの使用により効果的にすべてのルートがコミュニティ リスト 2 で許可されたことを示しています。

```
Router# 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。BGP コミュニティは、複雑で規模の大きなネットワークでインバウンドとアウトバウンドのルートをフィルタリングする手段を提供します。個別のピア

について長大なアクセス リストやプレフィクス リストを編集する代わりに、BGP では同一のルーティングポリシーを持つピアを、たとえそれらが異なる自律システムやネットワークに分散していたとしても、グループ化することができます。

この作業において 図 7 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。

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。

制約事項

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、ステップ 10 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-number* | *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：** `Router> enable`	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。
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 extcommunity-list** {*expanded-list-number* | **expanded** *list-name* | *standard-list-number* | **standard** *list-name*} **例：** `Router(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：** `Router(config-extcomm-list)# 10 deny _50000_` および **例：** `Router(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、この作業に適用される構文だけが使用されます。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 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：** `Router(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、この作業に適用される構文だけが使用されます。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 7	**exit** **例：** `Router(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：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 10	必要な BGP ピアすべてについて、ステップ 10 を繰り返します。	—
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 プレフィクスを指定します。 **（注）** **vrf** キーワードと *vrf-name* 引数は、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：** `Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0`	（任意）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判断します。 **（注）** この例では、この作業に適用される構文だけが使用されます。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 13	**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 14	**show ip extcommunity-list** [*list-name*] **例：** `Router# 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。

```
Router# 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。

前提条件

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。

制約事項

- 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 IP バージョン 6（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 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。
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。

	コマンドまたはアクション	目的
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：** `Router(config-route-map)# match policy-list POLICY-LIST-NAME-1`	指定したポリシー リストに一致する句を作成します。 • 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

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。Cisco IOS Release 12.3(2)T、12.0(24)S、12.2(33)SRB、およびそれ以降のリリースでは、BGP ルート マップ設定に continue 句が導入されています。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した。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。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。

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では、アウトバウンド ルート マップで continue 句がサポートされるようになりました。

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（またはジャンプする）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。

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。例として、「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：例」（P.77）を参照してください。

制約事項

- 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。
- 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. **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* [**additive**] [*well-known-community*] | **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：** `Router> enable`	特権 EXEC モードなどの上位の特権レベル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。
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 プロセスを作成します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(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。

	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 プレフィクスを指定します。 **vrf** キーワードと *vrf-name* 引数は、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：** `Router(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：** `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 8	**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-name* {**permit** | **deny**} [*sequence-number*] **例：** `Router(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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 11	**set community** *community-number* [**additive**] [*well-known-community*] | **none**} **例：** `Router(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 12	**continue** [*sequence-number*] **例：** `Router(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。 **（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。
ステップ 13	**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 14	**show route-map** [*map-name*] **例：** `Router# 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。

```
Router# 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

ここでは、次の例について説明します。

インバウンド パス選択の変更：例

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 アトリビュート 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 プレフィクス マッチングが利用できます。次に、**set local-preference** 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
```

4 バイト自律システム番号を使用した AS-path アトリビュートの変更によるインバウンド パス選択の変更：例

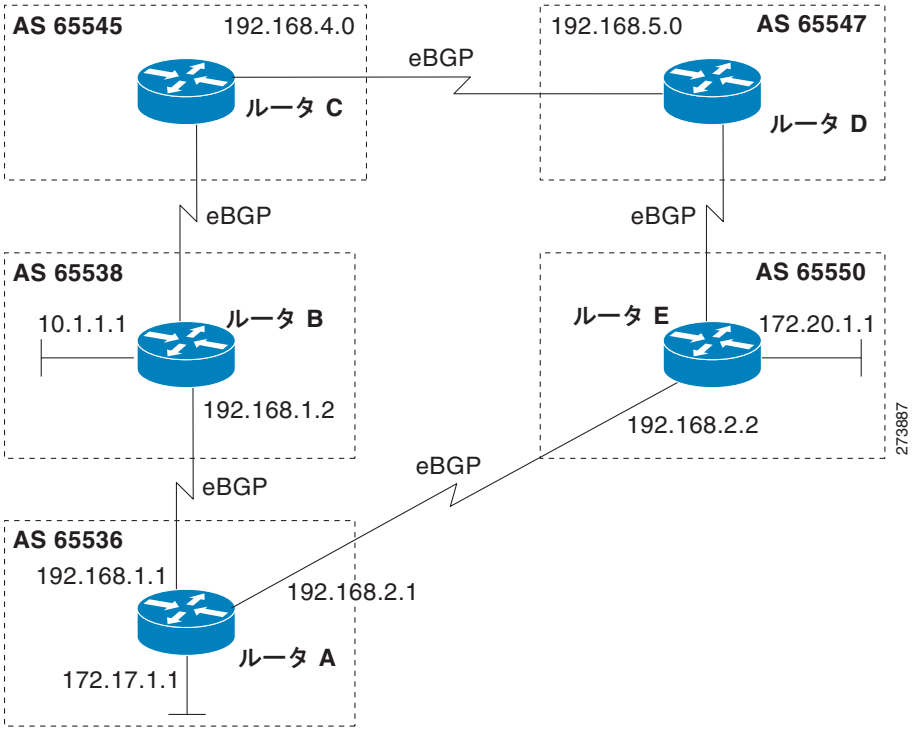
この例は、AS-path アトリビュートの変更によって 172.17.1.0 宛てトラフィックのインバウンド パス選択を変化させるために BGP を設定する方法を示します。Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SXI1、およびそれ以降のリリースで、BGP は 4 オクテット（4 バイト）自律システム番号をサポートするようになりました。この例の 4 バイト自律システム番号は、デフォルトの asplain（10 進数）形式です。たとえば、図 8（P.49）において、ルータ B は自律システム番号 65538 にあります。4 バイト自律システム番号についてのさらに詳しい紹介は、「BGP 自律システム番号の形式」（P.4）を参照してください。

AS-path アトリビュートの変更は、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、図 9 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 アトリビュートが

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。図 9 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 アトリビュート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 9　　AS-path アトリビュート変更のネットワーク トポロジ



この例の設定は、図 9 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
```

アウトバウンド パス選択の変更：例

次に、アウトバウンド ルート フィルタを作成し、ルータ A（10.1.1.1）がルータ B（172.16.1.2）へフィルタをアドバタイズするよう設定する例を示します。FILTER という名前の IP プレフィクスが作成され、サブネット 192.168.1.0/24 をアウトバウンド ルート フィルタリングに指定します。ルータ A がアウトバウンド ルート フィルタをルータ B へアドバタイズできるよう、ORF 送信機能がルータ A で設定されます。

ルータ A 設定（送信側）

```
ip prefix-list FILTER seq 10 permit 192.168.1.0/24
!
router bgp 65100
 address-family ipv4 unicast
 neighbor 172.16.1.2 remote-as 65200
 neighbor 172.16.1.2 ebgp-multihop
 neighbor 172.16.1.2 capability orf prefix-list send
 neighbor 172.16.1.2 prefix-list FILTER in
 end
```

ルータ B 設定（受信側）

次に、ORF 受信機能をルータ A へアドバタイズするようにルータ B を設定する例を示します。ORF 機能が交換された後、ルータ B は FILTER プレフィクス リストで定義されたアウトバウンド ルート フィルタをインストールします。アウトバウンド ルート フィルタをアクティブ化するため、この設定の最後にルータ B でインバウンド ソフト リセットが開始されます。

```
router bgp 65200
 address-family ipv4 unicast
 neighbor 10.1.1.1 remote-as 65100
 neighbor 10.1.1.1 ebgp-multihop 255
 neighbor 10.1.1.1 capability orf prefix-list receive
 end
clear ip bgp 10.1.1.1 in prefix-filter
```

次の例は、set-as-path という名前のルート マップがどのようにネイバー 10.69.232.70 へのアウトバウンド アップデートに適用されるかを示します。ルート マップは自律システム パス「65100 65100」を、アクセス リスト 1 を渡すルートにプリペンドします。ルート マップの 2 番目の部分は、他のルータへのアドバタイズを許可するためのものです。

```
router bgp 65100
 network 172.16.0.0
 network 172.17.0.0
 neighbor 10.69.232.70 remote-as 65200
 neighbor 10.69.232.70 route-map set-as-path out
!
route-map set-as-path 10 permit
 match address 1
 set as-path prepend 65100 65100
!
route-map set-as-path 20 permit
 match address 2
!
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit 172.17.0.0 0.0.255.255
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

プレフィクス リストによる BGP プレフィクスのフィルタリング：例

ここでは、次の例について説明します。

シングル プレフィクス リストを使用した BGP プレフィクスのフィルタリング

次に、プレフィクス 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、プレフィクス リストでプレフィクス 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、プレフィクス長が /8 ～ /24 のプレフィ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 Routing Information Protocol（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クスへの受信アップデートをフィルタリングし、アップデートされているプレフィクスのゲートウェイ（ネクストホップ）をプレフィクス リスト *name2* へマッチングするよう、イーサネット インターフェイス 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 ethernet 0
```

プレフィクスのグループを使用した BGP プレフィクスのフィルタリング

次に、ネットワーク 192/8 でプレフィクス長が 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
```

プレフィクス リスト エントリの追加と削除

プレフィクス 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
```

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：例

このセクションでは、BGP コミュニティをルート マップと使用した 2 つの例を示します。

1 番目の例は、set-community というルート マップがネイバー 172.16.232.50 のアウトバウンド アップデートにどのように適用されるかを示します。アクセス リスト 1 を渡すルートは、特別なコミュニティ アトリビュート値 no-export 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 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 番目の例は、*set-community* というルート マップがネイバー 172.16.232.90 のアウトバウンド アップデートにどのように適用されるかを示します。自律システム 70 で生成されるルートはすべて、コミュニティ値 200 200 を自身の既存の値に追加します。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 .*
```

AS-path フィルタを使用したトラフィック フィルタリング：例

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 .*
```

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 フィルタリング：例

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。

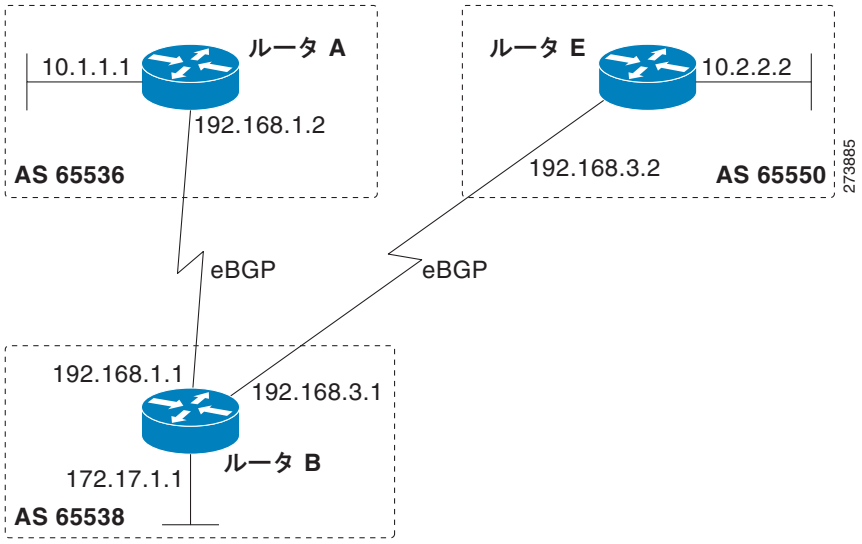
```
ip as-path access-list 2 permit ^1\.0$
router bgp 1.2
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.3.2 filter-list 2 in
  end
```

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：例

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 10　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、図 10 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 4 バイト自律システム 65550 からの、または 65550 経由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。

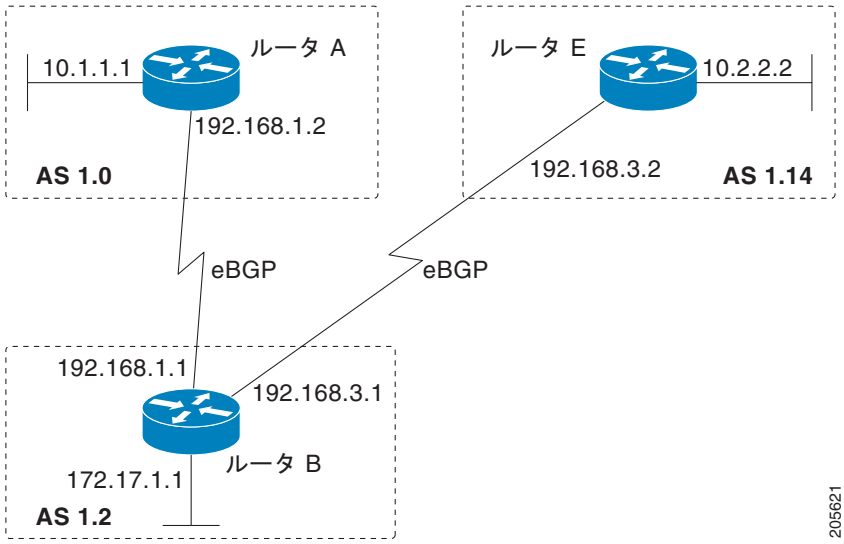
```
ip extcommunity-list expanded DENY65550
 10 deny _65550_
 20 deny ^65550 .*
 resequence 50 100
 exit
router bgp 65538
 network 172.17.1.0 mask 255.255.255.0
 address-family ipv4 unicast
  neighbor 192.168.3.2 remote-as 65550
  neighbor 192.168.1.2 remote-as 65536
  neighbor 192.168.3.2 activate
  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 11　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、図 11 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 4 バイト自律システム 65550 からの、または 65550 経由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
```

BGP ルート マップを使用したトラフィック フィルタリング：例

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
```

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：例

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 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
```

次の作業

- BGP の拡張機能の設定を行う場合、「Configuring Advanced BGP Features」モジュールに進みます。
- BGP ネイバー セッションのオプションを設定するには、「Configuring BGP Neighbor Session Options」モジュールに進みます。
- 内部 BGP の設定を行う場合、「Configuring Internal BGP Features」モジュールに進みます。

参考資料

次のセクションでは、外部 BGP を使用したサービス プロバイダーとの接続に関連した参考資料を紹介します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands 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 Overview」モジュール
BGP 基本作業の設定	「Configuring a Basic BGP Network」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）

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 5 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

このテクノロジーに含まれる、ここで記述されていない機能の情報については、『Cisco BGP Implementation Roadmap』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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 5 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 5　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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ポリシー設定」（P.9） • 「AS-path フィルタを使用した BGP プレフィクスのフィルタリング」（P.45）
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 アトリビュート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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP コミュニティ」（P.10） • 「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」（P.52）

表 5　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 （続き）

機能名	リリース	機能の設定情報
BGP プレフィクスベース アウトバウンド ルート フィルタリング	12.0(22)S 12.2(4)T 12.2(14)S 15.0(1)S	BGP プレフィクスベース アウトバウンド ルート フィルタリング機能は、BGP ORF 送受信機能を使用して、BGP ピアの間で送られる BGP アップデートの数を最小化します。この機能を設定すると、不要なルーティング アップデートをソースでフィルタリングできるため、ルーティング アップデートの生成や処理に必要なシステム リソースの量を減らす助けになります。たとえば、この機能を使用して、サービス プロバイダー ネットワークからのルート全体を受け付けるのではないルータで、ルータに要求される処理の量を減らすことができます。 次のセクションで、この機能に関する情報を参照できます。 • 「アウトバウンド BGP ルート プレフィクスのフィルタリング」（P.23） • 「アウトバウンド パス選択の変更：例」（P.70）
BGP ルート マップ継続	12.0(24)S 12.2(18)S 12.2(18)SXD 12.2(27)SBC 12.3(2)T 15.0(1)S Cisco IOS XE 3.1.0SG	BGP ルート マップ継続機能により、continue 句が BGP ルート マップ設定に導入されます。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。 次のセクションで、この機能に関する情報を参照できます。 • 「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」（P.62） • 「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：例」（P.77）
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	12.0(31)S 12.2(33)SB 12.2(33)SRB 12.2(33)SXI 12.4(4)T 15.0(1)S Cisco IOS XE 3.1.0SG	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。 次のセクションで、この機能に関する情報を参照できます。 • 「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」（P.62） • 「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：例」（P.77）

表 5　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 （続き）

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 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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ルート マップ ポリシー リスト」（P.12） • 「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」（P.59）

表 5　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 （続き）

機能名	リリース	機能の設定情報
4 バイト ASN に対する BGP サポート	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 15.0(1)S Cisco IOS XE 3.1.0SG	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、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す。 Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、および 12.2(33)SXI1 では、シスコは 4 バイト自律システム番号の実装時に、asplain 形式を正規表現マッチングのデフォルト、また自律システム番号の出力表示形式として使用しています。しかし、RFC 5396 が記述する asplain と asdot 形式のどちらでも、4 バイト自律システム番号を設定できます。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** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 自律システム番号の形式」（P.4） • 「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 プレフィクスのフィルタリング」（P.48） • 「4 バイト自律システム番号を使用した AS-path アトリビュートの変更によるインバウンド パス選択の変更：例」（P.68） • 「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 フィルタリング：例」（P.74） • 「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：例」（P.74） この機能により、次の各コマンドが追加または変更されています。**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**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 5　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 （続き）

機能名	リリース	機能の設定情報
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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP コミュニティ」（P.10） • 「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」（P.55）
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	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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP コミュニティ」（P.10） • 「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」（P.55）
BGP 4 プレフィクス 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	この機能については、次の項に説明があります。 • 「BGP ポリシー設定」（P.9） • 「インバウンド パス選択の変更：例」（P.67）

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 Autonomous System Number（ASN; 自律システム番号）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 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 ASN を削除することが必要です。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「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」（P.12）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

目次

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

この機能には、次の制約事項があります。

- 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

プライベート 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。有効な範囲は 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。なぜならプライベート AS 番号は一意ではなく、BGP 最良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、発信更新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 Release 15.1(2)T より前は、この機能に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、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、長さゼロの AS パスにはなりません。
- **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更新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

ここでは、次の作業について説明します。

- 「AS パスからプライベート ASN の削除および交換（Cisco IOS リリース　15.1(2)T 以降）」（P.3）（必須）

AS パスからプライベート ASN の削除および交換（Cisco IOS リリース 15.1(2)T 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。さらにプライベート AS 番号をローカル ルータの AS 番号と交換する場合は、ステップ 17 で **all replace-as** キーワードを含めてください。

この作業例は、図 1（P.8）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** の例
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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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。
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

ここでは、次の例について説明します。

- 「例：プライベート ASN の削除（Cisco IOS Release 15.1(2)T）」（P.6）
- 「例：プライベート ASN の削除および交換（Cisco IOS Release 15.1(2)T）」（P.7）
- 「例：プライベート ASN の削除（Cisco IOS Release 12.2）」（P.8）

例：プライベート ASN の削除（Cisco IOS Release 15.1(2)T）

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#
```

例：プライベート ASN の削除および交換（Cisco IOS Release 15.1(2)T）

次の例では、ルータ A がピア 172.30.0.7 にプレフィクスを送信すると、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

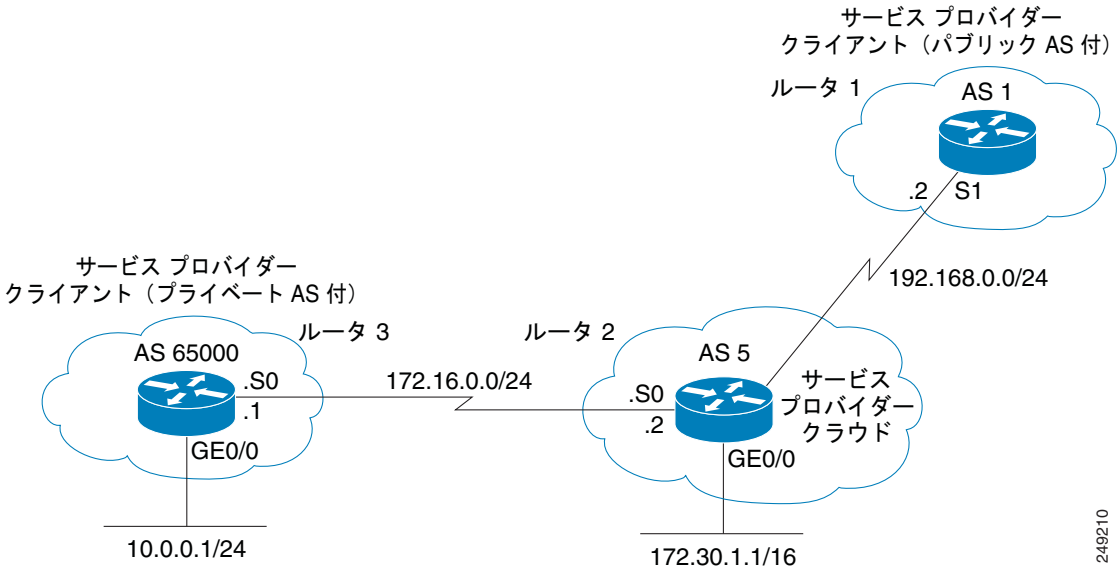
```
router bgp 200
 bgp log-neighbor-changes
 neighbor 172.30.0.6 remote-as 100
 no auto-summary
```

例：プライベート ASN の削除（Cisco IOS Release 12.2）

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。

図 1 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 1　　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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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	参照先
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*』
このテクノロジーについて、ここで説明していない機能に関する情報	『*BGP Features Roadmap*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB 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、および機能セットの 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

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

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　BGP - プライベート AS の削除および交換の機能情報

機能名	リリース	機能情報
BGP - プライベート AS の削除および交換	15.1(2)T、15.0(1)S	プライベート Autonomous System（AS; 自律システム）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**

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、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。このモジュールには、BGP ネイバー セッションのコマンドを使用して、高速セッションを無効に設定し、ピアリング セッションがディセーブルまたはダウン状態のときにルータが BGP ネイバー ピアリング セッションを自動的に再確立するように設定し、自律システムの移行に役立つオプションを設定し、簡単なセキュリティ メカニズムを設定して外部 BGP（eBGP）ピアリング セッションを CPU 利用率に基づく攻撃から防御する作業が含まれます。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP ネイバー セッションのオプション設定の機能情報」（P.46）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

BGP ネイバー セッション オプションの設定の前提条件

BGP の拡張機能を設定する前に、「Cisco BGP Overview」モジュールと「Configuring a Basic BGP Network」モジュールについて十分に理解しておく必要があります。

BGP ネイバー セッション オプションの設定の制約事項

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。

BGP ネイバー セッション オプションの設定に関する情報

このモジュールで BGP 機能を設定するには、次の概念を理解しておく必要があります。

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 Transmission Control Protocol（TCP; 伝送制御プロトコル）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、Cisco IOS 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 セッションによってもたらされる可能性がある不安定な状態から保護します。BGP ルータは、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、拒否文が返された場合、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。

最大プレフィクス到達後の BGP ネイバー セッションの再起動

プレフィクス制限および BGP ピアリング セッション

BGP を実行するルータがピア ルータから受信可能なプレフィクスの最大数に関して設定可能な制限があります。この制限は、**neighbor maximum-prefix** コマンドで設定されます。ルータがピア ルータから過剰のプレフィクスを受信し、最大プレフィクス制限を超えると、このピアリング セッションはディセーブルになるか、ダウン状態になります。このセッションは、ネットワーク オペレータが **clear ip bgp** コマンドを入力して、手動でセッションを再アクティブ化するまでダウン状態のままです。**clear ip bgp** コマンドを入力すると、格納されたプレフィクスはクリアされます。

最大プレフィクス制限による BGP ネイバー セッションの再起動

Cisco IOS Release 12.0(22)S、12.2(15)T、12.2(18)S、およびこれら以降のリリースでは、**restart** キーワードが導入され、**neighbor maximum-prefix** コマンドの機能が拡張されています。この機能拡張により、ネットワーク オペレータは、BGP ネイバー ピアリング セッションがディセーブルまたはダウン

状態のときにルータがこのピアリング セッションを自動的に再確立するように設定できます。ピアリングが自動的に再確立できる設定可能な時間間隔があります。**restart** キーワードの設定可能なタイマー引数は、分単位で指定されます。時間の範囲は、
1 ～ 65,535 分です。

BGP ネットワーク自律システムの移行

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 アトリビュート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 パスのカスタマイゼーションにより、設定ミスによりルーティング ループが作成される可能性が高まります。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、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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す。

Cisco の 4 バイト自律システム番号の実装は、Request For Comments（RFC; コメント要求）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。RFC 4893 では新たに 23456 が予約済み（プライベート）自律システム番号に指定され、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なくなっています。

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。

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、通常、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ディセーブルにしようとする典型的な力任せの Denial of Service（DoS; サービス拒絶）攻撃です。

TTL セキュリティ チェックは、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、このパケットはサイレントに廃棄され、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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。この機能がイネーブルの場合、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。この機能をイネーブルにすると、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** コマンドを使用してディセーブル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** コマンドを使用してイネーブル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数が一致するように *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。この機能がイネーブルの場合、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 Path 最大伝送ユニット（MTU）Discovery に対する BGP サポート

Path MTU Discovery（PMTUD）

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、Maximum Transmission Unit（MTU; 最大伝送ユニット）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、Maximum Segment Size（MSS; 最大セグメント サイズ）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。

Path MTU Discovery（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、インターネット制御メッセージ プロトコル（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イネーブルにされますが、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 をディセーブル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、任意のパケットから転送された TCP 接続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 をディセーブルにする必要がある場合があります。Cisco IOS Release 12.2(33)SRA、12.2(31)SB、12.2(33)SXH、12.4(20)T、およびこれら以降のリリースでは、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ディセーブル、または再度イネーブルにできます。TCP の PMTUD をすべての BGP ネイバーに対してグローバルにディセーブルにするには、**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 をディセーブルにするには、**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 のグローバルなディセーブル化」（P.22）または「単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化」（P.25）を参照してください。

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。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ピア グループのアクティベーション（*範囲のグループの受信*と呼ばれる）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コマンドライン インターフェイス（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には、次の 3 つの **show** 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アップデートされている必要があります。コマンドは、**show ip bgp neighbors**、**show ip bgp peer-group**、**show ip bgp summary** コマンドです。

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 ネイバー セッションのオプションの設定方法

ここでは、次の作業または作業グループについて説明します。

- 「高速セッションの非アクティブ化の設定」（P.8）
- 「最大プレフィ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ルータの設定」（P.12）
- 「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」（P.16）
- 「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」（P.18）
- 「セッションごとの TCP の PMTUD に対する BGP サポートの設定」（P.22）
- 「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」（P.31）

高速セッションの非アクティブ化の設定

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 Interior Gateway Protocol（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、「Configuring Internal BGP Features」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」（P.9）
- 「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」（P.10）

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。

IGP ルートの積極的ダンプニング

この機能をイネーブルにすると、BGP コンバージェンス時間が大幅に向上します。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアは、引き続き BGP ネイバー セッションに不安定な状態をもたらす場合があります。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：** `Router> enable`	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。
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*] **例：** `Router(config-router-af)# 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* **remote-as** *autonomous-system-number* **例：** `Router(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：** `Router(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：** `Router(config-router-af)# 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。

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、拒否文が返された場合、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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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	**neighbor** *ip-address* **fall-over** [**route-map** *map-name*] **例：** `Router(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：** `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	**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 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：** `Router(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、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：** `Router(config-route-map)# match ip address prefix-list FILTER28`	指定されたプレフィクス 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、この作業に適用される構文だけが使用されます。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 10	**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。

次の作業

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、ネクストホップの RIB にインストールされたルートの変更に対する BGP の応答時間を向上させます。また、BGP コンバージェンス全体も向上させます。BGP ネクストホップ アドレス トラッキングの詳細については、「Configuring Advanced BGP Features」モジュールを参照してください。

最大プレフィ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ルータの設定

BGP ピアから受信されたプレフィクス数が最大プレフィクス制限を超えたときに、ルータによって 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。

ネイバー セッションの再確立

ネットワーク オペレータは、設定された最大プレフィ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 を実行しているルータを設定できます。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。

制約事項

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、超過プレフィクス数を送信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クス数を減らす必要があります。プレフィ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、ネットワークで過剰な数のプレフィクスが即座にアドバタイズされ、除去されます。この場合、ネットワーク オペレータが問題の原因を修正する間に、**warning-only** キーワードを設定し、再起動機能をディセーブルにできます。

手順の概要

1. **enable**

2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
5. **exit**
6. **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：** `Router> enable`	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。
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* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**] **例：** `Router(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クス制限を設定します。 • **restart** キーワードおよび *restart-interval* 引数を使用して、最大プレフィクス制限を超えたためにディセーブルになったネイバー 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。*restart-interval* の設定範囲は、1 ～ 65535 分 です。 • **warning-only** キーワードを使用して、過剰なプレフィクスを送信しているピアを修正できるように、再起動機能がディセーブルになるようにルータを設定します。 **（注）** *restart-interval* が設定されていないと、最大プレフィクス制限を超えた後もディセーブルになったセッションはダウン状態のままになります。これがデフォルトの動作です。

	コマンドまたはアクション	目的
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 6	**show ip bgp neighbors** *ip-address* **例：** `Router# 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。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

show ip bgp neighbors コマンドの次の出力例により、ディセーブルになったネイバー 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 の最大プレフィクス制限が 1000 プレフィクス、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。

```
Router# 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 ソフト再設定を使用して 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クスをクリアして、BGP を実行しているルータが最大プレフィクス制限を超えないようにするために使用できます。BGP ソフト再設定の使用方法の詳細については、「Configuring a Basic BGP Network」モジュールの「Monitoring and Maintaining Basic BGP task」を参照してください。

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。ネットワーク オペレータは、最大プレフィクス制限に設定された値および過剰な数のプレフィ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。このコマンドを使用する必要があるのは、トラブルシューティング時または過剰な数のプレフィクスを送信しているルータを調整する場合だけです。BGP のルートのダンプニングの詳細については、「Configuring Advanced BGP Features」モジュールを参照してください。

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。

制約事項

- この機能は、正しい eBGP ピアリング セッションのため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。
- この機能は、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に設定できます。このコマンドがピアのグループに適用されると、そのピアは個別にカスタマイズできなくなります。

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* **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]
6. **neighbor** *ip-address* **remove-private-as**
7. **exit**
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。
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`	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 アトリビュート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 アトリビュートにプリペンドします。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、プリペンドされません。 • **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：** `Router(config-router)# neighbor 10.0.0.1 remove-private-as`	（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。 • 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 アトリビュートから自動的に削除されます。
ステップ 7	**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。 • このコマンドを繰り返し、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 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(config)# 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）。

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 値以上の場合だけ 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、次の作業を設定します。

前提条件

- この機能の効果を最大化するには、これを参加している各ルータで設定することを推奨します。この機能をイネーブルにすると、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。

制約事項

- この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ディセーブル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、この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：** `Router> enable`	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。
ステップ 2	**trace** [*protocol*] *destination* **例：** `Router# 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数を決定します。
ステップ 3	**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 4	**router bgp** *autonomous-system-number* **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 プロセスを作成します。
ステップ 5	**neighbor** *ip-address* **ttl-security hops** *hop-count* **例：** `Router(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数に設定されます。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。 • この機能がイネーブルの場合、BGP は、予想される TTL 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、サイレントに廃棄されます。 • 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。
ステップ 6	**end** **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 running-config** **例：** `Router# 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 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。ここには、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、この作業に適用される構文だけが使用されます。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 8	**show ip bgp neighbors** [*ip-address*] **例：** `Router# 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、この機能がイネーブルの場合、「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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

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、次の作業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 のグローバルなディセーブル化」（P.22）
- 「単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化」（P.25）
- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化」（P.27）
- 「単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化」（P.29）

すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化

すべての BGP セッションに対して TCP の PMTUD をディセーブルにするには、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、デフォルトでイネーブルになりますが、**show ip bgp neighbors** コマンドを入力して、TCP の PMTUD がイネーブルになっていることを確認することを推奨します。

前提条件

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：** `Router> enable`	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。
ステップ 2	**show ip bgp neighbors** [*ip-address*] **例：** `Router# 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 がイネーブルかどうかを判断します。 **（注）** この例では、この作業に適用される構文だけが使用されます。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 3	**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 4	**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 5	**no bgp transport path-mtu-discovery** **例：** `Router(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 をディセーブルにします。
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。
ステップ 7	**show ip bgp neighbors** **例：** `Router# 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 がイネーブルであることは、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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対してイネーブル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 がイネーブル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** コマンドが入力された後の **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 のディセーブル化

internal BGP（iBGP; 内部 BGP）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 をディセーブルにするには、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。

前提条件

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イネーブル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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 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。

	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：** `Router(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：** `Router(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。 • 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 7	**no neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**} **例：** `Router(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 をディセーブルにします。 • この例では、TCP の PMTUD がネイバー 172.16.1.1 に対してディセーブルになります。
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。
ステップ 9	**show ip bgp neighbors** **例：** `Router# 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 をイネーブルにしたことを表示しません。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力例は、TCP の PMTUD が BGP ネイバー 172.16.1.1 に対してディセーブルにされたが、BGP ネイバー 192.168.2.2 に対しては引き続きイネーブル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 がイネーブル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 のグローバルなイネーブル化

すべての BGP セッションに対して TCP の PMTUD をイネーブルにするには、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、デフォルトでイネーブルになりますが、この機能がディセーブルになっている場合、この作業によってこの機能を再度イネーブルにできます。TCP の PMTUD がイネーブル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。

前提条件

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：** `Router> enable`	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。
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 プロセスを作成または設定します。
ステップ 4	**bgp transport path-mtu-discovery** **例：** `Router(config-router)# bgp transport path-mtu-discovery`	すべての BGP セッションに対して TCP の PMTUD をイネーブルにします。
ステップ 5	**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。
ステップ 6	**show ip bgp neighbors** **例：** `Router# 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 をイネーブルにしたことを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対してイネーブル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 がイネーブル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 のイネーブル化

外部 BGP（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 をイネーブルにするには、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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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 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：** `Router(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：** `Router(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。 • この例では、eBGP ネイバー 192.168.2.2 がアクティブ化されます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**} **例：** `Router(config-router-af)# neighbor 192.168.2.2 transport path-mtu-discovery`	単一の BGP ネイバーに対して TCP の PMTUD をイネーブルにします。 • この例では、TCP の PMTUD が eBGP ネイバー 192.168.2.2 に対してイネーブルにされます。
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。
ステップ 9	**show ip bgp neighbors** [*ip-address*] **例：** `Router# 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。 • この例では、このコマンドの出力は、ネイバー 192.168.2.2 が TCP の PMTUD をイネーブルにしたことを示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

show ip bgp neighbors コマンドの次の出力例は、TCP の PMTUD が BGP ネイバー 192.168.2.2 に対してイネーブルにされたことを示します。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 がイネーブル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
```

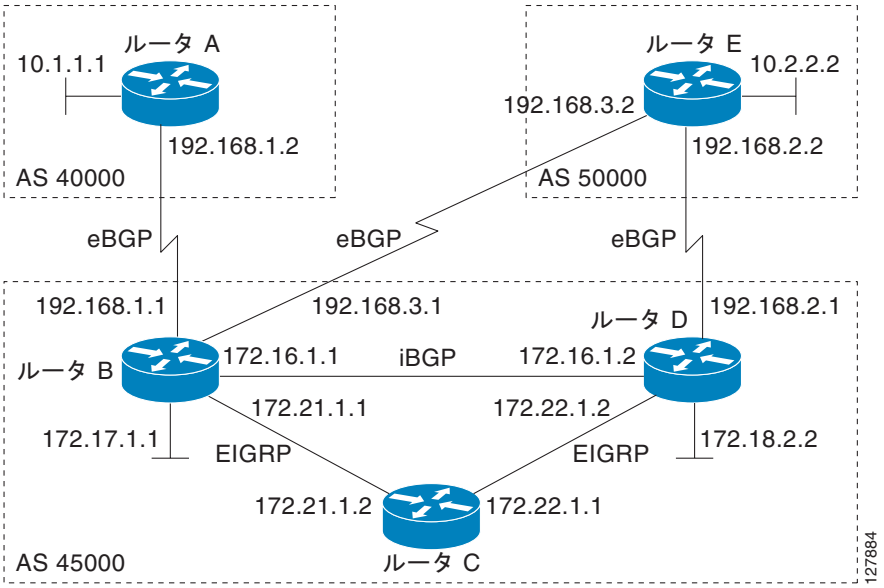
サブネット範囲を使用する BGP ダイナミック ネイバーの実装

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 グループが図 1 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（図 1 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、隣接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 1　BGP ダイナミック ネイバー トポロジ



前提条件

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。

制約事項

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** *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**
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：** `RouterB> enable`	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。 • この設定はルータ B に入力されます。
ステップ 2	**configure terminal** **例：** `RouterB# configure terminal`	グローバル コ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：** `RouterB(config)# router bgp 45000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp log-neighbor-changes** **例：** `RouterB(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。予期しないネイバーのリセットは、ネットワークでのエラー率が高いことまたはパケット損失が高いことを示す場合があり、調査する必要があります。
ステップ 5	**neighbor** *peer-group-name* **peer-group** **例：** `RouterB(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。

	コマンドまたはアクション	目的
ステップ 6	**bgp listen** [**limit** *max-number*] **例：** RouterB(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。 • この例では、作成可能なダイナミック ネイバーの最大数は、200 です。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細な構文については、ステップ 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：** RouterB(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クス範囲を定義します。 • この例では、プレフィクス範囲 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：** RouterB(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。
ステップ 9	**neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] **例：** RouterB(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 グループだけとともに使用され、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：** RouterB(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。

	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*} **activate** **例：** `RouterB(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：** `RouterB(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：** `RouterE> enable`	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。 • この設定はルータ E に入力されます。
ステップ 15	**configure terminal** **例：** `RouterE# configure terminal`	グローバル 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：** `RouterE(config)# router bgp 50000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] **例：** `RouterE(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（図 1 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：** `RouterB# show ip bgp summary`	（任意）BGP ネイバーへのすべての接続の BGP パス、プレフィクス、およびアトリビュート情報を表示します。 • この手順では、この設定はルータ B に戻っています。

	コマンドまたはアクション	目的
ステップ 20	**show ip bgp peer-group** [*peer-group-name*] [**summary**] **例：** `RouterB# show ip bgp peer-group group192`	（任意）BGP ピア グループの情報を表示します。 • この例では、受信範囲グループであるグループ 192 の情報が表示されます。
ステップ 21	**show ip bgp neighbors** [*ip-address*] **例：** `RouterB# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの BGP 接続および TCP 接続の情報が表示されます。 • 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。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に示す出力例は、この作業の適切な設定手順がルータ B とルータ E の両方で完了した後に、図 1 のルータ 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 のメンバであることを示します。この出力は、IP プレフィクス範囲 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
.
.
.
```

BGP ネイバー セッション オプションの設定例

ここでは、次の設定例について説明します。

- 「BGP ネイバー の高速セッションの非アクティブ化の設定：例」（P.38）
- 「高速セッション非アクティブ化の選択的アドレス トラッキングの設定：例」（P.38）
- 「最大プレフィクス制限設定後のセッションの再起動：例」（P.38）
- 「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」（P.38）
- 「TTL セキュリティ チェックの設定：例」（P.40）
- 「セッションごとの TCP の PMTUD に対する BGP サポートの設定：例」（P.40）
- 「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：例」（P.41）

BGP ネイバー の高速セッションの非アクティブ化の設定：例

次の例では、BGP ルーティング プロセスがルータ A およびルータ B で設定され、この 2 つのルータ間でネイバー 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ルータで必要ではありませんが、このネイバー セッションが無効にされている場合、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。

ルータ A

```
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 fall-over
 end
```

ルータ B

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

高速セッション非アクティブ化の選択的アドレス トラッキングの設定：例

次に、/28 のプレフィ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
```

最大プレフィクス制限設定後のセッションの再起動：例

次の例では、ネイバー 192.168.6.6 で許可されるプレフィクスの最大数が 2000 に設定され、ピアリング セッションがディセーブルになった場合に、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ルータが設定されます。

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 2000 restart 30
```

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

次に、この機能の設定方法および確認方法の例を示します。

- 「デュアル AS の設定：例」（P.39）
- 「デュアル AS コンフェデレーションの設定：例」（P.39）
- 「Replace-AS の設定：例」（P.40）

デュアル AS の設定：例

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
```

デュアル AS コンフェデレーションの設定：例

次の例は、前の例のルータ 1 の設定で使用できます。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
 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
```

Replace-AS の設定：例

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
```

TTL セキュリティ チェックの設定：例

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
```

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

ここでは、次の設定例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 のグローバルなディセーブル化：例」（P.40）
- 「単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化：例」（P.41）
- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化：例」（P.41）
- 「単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化：例」（P.41）

すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化：例

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD をディセーブル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 がディセーブル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
```

単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化：例

次に、外部 BGP（eBGP）ネイバー 192.168.2.2 に対して TCP の PMTUD をディセーブル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
```

すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化：例

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD をイネーブル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 がイネーブル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
```

単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化：例

次に、外部 BGP（eBGP）ネイバー 192.168.2.2 に対して TCP の PMTUD をイネーブル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 がイネーブル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
```

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：例

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。次の設定例は、サブネット範囲を使用する BGP ダイナミック ネイバーを実装する方法を示します。

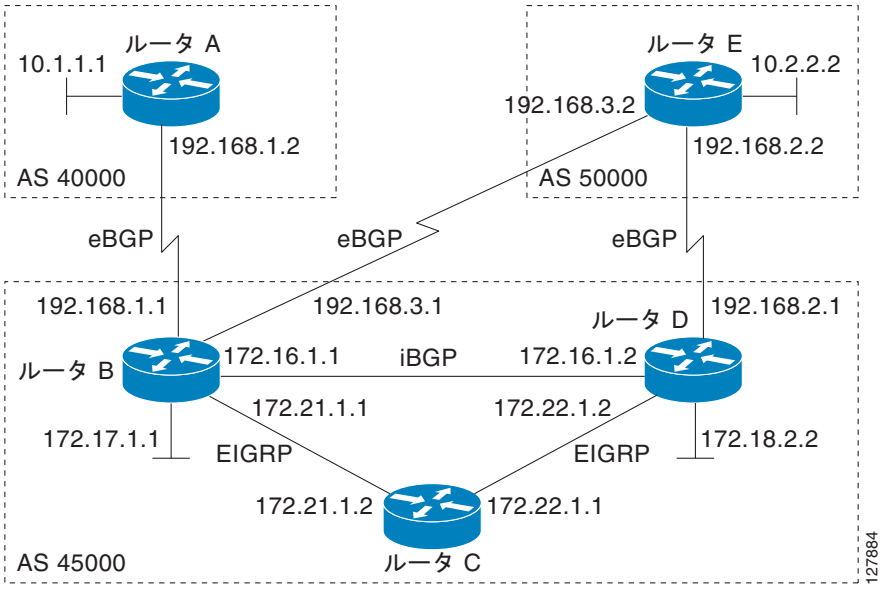
次の例では、2 つの BGP ピア グループが図 2 のルータ B に作成され、ダイナミック BGP ネイバー数に関してグローバル制限が設定され、サブネット範囲がピア グループに関連付けられます。サブネット範囲を設定すると、ダイナミック BGP ネイバー プロセスがイネーブルになります。このピア グループは、ローカル ルータの BGP ネイバー テーブルに追加され、代替自律システム番号もこのピア グループの 1 つであるグループ 192 に設定されます。このサブネット範囲ピア グループおよび標準 BGP ピアは、その後 IPv4 アドレス ファミリの下でアクティブ化されます。

この設定は、別のルータ（図 2 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、隣接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（図 2 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、**show ip bgp summary** コマンドの出力がルータ B に入力されて終了します。

図 2　　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** コマンドは、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
```

次の作業

- 外部サービス プロバイダーに接続して、他の外部 BGP 機能を使用するには、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。
- 一部の内部 BGP 機能を設定するには、『*Cisco IOS IP Routing Protocols Configuration Guide*』の BGP セクションで、「Configuring Internal BGP Features」の章を参照してください。
- BGP ネクストホップ アドレス トラッキングやルート ダンプニングなどの BGP の拡張機能の一部を設定する場合は、「Configuring Advanced BGP Features」モジュールを参照してください。

参考資料

ここでは、BGP の拡張機能の設定に関連する参考資料について説明します。

関連資料

関連項目	参照先
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 Overview」モジュール
BGP の基本作業のコンセプトと設定の詳細。	「Configuring a Basic BGP Network」モジュール
高度な BGP 作業の概念および設定の詳細	「Configuring Advanced BGP Features」モジュール

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/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

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS リリース 12.2(1)、12.0(3)S、12.2(33)SRA、12.2(31)SB、12.2(33)SXH、またはこれら以降のリリースで導入または変更された機能だけがこのテーブルに表示されます。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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	機能の設定情報
BGP ダイナミック ネイバー	12.2(33)SXH 15.0(1)S	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。3 つの **show** コマンドの出力は、ダイナミック ネイバーに関する情報を表示するようにアップデートされています。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ダイナミック ネイバー」（P.8） • 「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」（P.31） • 「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：例」（P.41） 次のコマンドがこの機能によって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**。
最大プレフィクス制限後の BGP 再起動セッション	12.0(22)S 12.2(15)T 12.2(18)S 15.0(1)S	最大プレフィクス制限後の BGP 再起動セッション機能により、**restart** キーワードが導入されて、**neighbor maximum-prefix** コマンドの機能が拡張されます。この機能拡張により、ネットワーク オペレータは、ピアから受信したプレフィクス数が最大プレフィクス制限を超えたときに、ピアリング セッションが別のルータによって再確立される時間間隔を設定できます。 次のセクションで、この機能に関する情報を参照できます。 • 「最大プレフィクス到達後の BGP ネイバー セッションの再起動」（P.3） • 「最大プレフィ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ルータの設定」（P.12） • 「最大プレフィクス制限設定後のセッションの再起動：例」（P.38） 次のコマンドが変更されました。**neighbor maximum-prefix**、**show ip bgp neighbors**。

表 1　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 （続き）

機能名	リリース	機能の設定情報
BGP の選択的アドレス トラッキング	12.4(4)T 12.2(31)SB 12.2(33)SRB	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。 次のセクションで、この機能に関する情報を参照できます。 • 「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」（P.3） • 「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」（P.10） • 「高速セッション非アクティブ化の選択的アドレス トラッキングの設定：例」（P.38） この機能によって、**bgp nexthop** コマンドおよび **neighbor fall-over** コマンドが変更されました。

表 1　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 （続き）

機能名	リリース	機能の設定情報
4 バイト ASN に対する BGP サポート	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 15.0(1)S	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、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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す。 Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、および 12.2(33)SXI1 では、4 バイト自律システム番号の Cisco による実装は、自律システム番号のデフォルトの正規表現一致および出力表示形式として asplain 形式を使用しますが、RFC 5396 で説明されているように、4 バイト自律システム番号を asplain 形式と asdot 形式の両方に設定できます。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** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネットワーク自律システムの移行」（P.4） この機能により、次の各コマンドが追加または変更されています。**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**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 1　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 （続き）

機能名	リリース	機能の設定情報
ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	12.0(27)S 12.2(25)S 12.3(11)T 12.2(33)SRA 12.2(33)SXH 15.0(1)S	ネットワーク AS 移行に対するデュアル 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 機能が拡張されます。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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネットワーク自律システムの移行」（P.4） • 「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」（P.16） • 「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」（P.38） 次のコマンドがこの機能によって変更されました。**neighbor local-as**。
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	12.0(29)S 12.3(14)T 12.2(33)SRA 12.2(31)SB 12.2(33)SXH 15.0(1)S	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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP の高速ピアリング セッションの非アクティブ化」（P.3） • 「BGP ネイバー の高速セッションの非アクティブ化の設定」（P.9） • 「BGP ネイバー の高速セッションの非アクティブ化の設定：例」（P.38） 次のコマンドがこの機能によって変更されました。**neighbor fall-over**。

表 1　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 （続き）

機能名	リリース	機能の設定情報
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	伝送制御プロトコル（TCP）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、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。 次のセクションで、この機能に関する情報を参照できます。 • 「セッションごとの TCP Path 最大伝送ユニット（MTU）Discovery に対する BGP サポート」（P.7） • 「セッションごとの TCP の PMTUD に対する BGP サポートの設定」（P.22） • 「セッションごとの TCP の PMTUD に対する BGP サポートの設定：例」（P.40） 次のコマンドがこの機能によって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、external Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネイバー セッションの TTL セキュリティ チェック」（P.5） • 「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」（P.18） • 「TTL セキュリティ チェックの設定：例」（P.40） 次のコマンドがこの機能によって導入または変更されました。**neighbor ttl-security**、**show ip bgp neighbors**。

内部 BGP 機能の設定

このモジュールでは、内部 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）機能を設定する手順について説明します。Internal BGP（iBGP; 内部 BGP）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ボーダー ゲートウェイ プロトコル（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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「内部 BGP 機能設定用の機能情報」（P.16）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

内部 BGP 機能の設定法

次のセクションには任意の内部 BGP（iBGP）設定作業があります。

- 「ルーティング ドメイン コンフェデレーションの設定」（任意）
- 「ルート リフレクタの設定」（任意）
- 「BGP タイマーの調整」（任意）
- 「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」（任意）
- 「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」（任意）
- 「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」（任意）
- 「ルート ダンプニングの設定」（任意）

ルーティング ドメイン コンフェデレーションの設定

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。それぞれの自律システムはそれ自体内で完全メッシュ化され、同一のコンフェデレーションにある他の自律システムとの接続をいくつか持っています。他の自律システムのピアに external BGP（eBGP; 外部 BGP）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）アトリビュート、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 Interior Gateway Protocol（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 コンフェデレーション ID 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 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。

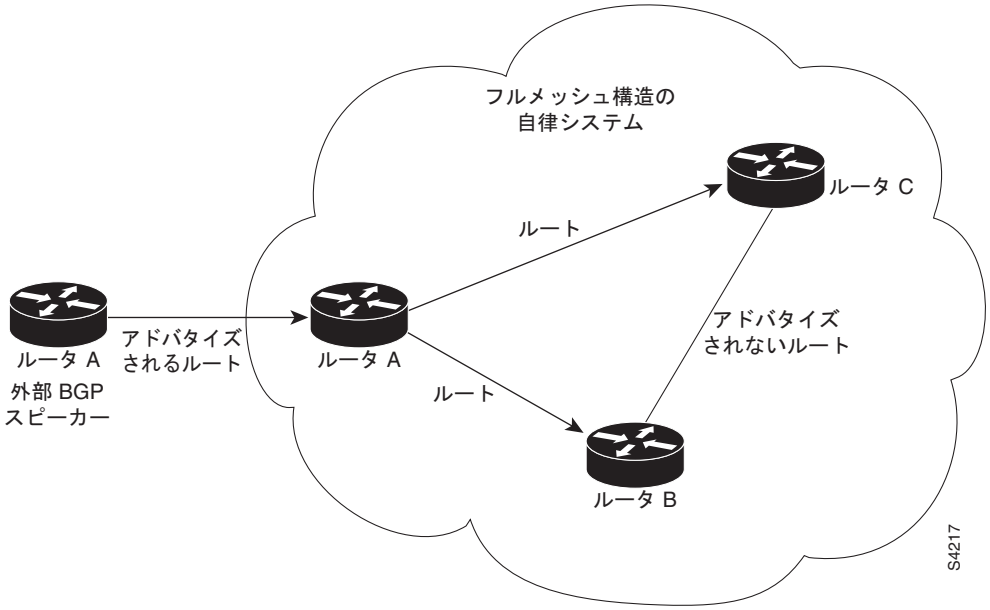
iBGP メッシュを削減する他の方法については「ルート リフレクタの設定」を参照してください。

ルート リフレクタの設定

BGP を使用するには、iBGP スピーカーすべて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、この要件はうまくスケーリングできません。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。

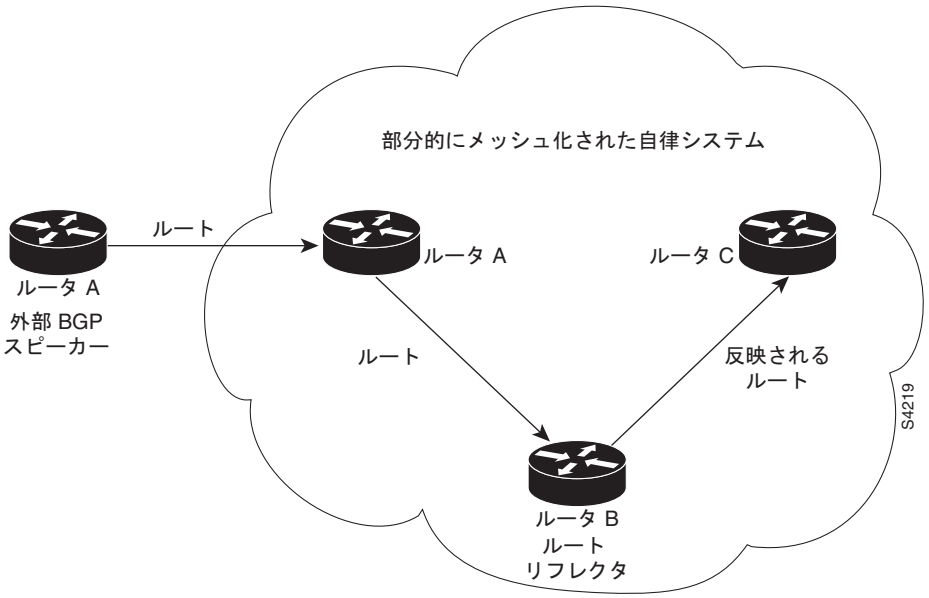
図 1 に、3 つの iBGP スピーカー（ルータ A、B、C）を持つ、単純な iBGP 設定の例を示します。ルート リフレクタがない場合、外部ネイバーからルータ A がルートを受信すると、ルータ B および C にもアドバタイズする必要があります。ルータ B および C は、iBGP が学習したルートを他の iBGP スピーカーに再アドバタイズしません。その理由は、これらのルータは内部のネイバーから学習したルートを他の内部ネイバーに渡さないからです。こうして、ルーティング情報のループを回避します。

図 1　　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、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 スピーカーが完全メッシュ化されてい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 ピアが設定されます。図 2 では、ルータ B はルート 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。

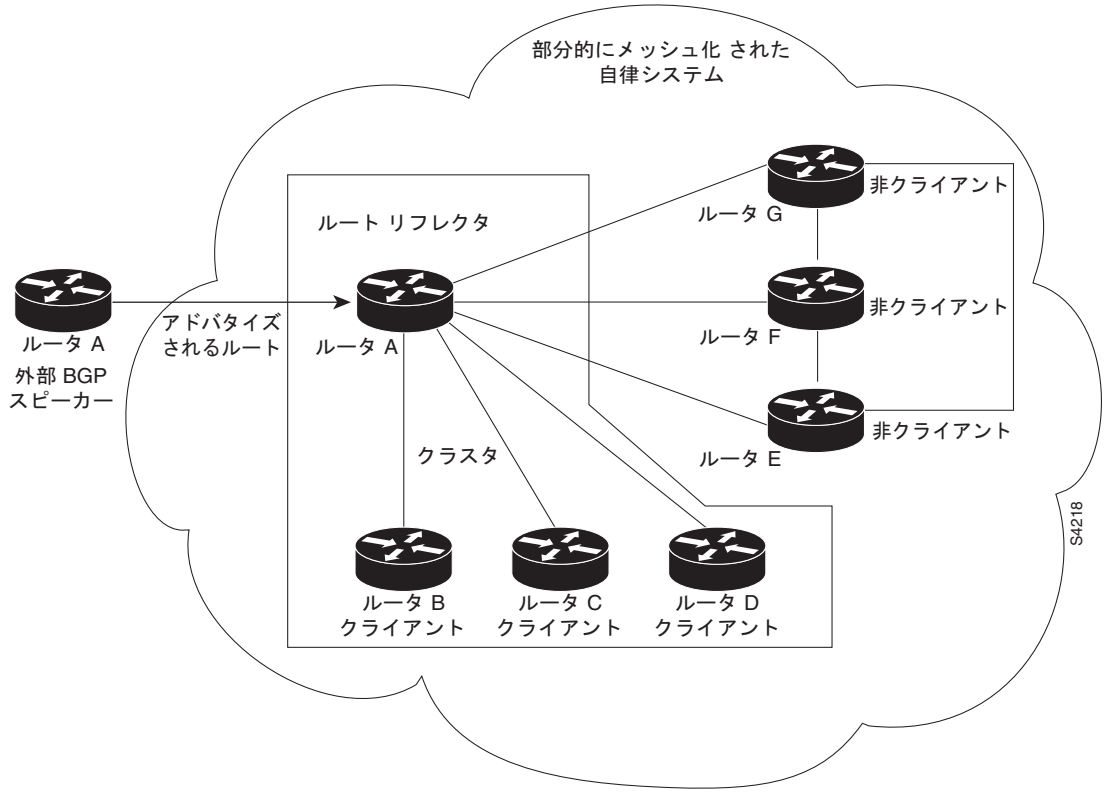
図 2　ルート リフレクタのある単純な BGP モデル



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、この 2 種類のグループ間のルートを反映します。ルート リフレクタおよびそのクライアントのピアは、*クラスタ*を形成します。非クライアント ピアは互いに完全メッシュ化されている必要がありますが、クライアントのピアは、完全メッシュ化されている必要はありません。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。

図 3 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 を持つクラスタのルート リフレクタです。ルータ E、F、および G は完全メッシュ化された、非クライアント ルータです。

図 3　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、ネイバーによっ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は、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されます。
- 非クライアント ピアからのルートは、すべてのクライアントにアドバタイズされます。
- クライアントからのルートは、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されます。したがって、そのクライアントは完全メッシュ化されている必要はありません。

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。

ルート リフレクタ対応の BGP スピーカーとともに、ルート リフレクタの概念を理解しない 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。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することができます。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することができます。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。

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 リストのアトリビュートを表示します。

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ディセーブルにするには、**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 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、ルーティングがループするのを防ぐために次のようなメカニズムがあります。

- 送信元 ID は、任意で非遷移な BGP アトリビュートです。これは 4 バイトのアトリビュートで、ルート リフレクタにより作成されます。このアトリビュートは、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 リストは任意で非遷移な BGP アトリビュートです。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。このアトリビュートを使用して、ルート リフレクタは、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 バックするかを識別することができます。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** 句を使用し、アトリビュートの変更や、場合によってはルーティング ループの作成を行うことができます。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 **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 プレフィクスを他の Provider Edge（PE; プロバイダー エッジ）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 プレフィクスを反映できるルート リフレクタの設定については、「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例」（P.13）に例が示されています。VPLS オートディスカバリの詳細については、『*Cisco IOS MPLS Configuration Guide*』の「VPLS Autodiscovery:BGP Based」の章を参照してください。

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（この後 Cisco IOS 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。これらのタイマーを調整することができます。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
`Router(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
`Router(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上書きします。

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 アトリビュート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** ルータ コンフィギュレーション コマンドがイネーブルの場合、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 コマンドがイネーブルな場合は、すべてのパスは完全に比較可能で、**bgp deterministic med** コマンドがイネーブル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。

ルート ダンプニングの設定

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 という 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てみます。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。すると、自律システム 2 の境界ルータは、自律システム 3 に取り消しメッセージを伝播します。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。

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。再び、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。ペナルティは累積します。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。そのため、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。

ルート ダンプニングの用語の概要

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最良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。ペナルティの減少プロセスは、5 秒ごとに行われます。
- 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。ルートの抑制解除プロセスは 10 秒ごとに発生します。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。

ルート ダンプニングのイネーブル

BGP ルート ダンプニングをイネーブルにするには、次のコマンドをアドレス ファミリまたはルータ 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 dampening`	BGP ルート ダンプニングをイネーブルにします。

さまざまなダンプニング要素のデフォルト値を変更するには、次のコマンドをアドレス ファミリ モードまたはルータ 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 dampening` *half-life reuse suppress max-suppress* [`route-map` *map-name*]	ルート ダンプニング要素のデフォルト値を変更します。

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 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 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 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 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 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。
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 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 dampening** [*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。

内部 BGP 機能の設定例

内部 BGP 機能の設定例は次のとおりです。

- 「ルート マップのある BGP コンフェデレーションの設定例」（P.11）
- 「BGP コンフェデレーションの例」（P.12）
- 「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例」（P.13）

ルート マップのある BGP コンフェデレーションの設定例

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の他の設定例については、この章の「BGP コンフェデレーションの例」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 アトリビュート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 community アトリビュートがそのルートをフィルタ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 アトリビュート値を持っています。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 外部の BGP スピーカーによるこれらのルートのアドバタイズメントを自動的に防ぎます。

```
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
!
```

BGP コンフェデレーションの例

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。この自律システムを複数の自律システムに内部分割することは、コンフェデレーション外部のピアには知らされていません。

```
router bgp 701
 neighbor 172.16.232.56 remote-as 500
 neighbor 10.200.200.205 remote-as 701
```

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例

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、次の **address-family l2vpn vpls** 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
!
```

参考資料

ここでは、内部 BGP 機能の設定に関連する参考資料について説明します。

関連資料

関連項目	参照先
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP の概要	『*Cisco BGP Overview*』
基本的な BGP 設定作業	『*Configuring a Basic BGP Network*』

関連項目	参照先
サービス プロバイダーへの接続	『*Connecting to a Service Provider Using External BGP*』
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	『Configuring IP Routing Protocol-Independent Features』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

内部 BGP 機能設定用の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 12.2(1)、12.0(3)S、12.2(27)SBC、12.2(33)SRB、12.2(33)SXH、またはそれ以降のリリースで追加または変更された機能だけが表に示されています。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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(32)S12 12.0(7)T 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 dampened-paths** • **show ip bgp flap-statistics** • **timers bgp**
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	12.2(33)SRE	この機能は Cisco 7600 および Cisco 7200 シリーズのルータで追加されました。この機能は次のセクションに記載されています。 • 「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」（P.7） • 「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例」（P.13）

BGP の拡張機能の設定

このモジュールでは、さまざまな拡張 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）機能を設定するための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。このモジュールには、BGP ネクストホップ アドレス トラッキング、BGP グレースフル リスタート機能を使用した BGP NonStop Forwarding（NSF; ノンストップ フォワーディング）認識、ルート ダンプニング、BGP に対する Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）サポート、Multi-Topology Routing（MTR）に対する BGP Management Information Base（MIB; 管理情報ベース）サポートと BGP サポートを設定する作業が含まれています。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP の拡張機能を設定するための機能情報」（P.61）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

BGP の拡張機能を設定するための前提条件

BGP の拡張機能を設定する前に、「Cisco BGP Overview」モジュールと「Configuring a Basic BGP Network」モジュールについて十分に理解しておく必要があります。

BGP の拡張機能を設定するための制約事項

- 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。
- マルチキャスト BGP ピアのサポートは、リリース 12.2(33)SRA よりも後の Cisco IOS ソフトウェアでは使用できません。

BGP の拡張機能の設定に関する情報

このモジュールで BGP 機能を設定するには、次の概念を理解しておく必要があります。

- 「BGP バージョン 4」（P.2）
- 「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」（P.3）
- 「BGP ノンストップ フォワーディング認識」（P.4）
- 「BGP ルート ダンプニング」（P.7）
- 「BGP 用の双方向フォワーディング検出（BFD）」（P.8）
- 「BGP MIB サポート」（P.8）
- 「MTR に対する BGP サポート」（P.10）

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 Cisco IOS ソフトウェア実装には、BGP が 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できるようにするマルチプロトコル拡張機能と、IP Version 4（IPv4; IP バージョン 4）、IP Version 6（IPv6; IP バージョン 6）、Virtual Private Networks Version 4（VPNv4; バーチャル プライベート ネットワーク バージョン 4）、および Connectionless Network Services（CLNS; コネクションレス型ネットワーク サービス）を含む複数のレイヤ 3 プロトコル アドレス ファミリが組み込まれています。基本的な BGP ネットワークの設定に関する詳細については、「Configuring a Basic BGP Network」モジュールを参照してください。

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、external BGP（eBGP; 外部 BGP）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、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。

BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）と呼ばれてはいますが、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。同一組織内の BGP ピアは、internal BGP（iBGP; 内部 BGP）ピアリング セッションによっ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。

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

BGP ネクストホップ アドレス トラッキングを設定するには、次の概念を理解しておく必要があります。

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 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、Routing Information Base（RIB; ルーティング情報ベース）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 サイクル間での最良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 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 最良パスを選択、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、Interior Gateway Protocol（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。

選択的 BGP ネクストホップ ルート フィルタリング

Cisco IOS Release 12.4(4)T、12.2(33)SRB、およびそれ以降のリリースでは、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 アトリビュートに適用されるプレフィクスの長さを設定できます。ルート マップは BGP 最良パスの計算中に使用され、BGP プレフィクスのネクストホップ アトリビュート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） **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 ノンストップ フォワーディング認識

BGP ノンストップ フォワーディング（NSF）認識を設定するには、次の概念を理解しておく必要があります。

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ルータ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。

このマニュアルでは、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。デバイスは、NSF サポートするよう設定されている場合は NSF 対応であると見なすため、NSF 認識または NSF 対応のネイバーからルーティング情報を再作成します。

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 FIB 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。その後、CEF は、新しい FIB 情報でラインカードを更新します。

（注） 現在、EIGRP では NSF 認識だけがサポートされます。EIGRP に対する Stateful Switchover（SSO; ステートフル スイッチオーバー）サポートは、将来のリリースに統合されます。

NSF のシスコ エクスプレス フォワーディング

NSF の主要な要素はパケットの転送です。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。この機能によって、スイッチオーバー中のトラフィックの中断が軽減されます。

通常の NSF 操作中に、アクティブな Route Processor（RP; ルート プロセッサ）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が、リフレッシュされていることを示す新しいバージョン（「エポック」）番号を受信します。ラインカードや転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIB が収束すると、RP が信号通知を行います。ソフトウェアが、現在のスイッチオーバー エポックよりも古いエポックを持つすべての FIB と隣接エントリを削除します。これで、FIB は最新のルーティング プロトコル転送情報となります。

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。スイッチオーバー後に、ルーティング プロトコルは、ルーティング テーブルを再作成するのに役立つように、NSF 認識ネイバー デバイスがステート情報を送信することを要求します。

（注） NSF 操作の場合、ルーティング プロトコルがルーティング情報を再作成している間、ルーティング プロトコルは CEF に依存してパケットの転送を続行します。

NSF のための BGP グレースフル リスタート

NSF 対応のルータは、BGP ピアと BGP セッションを開始すると、OPEN メッセージをピアに送信します。メッセージには、NSF 対応ルータまたは NSF 認識ルータに「グレースフル リスタート機能」があることを示す宣言が含まれています。グレースフル リスタートとは、スイッチオーバー後に BGP ルーティング ピアでルーティング フラップが発生しないようにするためのメカニズムです。BGP ピアがこの機能を受信すると、メッセージを送信しているデバイスが NSF 対応であることを認識します。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、このセッションでグレースフル リスタートを行うことはできません。

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中に、再起動したときに NSF 対応ルータ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 ピア間で交換されています。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 メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応デバイスとの BGP セッションは確立されます。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

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イネーブルにするには、**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 Interior Gateway Protocol 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 認識は自動的にイネーブルにされないため、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。

ネイバーごとの BGP グレースフル リスタート

Cisco IOS Release 12.2(33)SRC、（Cisco 10000 シリーズ ルータを備えたプラットフォーム上の）12.2(33)SB、15.0(1)M、およびそれ以降のリリースで、個別の BGP ネイバーごとに 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イネーブルまたはディセーブルにできます。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** コマンドを使用した場合だけ使用可能ですが、**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配置で最適な値です。これらの値を調整するのは、経験を積んだネットワーク オペレータだけにしてください。

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 という 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てみます。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 に伝搬します。ネットワーク A へのルートが再度表示されると、自律システム 1 はアドバタイズメント メッセージを自律システム 2 に送信し、自律システム 2 がそのメッセージを自律システム 3 に送信します。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。

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。再び、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。ペナルティは累積します。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。そのため、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。

ルート ダンプニングの用語の概要

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最良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。ペナルティの減少プロセスは、5 秒ごとに行われます。
- 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。ルートの抑制解除プロセスは 10 秒ごとに発生します。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 用の双方向フォワーディング検出（BFD）

BGP に対する双方向フォワーディング検出（BFD）サポートが、Cisco IOS リリース 12.0(31)S、12.4(4)T、12.0(32)S、12.2(33)SRA、12.2(33)SXH、12.2(33)SB、およびそれ以降のリリースで導入されました。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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。

BFD については警告が 1 つ存在します。BGP が実行されているルータでは、BFD と BGP のグレースフル リスタート機能は両方とも設定できません。インターフェイスがダウンすると、BFD は障害を検出し、トラフィック転送にインターフェイスを使用できないこと、および BGP セッションがダウンしたことを示します。ただし、BGP セッションがダウンしている場合でも、グレースフル リスタートによって、NSF をサポートするプラットフォームでのトラフィック転送が引き続き可能であり、ダウンしているインターフェイスを使用してトラフィックを転送できます。BGP が実行されているルータで NSF 用の 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。

BFD の詳細については、『Bidirectional Forwarding Detection』コンフィギュレーション ガイドを参照してください。

BGP MIB サポート

BGP をサポートするための管理情報ベース（MIB）は CISCO-BGP4-MIB です。Cisco IOS Release 12.0(26)S、12.3(7)T、12.2(25)S、12.2(33)SRA、12.2(33)SXH、およびそれ以降のリリースでは、BGP MIB サポート拡張機能によって、新しい Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知用に CISCO-BGP4-MIB のサポートが導入されました。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」（P.9）
- 「BGP ルートが受信したルートのサポート」（P.9）

BGP FSM 遷移変更のサポート

cbgpRouteTable では、BGP Finite State Machine（FSM; 有限状態マシン）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、トラップを個別にイネーブルにするか、既存の FSM 後方移行と、RFC 1657 で定義されている設定済みの状態トラップと一緒にイネーブルにすることができます。

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、プレフィクス、およびプレフィ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*

MTR に対する BGP サポート

MTR に対する BGP サポートが Cisco IOS Release 12.2(33)SRB で導入されました。詳細については、マニュアル『Multi-Topology Routing』を参照してください。MTR をサポートするために BGP を使用する前に、次の概念について十分に理解しておく必要があります。

BGP ネットワーク スコープ

新しい設定階層である、名前付きスコープが BGP プロトコルに導入されました。BGP 用の MTR 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 モードなどのいくつか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。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 モードが開始され、このコマンドの入力時にルーティング テーブルのコレクションが作成されます。スコープ階層下で設定された BGP コマンドは、単一のネットワーク用に（グローバルに）設定されるか VRF 単位で設定され、スコープ コマンドと呼ばれます。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

BGP CLI は、事前 MTR BGP 設定の下位互換性を提供し、MTR の階層実装を提供するために変更されています。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 ファミリ設定と事前 MTR 設定の 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 ファミリとトポロジ設定では、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 モードで使用するように一般的なセッション コマンドとピア テンプレートを設定できます。

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 VRF 用に定義します。アドレス ファミリ コンフィギュレーション モードを開始するには、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** コマンドを設定します。Subaddress-Family Identifier（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。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 モードを開始すると、BGP は事前 MTR ベースの CLI を使用するよう設定されます。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、ルータは、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。

BGP トポロジ コンフィギュレーション モードを開始するには、アドレス ファミリ コンフィギュレーション モードで **topology**（BGP）コマンドを設定します。1 つのルータで 32 個までのトポロジ（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。

次に、MTR 実装用の BGP の設定時に使用される階層レベルを示します。

```
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

MTR は、セッション単位で 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最良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 RIB と 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、隣接ルータのクラス固有のトポロジ内にある 1 つのルータにクラス固有のトポロジから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。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** コマンドは、ネイバーの IP アドレスとトポロジ ID を使用して設定されます。

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 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最良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 最良パスの計算動作ごとに、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

BGP を使用したトポロジのインポート機能はトポロジ変換と似ています。違いは、ルートが BGP を使用して同一ルータ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** コマンドを入力します。クラス固有のトポロジまたは基本トポロジの名前は、このコマンドの入力時に指定されます。最良パスの計算は、インポート済みのルートがトポロジの 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リングできるようにする **route-map** キーワードも含まれています。

BGP の拡張機能の設定方法

ここでは、次の作業グループについて説明します。

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 Interior Gateway Protocol（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」（P.35）を参照してください。

BGP ネクストホップ アドレス トラッキングのディセーブル化

この作業は、BGP ネクストホップ アドレス トラッキングをディセーブル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イネーブルになっています。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 トラッキングをディセーブルにすると役に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イネーブルにするには、**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**]]
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：** `Router> enable`	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。
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 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。

	コマンドまたはアクション	目的
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 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：** `Router(config-router-af)# no bgp nexthop trigger enable`	BGP ネクストホップ アドレス トラッキングをディセーブルにします。 • 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イネーブルになっています。 • この例では、ネクストホップ アドレス トラッキングをディセーブルにします。
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。

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。

Interior Gateway Protocol と一致するような遅延間隔の調整

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、Interior Gateway Protocol（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。

アグレッシブ IGP ルート ダンプニング

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 Interior Gateway Protocol（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. **no 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：** `Router> enable`	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。
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 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：** `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。 • 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：** `Router(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。 • 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：** `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 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。

bgp nexthop コマンドの使用方法のその他の例については、「BGP 選択的ネクストホップ ルート フィルタリングの設定：例」（P.50）を参照してください。

BGP Next_Hop アトリビュート

Next_Hop アトリビュートは、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 アトリビュートは変更されません。

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。

制約事項

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. **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：** `Router> enable`	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。
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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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：** `Router(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：** `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 7	**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 8	**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 FILTER25 seq 5 permit 0.0.0.0/0 le 25`	BGP ネクストホップ ルート フィルタリングのプレフィクス 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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 10	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] **例：** `Router(config-route-map)# match ip address prefix-list FILTER25`	指定されたプレフィクス 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、この作業に適用される構文だけが使用されます。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 11	**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 12	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(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。
ステップ 13	**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 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。 • 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、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

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 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 リスタートをイネーブルまたはディセーブル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」（P.19）
- 「BGP NSF 認識タイマーの設定」（P.21）
- 「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」（P.22）
- 「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」（P.28）
- 「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」（P.31）
- 「BGP ノンストップ フォワーディング認識の設定の確認」（P.33）

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イネーブルにします。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配置で最適な値です。これらの値を調整するのは、経験を積んだネットワーク オペレータだけにしてください。

制約事項

BGP が実行されているルータで NSF 用の 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。詳細については、「BGP 用の双方向フォワーディング検出（BFD）」（P.8）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. **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：** `Router> enable`	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。
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	**bgp graceful-restart** [**restart-time** *seconds*] [**stalepath-time** *seconds*] **例：** `Router(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：** `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。

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 および BGP 接続に関する情報を表示します。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、「Configuring a Basic BGP Network」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。

BGP グレースフル リスタート タイマー

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配置で最適な値です。これらの値を調整するのは、経験を積んだネットワーク オペレータだけにしてください。

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：** `Router> enable`	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。
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。

	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：** `Router(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。設定可能な値の範囲は 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：** `Router(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。設定可能な値の範囲は 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	`Router(config-router)# 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。

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、「Configuring a Basic BGP Network」モジュールを参照してください。

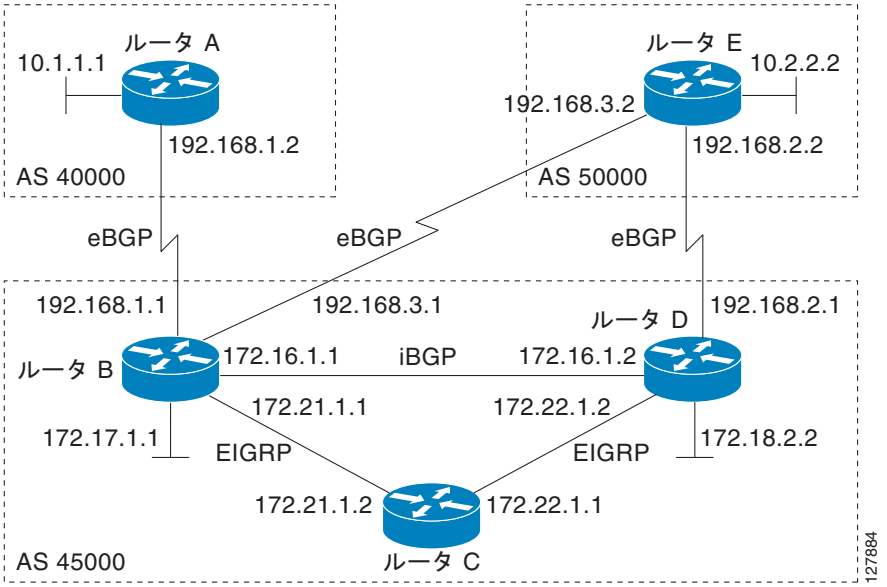
BGP ピア セッション テンプレートを使用した BGP グレースフル リスタートのイネーブル化とディセーブル化

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、図 1 のルータ B で設定が実行され、図 1 のルータ A とルータ E にある 2 つの外部 BGP ネイバーが識別されます。ルータ A にある最初の BGP ピアは、BGP グレースフル リスタートをイネーブルにする最初のピア 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 リスタートをディセーブルにする 2 番目のテンプレートを継承します。任意の **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 1　　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、「BGP NSF 認識タイマーの設定」（P.21）に示すように、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。

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 テンプレートの詳細については、「Configuring a Basic BGP Network」モジュールを参照してください。

前提条件

この作業では、Cisco IOS Release 12.2(33)SRC または 12.2(33)SB が必要です。

制約事項

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-name*
13. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
14. **neighbor** *ip-address* **inherit peer-session** *session-template-name*
15. **end**
16. **show ip bgp template peer-session** [*session-template-name*]
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：** `Router> enable`	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。
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-session** *session-template-name* **例：** `Router(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：** `Router(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 リスタート機能をディセーブルにするには、**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。
ステップ 6	**exit-peer-session** **例：** `Router(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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 8	**ha-mode graceful-restart** [**disable**] **例：** `Router(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 リスタート機能をディセーブルにするには、**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：** `Router(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：** `Router(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。予期しないネイバーのリセットは、ネットワークでのエラー率が高いことまたはパケット損失が高いことを示す場合があり、調査する必要があります。
ステップ 11	**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、192.168.1.2 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（ステップ 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：** `Router(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：** `Router(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（ステップ 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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 15	**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 16	**show ip bgp template peer-session** [*session-template-number*] **例：** `Router# 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。
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：** `Router# 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（図 1 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、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。

```
Router# 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（図 1 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。

```
Router# 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
```

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

図 1 のピア C にある内部 BGP ピアで BGP グレースフル リスタートをイネーブルにするには、図 1 のルータ B でこの作業を実行します。アドレス ファミリ IPv4 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 リスタートがイネーブルにされます。BGP グレースフル リスタートがイネーブルになっていることを確認するには、任意の **show ip bgp neighbors** コマンドを使用します。

前提条件

この作業では、Cisco IOS Release 12.2(33)SRC、12.2(33)SB、または 15.0(1)M が必要です。

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：** `Router> enable`	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。
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	**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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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：** `Router(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（ステップ 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：** `Router(config-router-af)# neighbor 172.21.1.2 activate`	ネイバーが IPv4 アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。 • 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。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** *ip-address* **ha-mode graceful-restart** [**disable**] **例：** `Router(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 リスタート機能をディセーブルにするには、**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：** `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 9	**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 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。

```
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
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、図 1 のルータ D にある BGP ネイバーである 172.16.1.2 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 リスタートはディセーブルにされます。

前提条件

この作業では、Cisco IOS Release 12.2(33)SRC、12.2(33)SB、または 15.0(1)M が必要です。

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：** `Router> enable`	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。
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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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：** `Router(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：** `Router(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：** `Router(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 リスタート機能をディセーブルにするには、**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、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：** `Router(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。

	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`	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：** `Router# 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リングされ、「Graceful-Restart is disabled」行には、このネイバーのグレースフル リスタート機能がディセーブルに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。

```
Router# 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
```

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。

```
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。

```
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、図 1 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。

```
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 ルート ダンプニングの設定

このセクションの作業では、BGP ルート ダンプニングを設定およびモニタリングします。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ています。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 ルート ダンプニングのイネーブル化と設定」（P.35）
- 「BGP ルート ダンプニングのモニタリングとメンテナンス」（P.36）

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** *autonomous-system-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。
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。

	コマンドまたはアクション	目的
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 プレフィクスを指定します。 • **vrf** キーワードと *vrf-name* 引数は、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 ダンプニングをイネーブル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。
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とメンテナンス

BGP ルート ダンプニングをモニタリングして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 ip bgp flap-statistics** [**regexp** *regexp* | **filter-list** *access-list* | *ip-address mask* [**longer-prefix**]]
3. **clear ip bgp flap-statistics** [*neighbor-address* [*ipv4-mask*]] [**regexp** *regexp* | **filter-list** *extcom-number*]
4. **show ip bgp dampened-paths**
5. **clear ip bgp** [**ipv4** {**multicast** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast**] **dampening** [*neighbor-address*] [*ipv4-mask*]

手順の詳細

ステップ 1　enable

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。

```
Router> enable
```

ステップ 2 **show ip bgp flap-statistics** [**regexp** *regexp* | **filter-list** *access-list* | *ip-address mask* [**longer-prefix**]]

フラッピングが発生しているすべてのパスのフラップを監視するには、このコマンドを使用します。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。

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 172.17.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 10.0.0.0         172.17.232.177  4     00:13:31 00:18:10 100
*d 10.2.0.0         172.17.232.177  4     00:02:45 00:28:20 100
```

ステップ 3 **clear ip bgp flap-statistics** [*neighbor-address* [*ipv4-mask*]] [**regexp** *regexp* | **filter-list** *extcom-number*]

BGP ダンプニングがイネーブル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。引数またはキーワードが指定されていない場合は、すべてのルートのフラップ統計情報がクリアされます。フラップ統計情報は、半減期間中にピアが安定している場合にもクリアされます。BGP フラップ統計情報のクリア後に、ルート ダンプニングが発生する可能性は低くなります。

```
Router# clear ip bgp flap-statistics 172.17.232.177
```

ステップ 4 **show ip bgp dampened-paths**

フラッピングが発生しているすべてのパスのフラップを監視するには、このコマンドを使用します。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。

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse   Path
*d 10.0.0.0         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

ステップ 5 **clear ip bgp** [**ipv4** {**multicast** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4 unicast**] **dampening** [*neighbor-address*] [*ipv4-mask*]

格納されているルート ダンプニング情報をクリアするには、このコマンドを使用します。キーワードまたは引数を入力しないと、ルーティング テーブル全体のルート ダンプニング情報がクリアされます。次の例では、VPNv4 アドレス ファミリ プレフィクスのルート ダンプニング情報をネットワーク 192.168.10.0/24 からクリアし、抑制されているルートの抑制を解除します。

```
Router# clear ip bgp vpnv4 unicast dampening 192.168.10.0 255.255.255.0
```

BFD を使用した BGP コンバージェンス時間の短縮

BGP に対する BFD サポートが、Cisco IOS Release 12.0(31)S、12.4(4)T、12.2(33)SRA、12.2(33)SXH、12.2(33)SB、およびそれ以降のリリースで導入されました。BFD プロセスを開始するには、インターフェイスで BFD を設定します。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 プロトコルに対する BFD サポートの設定後に、隣接の作成が行われます。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。

- 「インターフェイスでの BFD セッション パラメータの設定」（P.38）
- 「BGP に対する BFD サポートの設定」（P.39）
- 「Cisco 7600 シリーズ ルータの BFD のモニタリングとトラブルシューティング」（P.40）

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。使用するルーティング 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、ご使用のバージョンの Cisco IOS ソフトウェアの IP ルーティング マニュアルを参照してください。

制約事項

- 現在シスコで採用している Cisco IOS Release 12.0(31)S、12.4(4)T、12.2(33)SRA、12.2(33)SXH、および 12.2(33)SB における BGP に対する BFD サポートでは、BFD は IPv4 ネットワークだけでサポートされ、非同期モードだけがサポートされます。非同期モードでは、いずれかの BFD ピアが BFD セッションを開始できます。
- BFD は、直接接続されたネイバーだけで機能します。BFD ネイバーは、1 つの IP ホップだけ離れている必要があります。マルチホップ設定はサポートされません。
- BGP が実行されているルータで NSF 用の 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。詳細については、「BGP 用の双方向フォワーディング検出（BFD）」（P.8）を参照してください。

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的な 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 ネイバーに対する 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。
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* **例：** `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	インターフェイスで BFD をイネーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

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。

前提条件

- BGP が、関与するすべてのルータで実行されている必要があります。
- BFD ネイバーに対する BFD セッションを実行するインターフェイスで BFD セッションの基本的な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」（P.38）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。
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 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`	フォ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。

Cisco 7600 シリーズ ルータの BFD のモニタリングとトラブルシューティング

Cisco 7600 シリーズ ルータで BFD をモニタまたはトラブルシューティングするには、ここでの手順を 1 つ以上実行します。

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。
ステップ 2	**show bfd neighbors** [**details**] **例：** `Router# show bfd neighbors details`	（任意）BFD 隣接データベースを表示します。 • **details** キーワードは、ネイバーごとの BFD プロトコル パラメータとタイマーをすべて表示されます。
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 パケットに関するデバッグ情報を表示します。

次の作業

別のルーティング プロトコルに対する BFD サポートの設定に関する詳細については、『Bidirectional Forwarding Detection』コンフィギュレーション ガイドを参照してください。

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：** `Router> enable`	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。
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	**snmp-server enable traps bgp** [[**state-changes** [**all**] [**backward-trans**] [**limited**]]	[**threshold prefix**]] **例：** `Router# 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 移行イベントに対するサポートをイネーブルにするために使用します。 • **all** キーワードは、FSM 移行イベントに対するサポートをイネーブルにします。 • **backward-trans** キーワードは、後方移行の状態変更イベントに対するサポートだけをイネーブルにします。 • **limited** キーワードは、後方移行の状態変更と設定された状態イベントに対するサポートをイネーブルにします。 • **threshold** キーワードと **prefix** キーワードは、指定されたピアで設定済みのプレフィクス最大制限に達した場合に通知をイネーブルにするために使用されます。
ステップ 4	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

MTR に対する BGP サポートの設定

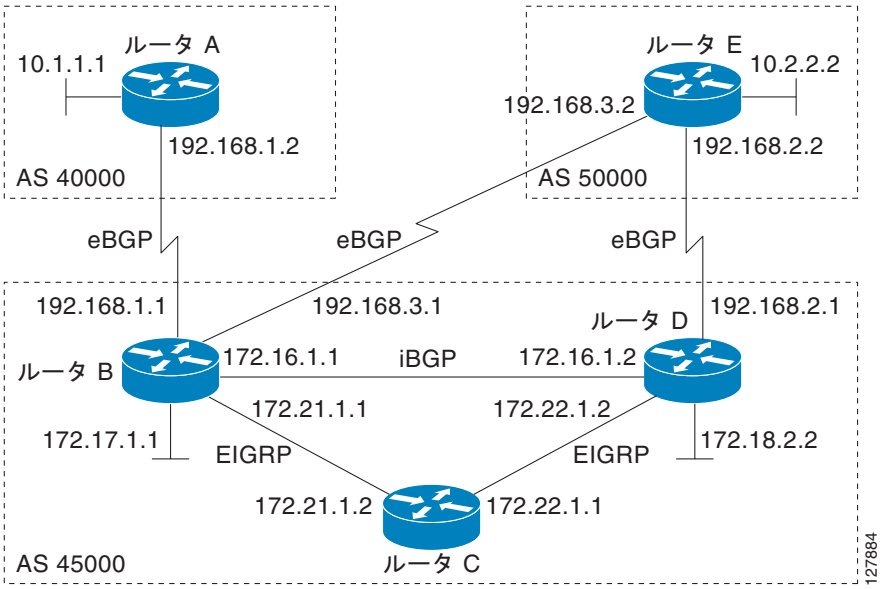
次の作業を実行する前に、設定済みの MTR トポロジが必要です。詳細については、Cisco IOS Release 12.2(33)SRB の「Multi-Topology Routing」機能を参照してください。

- 「BGP を使用した MTR トポロジのアクティブ化」（P.42）
- 「BGP を使用した MTR トポロジからのルートのインポート」（P.47）

BGP を使用した MTR トポロジのアクティブ化

この作業は、BGP を使用してアドレス ファミリ内で MTR トポロジをアクティブにする場合に実行します。図 2 のルータ B で設定するこの作業は、ルータ D とルータ 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、ネイバーはルータ スコープ コンフィギュレーション モードで設定されます。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 2　BGP ネットワーク ダイアグラム



BGP CLI は、事前 MTR BGP 設定の下位互換性を提供し、MTR の階層実装を提供するために変更されています。新しい設定階層である、名前付きスコープが BGP プロトコルに導入されました。BGP 用の MTR 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 モードなどのいくつか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。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 モードが開始され、このコマンドの入力時にルーティング テーブルのコレクションが作成されます。次に、MTR 実装用の BGP の設定時に使用される階層レベルを示します。

```
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
```

MTR をサポートするために BGP を使用する前に、「MTR に対する BGP サポート」（P.10）に記載されているすべての概念について十分に理解しておく必要があります。

前提条件

- MTR に対して設定されたすべてのルータで Cisco IOS Release 12.2(33)SRB またはそれ以降のリリースを実行している必要があります。
- グローバル MTR トポロジの設定が行われ、アクティブになっています。
- IP ルーティングと CEF がイネーブルになっています。

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。
- IPv4 アドレス ファミリ（マルチキャストとユニキャスト）だけがサポートされます。

- 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。

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-name***} **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。
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 4	**scope** {**global** | **vrf** *vrf-name*} **例：** `Router(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 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** キーワードと *vrf-name* 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：** `Router(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 ルータ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**} **例：** `Router(config-router-scope)# neighbor 172.16.1.2 transport multi-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。 • 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 Maximum Transmission Unit（MTU; 最大伝送ユニット）検出をイネーブルにするには、**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 ファミリが単一の TCP 転送セッションを使用することを指定するには、**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：** `Router(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 MDT アドレス プレフィ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、キーワード **unicast** 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。

	コマンドまたはアクション	目的
ステップ 8	**topology** {**base** | *topology-name*} **例：** `Router(config-router-scope-af)# topology VIDEO`	BGP がクラス固有トラフィックまたは基本トポロジ 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 9	**bgp tid** *number* **例：** `Router(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：** `Router(config-router-scope-af-topo)# neighbor 172.16.1.2 activate`	BGP ネイバーが、NSAP アドレス ファミリのプレフィクスをローカル 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 11	**neighbor** {*ip-address* | *peer-group-name*} **translate-topology** *number* **例：** `Router(config-router-scope-af-topo)# neighbor 172.16.1.2 translate-topology 200`	（任意）別のルータ上のトポロジからローカル ルータ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。 • ルータ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：** `Router(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：** `Router# 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：** `Router# 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。 **（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

次に、**show ip bgp topology** コマンドと VIDEO トポロジのサマリー出力の例を示します。

```
Router# 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 ルータでこの設定を繰り返します。同じルータ上のある 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、次の作業に進みます。

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ルータで設定されている場合に、同じルータ上のある 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クスを許可するためにプレフィクス リストが定義されます。このプレフィクス 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。

前提条件

- MTR に対して設定されたすべてのルータで Cisco IOS Release 12.2(33)SRB またはそれ以降のリリースを実行している必要があります。
- グローバル トポロジ設定が行われ、アクティブになっています。
- IP ルーティングと CEF がイネーブルになっています。

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 ループの発生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。
- IPv4 アドレス ファミリ（マルチキャストとユニキャスト）だけがサポートされます。
- 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。

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-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：** `Router> enable`	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。
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 TEN permit 10.2.2.0/24`	IP プレフィクス リストを設定します。 • この例では、プレフィクス 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：** `Router(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：** `Router(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、またはプレフィクス リストにより許可されているプレフィ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、プレフィクス リスト TEN によって許可されるプレフィ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：** `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 モードに戻ります。
ステップ 7	**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。

	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：** `Router(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 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** キーワードと *vrf-name* 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：** `Router(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：** `Router(config-router-scope-af)# topology VIDEO`	BGP がクラス固有トラフィックまたは基本トポロジ 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：** `Router(config-router-scope-af-topo)# import topology VOICE route-map 10NET`	（任意）同じルータ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リングするには、**route-map** キーワードを使用できます。
ステップ 12	**end** **例：** `Router(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。

BGP の拡張機能を設定するための設定例

ここでは、次の例について説明します。

BGP ネクストホップ アドレス トラッキングのイネーブル化とディセーブル化：例

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
```

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：例

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
```

BGP 選択的ネクストホップ ルート フィルタリングの設定：例

次に、BGP プレフィ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
```

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：例

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
```

ネイバーごとの 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：例

Cisco IOS Release 12.2(33)SRC、12.2(33)SB、および 15.0(1)M 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ました。次の例は、図 3 のルータ B で設定され、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 リスタート機能をイネーブルにして、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 リスタート機能をディセーブルにします。図 3 のルータ 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 リスタート機能はイネーブルになります。図 3 のルータ 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 リスタート機能がディセーブルにされた状態で設定されます。

図 3　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

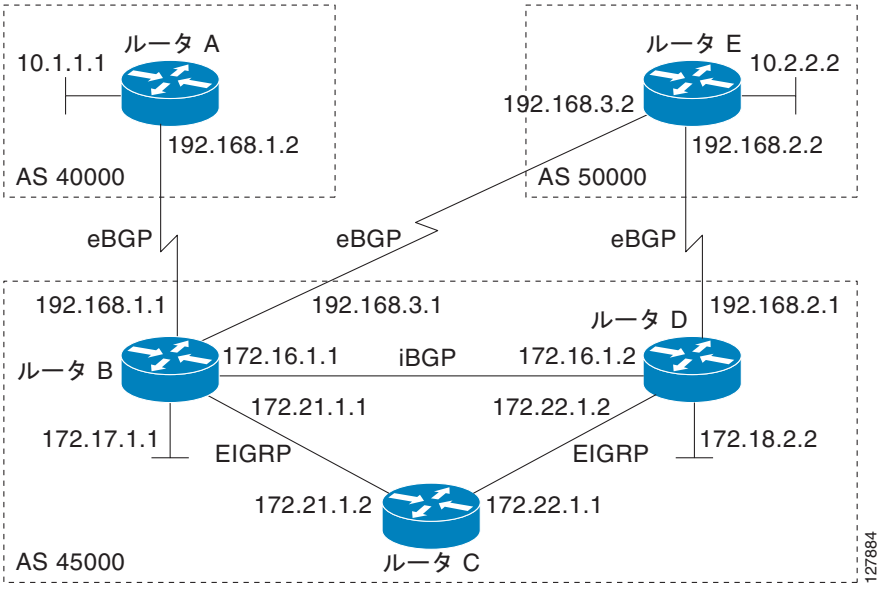


図 3 のルータ C にある個別の内部 BGP ネイバー 172.21.1.2 では BGP グレースフル リスタート機能はイネーブルになっているのに対して、図 3 のルータ D にある BGP ネイバー 172.16.1.2 では BGP グレースフル リスタートはディセーブルになっています。これは、ピア グループ PG1 のメンバであるためです。BGP グレースフル リスタートのディセーブル化は、ピア グループ PG1 のすべてのメンバについて設定されます。リスタート タイマーと失効パス タイマーは変更され、BGP セッションがリセットされます。

```
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。図 3 のルータ A にある個別の外部 BGP ネイバー 192.168.1.2 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 リスタート機能はディセーブルにされます。

```
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 *
```

BGP ルート ダンプニングの設定：例

次の例では、ACCOUNTING という名前のルート マップを使用してフィルタリングされたプレフィクスに適用される BGP ダンプニングを設定します。

```
ip prefix-list FINANCE permit 10.0.0.0/8
!
route-map ACCOUNTING
 match ip address ip prefix-list FINANCE
 exit
router bgp 50000
 address-family ipv4
 bgp dampening route-map ACCOUNTING
 end
```

BGP ネットワークでの BFD の設定：例

次の例では、単純な BGP ネットワークはルータ A とルータ B で構成されます。ルータ A 上のファスト イーサネット インターフェイス 0/1 は、ルータ B のファスト イーサネット インターフェイス 6/0 と同じネットワークに接続されています。グローバル コンフィギュレーション モードで開始されるこの例は、BFD の設定を示しています。

ルータ A の設定

```
!
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
!
router bgp 40000
 bgp log-neighbor-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
 !
 address-family ipv4
 neighbor 172.16.10.2 activate
 no auto-summary
 no synchronization
 network 172.18.0.0 mask 255.255.255.0
```

```
 exit-address-family
!
```

ルータ B の設定

```
!
interface FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router bgp 45000
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 40000
 neighbor 172.16.10.1 fall-over bfd
 !
 address-family ipv4
 neighbor 172.16.10.1 activate
 no auto-summary
 no synchronization
 network 172.17.0.0 mask 255.255.255.0
 exit-address-family
!
```

ルータ A での **show bfd neighbors details** コマンドの出力は、BFD セッションが作成されたこと、および BFD サポート用の BGP が登録されていることを確認します。関連するコマンド出力は、出力では太字で示されます。

ルータ A

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   332  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(15491)
Rx Count: 9160, Rx Interval (ms) min/max/avg: 200/440/332 last: 268 ms ago
Tx Count: 15494, Tx Interval (ms) min/max/avg: 152/248/197 last: 32 ms ago
Registered protocols: BGP
Uptime: 00:50:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

ルータ B にあるラインカードの **show bfd neighbors details** コマンドの出力は、BFD セッションが作成されたことを確認します。

（注） ルータ B は Cisco 12000 シリーズ ルータです。**show bfd neighbors details** コマンドはラインカードで実行する必要があります。**show bfd neighbors details** コマンドは、ラインカードで入力したときに登録済みのプロトコルを表示しません。

ルータ B

```
RouterB# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session

Press RETURN to get started!

LC-Slot6> show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

show ip bgp neighbors コマンドの出力は、BGP ネイバーの BFD がイネーブルになっていることを確認します。

ルータ A

```
RouterA# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
 Using BFD to detect fast fallover
.
.
.
```

ルータ B

```
RouterB# show ip bgp neighbors

BGP neighbor is 172.16.10.1,  remote AS 40000, external link
 Using BFD to detect fast fallover
.
.
.
```

BGP MIB サポートのイネーブル化：例

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。

```
Router(config)# snmp-server enable traps bgp
```

次の検証例は、BGP に対する SNMP サポートがイネーブルになっていて、running-config ファイルが表示されることを示します。

```
Router# show run | include snmp-server

snmp-server enable traps bgp
```

BGP を使用した MTR トポロジのアクティブ化：例

ここでは、次の設定例について説明します。

- 「BGP トポロジ変換設定」（P.56）
- 「BGP スコープのグローバルと VRF 設定」（P.56）
- 「BGP トポロジの検証」（P.57）

BGP トポロジ変換設定

次の例では、VIDEO トポロジで BGP を設定し、192.168.2.2 ネイバーでのトポロジ変換を設定します。

```
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
```

BGP スコープのグローバルと VRF 設定

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 VRF 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
```

BGP トポロジの検証

次に、**show ip bgp topology** コマンドのサマリー出力の例を示します。VIDEO という名前の MTR トポロジを使用するよう設定された BGP ネイバーに関する情報が表示されます。

```
Router# 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。

```
Router# show ip bgp topology VIDEO neighbors 172.16.12

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
.
.
.
```

BGP を使用した MTR トポロジからのルートのインポート：例

次に、BLUE という名前のルート マップが VOICE という名前の 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 BLUE
     end
clear ip bgp topology VIDEO 50000
```

次の作業

- 外部サービス プロバイダーに接続して、他の外部 BGP 機能を使用するには、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。
- 一部の内部 BGP 機能を設定するには、『*Cisco IOS IP Routing Protocols Configuration Guide*』の BGP セクションで、「Configuring Internal BGP Features」の章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を設定するには、「Configuring BGP Neighbor Session Options」モジュールを参照してください。

参考資料

ここでは、BGP の拡張機能の設定に関連する参考資料について説明します。

関連資料

関連項目	参照先
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 IOS IP Routing Protocols Configuration Guide*』の「Cisco BGP Overview」モジュール

関連項目	参照先
BGP の基本作業のコンセプトと設定の詳細。	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring a Basic BGP Network」モジュール
SNMP 操作と SNMP 操作に関する情報	『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」

規格

規格	タイトル
MDT SAFI	*MDT SAFI*

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 1657	『*Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*』
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 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 4724	『*Graceful Restart Mechanism for BGP*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

BGP の拡張機能を設定するための機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 12.2(1)、12.0(3)S、12.2(33)SRA、12.2(33)SXH、12.2(33)SB、またはそれ以降のリリースで導入または変更された機能だけが表に示されています。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　BGP の拡張機能を設定するための機能情報

機能名	リリース	機能の設定情報
ネイバーごとの BGP グレースフル リスタート	12.2(33)SRC 12.2(33)SB 15.0(1)M 15.0(1)S Cisco IOS XE 3.1.0SG	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。 Cisco IOS Release 12.2(33)SB では、プラットフォーム サポートには Cisco 10000 シリーズ ルータが組み込まれています。 次のセクションで、この機能に関する情報を参照できます。 • 「ネイバーごとの BGP グレースフル リスタート」（P.6） • 「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」（P.22） • 「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」（P.28） • 「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」（P.31） • 「ネイバーごとの 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：例」（P.51） この機能によって、**ha-mode graceful-restart**、**neighbor ha-mode graceful-restart**、**show ip bgp neighbors** の各コマンドが導入または変更されました。
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(33)SXH	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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP MIB サポート」（P.8） • 「BGP MIB サポートのイネーブル化」（P.41） • 「BGP MIB サポートのイネーブル化：例」（P.56） この機能では、**snmp-server enable traps bgp** コマンドが導入されました。

表 1　BGP の拡張機能を設定するための機能情報 （続き）

機能名	リリース	機能の設定情報
BGP ノンストップ フォワーディング（NSF）認識	12.2(15)T 15.0(1)S	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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ノンストップ フォワーディング認識」（P.4） • 「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」（P.19） • 「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：例」（P.51） • 「ネイバーごとの 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：例」（P.51） • 「BGP ルート ダンプニングの設定：例」（P.53） この機能によって、**bgp graceful-restart**、**show ip bgp**、**show ip bgp neighbors** の各コマンドが導入または変更されました。
BGP の選択的アドレス トラッキング	12.4(4)T 12.2(33)SRB	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。 次のセクションで、この機能に関する情報を参照できます。 • 「選択的 BGP ネクストホップ ルート フィルタリング」（P.3） • 「BGP 選択的ネクストホップ ルート フィルタリングの設定」（P.15） • 「BGP 選択的ネクストホップ ルート フィルタリングの設定：例」（P.50） この機能によって、**bgp nexthop** コマンドおよび **neighbor fall-over** コマンドが変更されました。

表 1　BGP の拡張機能を設定するための機能情報 （続き）

機能名	リリース	機能の設定情報
BFD に対する BGP サポート	12.0(31)S 12.4(4)T 12.2(33)SRA 12.2(33)SXH 12.2(33)SB 15.0(1)S	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。高速な転送パス障害検出に加えて、BFD は、ネットワーク管理者向けの一貫性のある障害検出方式を備えています。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。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 用の双方向フォワーディング検出（BFD）」（P.8） • 「BFD を使用した BGP コンバージェンス時間の短縮」（P.37） • 「BGP ネットワークでの BFD の設定：例」（P.53） この機能によって、**bfd**、**neighbor fall-over**、**show bfd neighbors**、**show ip bgp neighbors** の各コマンドが導入または変更されました。

表 1　BGP の拡張機能を設定するための機能情報 （続き）

機能名	リリース	機能の設定情報
MTR に対する BGP サポート	12.2(33)SRB	Multi-Topology Routing（MTR）に対する BGP サポートによって、MTR トポロジをサポートするために新しい設定階層とコマンドライン インターフェイス（CLI）コマンドが導入されました。新しい設定階層、つまりスコープは、MTR とは関係なく BGP によって実装できます。MTR によって、クラスベースの転送によるサービスの区別化を設定できます。MTR では、複数のユニキャスト トポロジと別個のマルチキャスト トポロジがサポートされます。トポロジは、一連の独立した Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）によって特徴付けられる、基礎となるネットワーク（または基本トポロジ）のサブセットです。 12.2(33)SRB では、この機能は Cisco 7600 で導入されました。 次のセクションで、この機能に関する情報を参照できます。 • 「MTR に対する BGP サポート」（P.10） • 「MTR に対する BGP サポートの設定」（P.42） • 「BGP を使用した MTR トポロジのアクティブ化：例」（P.56） • 「BGP を使用した MTR トポロジからのルートのインポート：例」（P.58） この機能によって、**address-family ipv4 (BGP)**、**bgp tid**、**clear ip bgp topology**、**import topology**、**neighbor translate-topology**、**neighbor transport**、**scope**、**show ip bgp topology**、**topology (BGP)** の各コマンドが導入または変更されました。

表 1　BGP の拡張機能を設定するための機能情報 （続き）

機能名	リリース	機能の設定情報
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	12.0(29)S 12.3(14)T 12.2(33)SXH 15.0(1)S	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、ルーティング情報ベース（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 サイクル間での最良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。 次のセクションで、この機能に関する情報を参照できます。 • 「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」（P.3） • 「BGP ネクストホップ アドレス トラッキングの設定」（P.13） • 「BGP ネクストホップ アドレス トラッキングのイネーブル化とディセーブル化：例」（P.50） • 「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：例」（P.50） この機能では、**bgp nexthop** コマンドが導入されました。

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、Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）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 Multiprotocol BGP（MP-BGP; マルチプロトコル BGP）サポートを設定する作業について説明します。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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 Open System Interconnection（OSI; 開放型システム間相互接続）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。

このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「CLNS に対する MP-BGP サポートの設定に関する機能情報」（P.36）を参照してください。

プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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、この機能でサポートされません。

次の BGP コマンドは、この機能でサポートされません。

- **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

CLNS に対する MP-BGP サポートを設定するには、次の概念について理解する必要があります。

- 「CLNS に対する MP-BGP サポートの設計機能」（P.2）
- 「汎用 BGP CLNS ネットワーク トポロジ」（P.3）
- 「DCN ネットワーク トポロジ」（P.4）
- 「CLNS に対する MP-BGP サポートの利点」（P.6）

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、コネクションレス型ネットワーク サービス（CLNS）をネットワーク レイヤ 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、ボーダー ゲートウェイ プロトコル（BGP）を使用できるようになります。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 Data Communications Network（DCN; データ通信ネットワーク）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」（P.4）を参照してください。

BGP は、Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）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手法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。

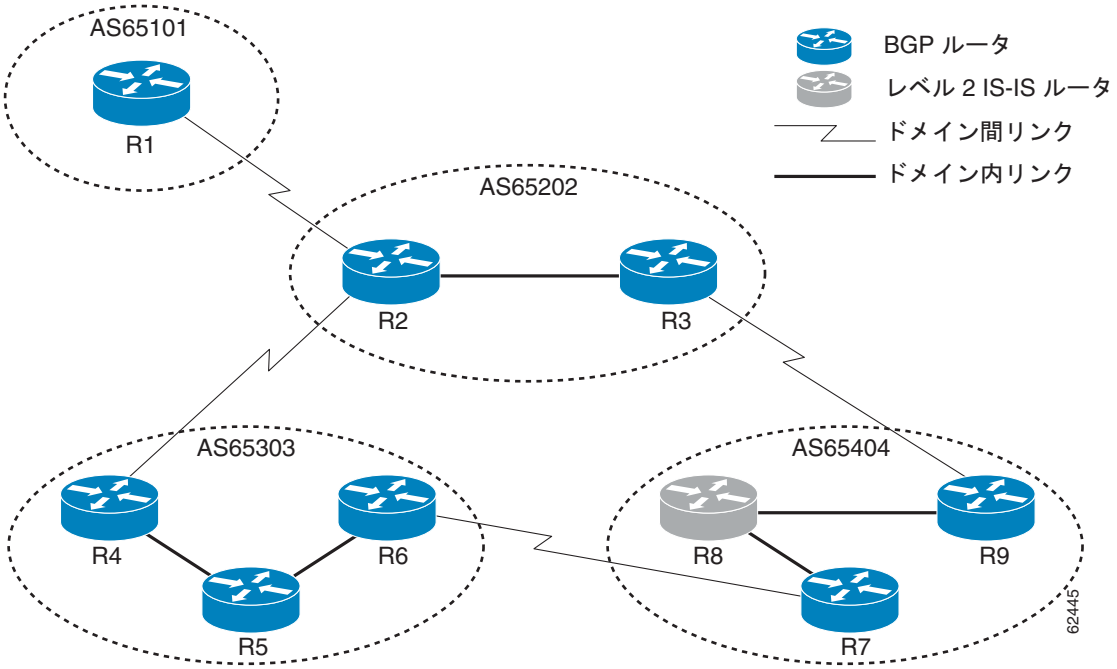
CLNS は Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスを使用して、そのすべてのネットワーク要素を識別します。BGP アドレス ファミリ サポートにより、NSAP アドレス プレフィクスは BGP を使用して転送できます。CLNS では、BGP プレフィクスが CLNS レベル 2 プレフィクス テーブルに挿入されます。この機能を使用すると、BGP をドメイン間ルーティング プロトコルとして個別の CLNS ルーティング ドメイン間で使用できます。

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

図 1 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、このマニュアルでは 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 1　　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。図 1 (P.3) 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。

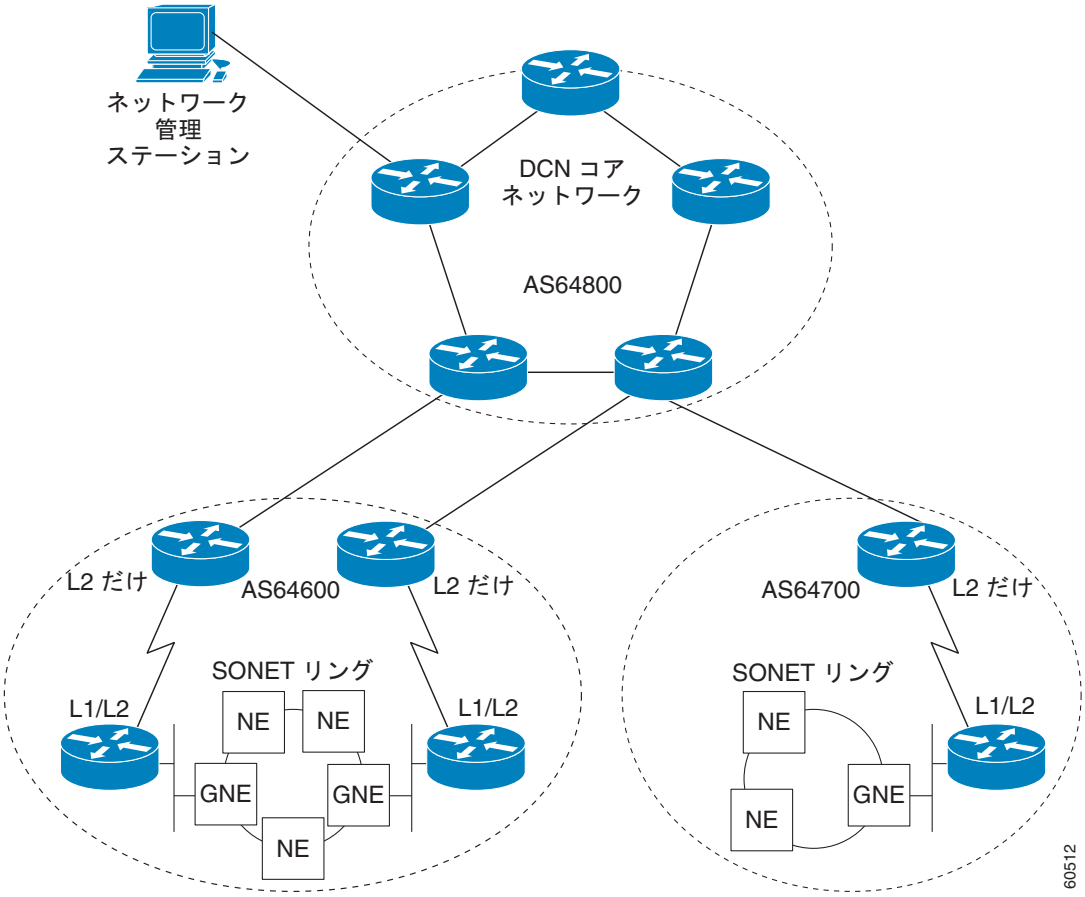
このマニュアルでの設定作業および設定例は、図 1（P.3）に示される総称ネットワーク設計に基づいています。図 1 のすべてのルータの設定は、「CLNS に対する MP-BGP サポートの実装：例」（P.30）に示されます。

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 リングを管理するデータ通信ネットワーク（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。

図 2 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。図 2 の NE で示される、SONET リングのネットワーク要素は、File Transfer, Access, and Management（FTAM）および Common Management Information Protocol（CMIP; 共通管理情報プロトコル）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 レイヤ 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 2　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、Intermediate System（IS; 中継システム）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 コアに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 ネットワーク要素によって表され、図 2 では GNE です。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 Central Office（CO; セントラル オフィス）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、Data Communications Channel（DCC; データ通信チャネル）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

ここでは、次の手順について説明します。特定のネットワークの場合、各手順を通して進める必要がない場合があります。必要な手順のステップを実行する必要がありますが、他のすべての手順は、ご使用のネットワークでの必要性に応じて実行します。

- 「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」（P.7）（必須）
- 「IS-IS ルーティング プロセスの設定」（P.9）（必須）
- 「BGP ネイバーに接続するインターフェイスの設定」（P.10）（必須）
- 「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」（P.11）（必須）

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。

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** コマンドの下に入力されたコマンドが 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ディセーブルにするために、ルータで設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **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。
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ディセーブルにします。
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 プレフィクスを指定します。デフォルトでは、**address-family nsap** コマンドで **unicast** キーワードが指定されない場合、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	**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。
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* 引数は、ルーティング プロセスの意味のある名前です。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。

	コマンドまたはアクション	目的
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。 • 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。
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`	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。
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 ethernet 0/1`	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)# clns router isis osi-as-202`	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。
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 プレフィクスのアドバタイジング

NSAP アドレス プレフィクスをアドバタイジングすると、プレフィクスが 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。
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ディセーブルにします。
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 プレフィクスを指定します。デフォルトでは、**address-family nsap** コマンドで **unicast** キーワードが指定されない場合、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。

	コマンドまたはアクション	目的
ステップ 7	**network** *nsap-prefix* [**route-map** *map-tag*] **例：** `Router(config-router-af)# network 49.0101.1111.1111.1111.1111.00`	ローカル OSI ルーティング ドメインの 1 つのプレフィクスをアドバタイズし、そのプレフィクスを BGP ルーティング テーブルに入力します。 **（注）** 1 つのプレフィクスをアドバタイズできるのは、そのプレフィクスが、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、「参考資料」（P.35）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。
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 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	**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：** `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。

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。
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ディセーブルにします。
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	**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-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：** `Router> enable`	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。
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ディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**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。
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 ルートをフィルタリングするには、**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。

前提条件

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。
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ディセーブルにします。
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)# 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

この作業を実行して NSAP プレフィクスに基づきアウトバウンド BGP アップデートをフィルタリングし、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** コマンドを実行します。この作業は、図 1 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 プレフィクスを拒否し、49 で始まる他のすべての NSAP プレフィクスを許可します。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-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：** `Router> enable`	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。
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	**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。

	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 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ディセーブルにします。
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：** `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 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。
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ディセーブルにします。
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：例」（P.30）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、図 1（P.3）に示されるルータ 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。

```
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。次に、図 1（P.3）に示されるルータ R2 の出力例を示します。i 49.0202.3333 [110/10] via R3 のルーティング テーブル エントリは、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を示します。

```
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, Ethernet0/1
```

```
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, Ethernet0/1
```

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。

```
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** 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 プレフィクス ルートが表示されます。次に、図 1（P.3）に示されるルータ R2 の出力例を示します。プレフィクス 49.0101 への 1 つの有効なルートが示されます。* でマーキングされている 2 つの有効なルートが、プレフィクス 49.0404 で示されます。2 番目のルートが *>i シーケンスでマーキングされ、このプレフィクスへの最良ルートを表しています。

```
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イネーブルにします。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 **degub** コマンドの使用の詳細については、『*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. コンソールを接続します。
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 Cisco IOS 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 接続を切断する必要がある場合は、**debug bgp nsap unicast** 出力を生成するプロセッサ負荷のためルータが応答できない場合があることから、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イネーブルにします。

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すると、指定されたサブコンポーネントに関する詳細なデバッグ情報が生成されます。

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ディセーブルにします。

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イネーブルにします。

CLNS に対する MP-BGP サポートの設定例

このセクションでは、前項の指定されたコンフィギュレーション作業と一致するコンフィギュレーション例を示します。図 1（P.3）のすべてのルータ コンフィギュレーションの概要を説明するために、各ルータの詳細なコンフィギュレーションがこのセクションの終わりに加えられています。

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：例

次の例では、自律システム AS65101 で、図 3（P.30）に示されるルータ R1 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ディセーブルにするために、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** コマンドでイネーブルにされると、ルータが 49.0101 の NSAP プレフィクスを 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
```

IS-IS ルーティング プロセスの設定：例

次の例では、図 3（P.30）に示されるルータ R1 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：例

次の例では、自律システム AS65202 で、図 3（P.30）に示されるルータ R2 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。イーサネット インターフェイス 0/1 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 ethernet 0/1
 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 プレフィクスのアドバタイジング：例

次の例では、図 3（P.30）に示されるルータ R1 が、49.0101 の NSAP プレフィ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
```

BGP から IS-IS へのルートの再配布：例

次の例では、自律システム AS65404 の 図 3（P.30）に示されるルータ R7 および R9 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
```

IS-IS から BGP へのルートの再配布：例

次の例では、自律システム AS65202 の 図 3（P.30）に示されるルータ R2 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ディセーブルにするために、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：例

図 1（P.3）に示されるルータ 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 プレフィクスに基づくインバウンド ルートのフィルタリング：例

次の例では、自律システム AS65101 の 図 3（P.30）に示されるルータ R1 が、デフォルト プレフィクス専用のプレフィクス リストで指定されたインバウンド ルートをフィルタリング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
```

NSAP プレフィ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：例

次の例では、アウトバウンド BGP アップデートが NSAP プレフィクスに基づいてフィルタリングされます。この例は、図 3（P.30）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 プレフィクスを拒否し、49 で始まる他のすべての NSAP プレフィクスを許可します。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
```

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：例

図 3（P.30）では、自律システム AS65101 が、他の 1 つの自律システム AS65202 だけに接続されます。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 図 3（P.30）に示されるルータ R2 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。

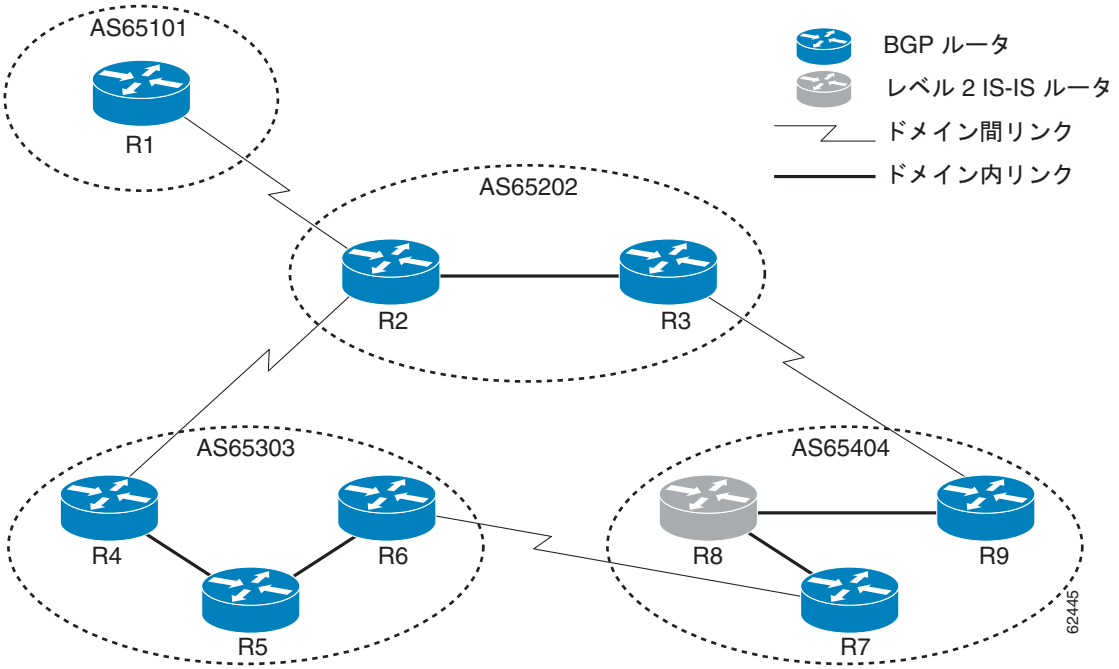
```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 no bgp default ipv4-unicast
 neighbor 10.1.2.1 remote-as 64101
 address-family nsap
  network 49.0202...
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
```

```
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：例

図 3 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。ここでは、図 3 に示され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 3　　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 「参考資料」（P.35） 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 ethernet 0/1
  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 ethernet 0/1
 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 ethernet 0/2
 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 ethernet 0/2
 ip address 10.4.5.5 255.255.255.0
 clns router isis osi-as-303
```

```
 no shutdown
!
interface ethernet 0/3
 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 ethernet 0/3
 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 ethernet 1/0
 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 ethernet 1/0
 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 ethernet 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 ethernet 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
```

参考資料

次のセクションでは、CLNS に対するマルチプロトコル BGP（MP-BGP）サポート機能に関する参考資料について説明します。

関連資料

関連項目	参照先
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
CLNS コマンド	『*Cisco IOS ISO CLNS Command Reference*』

規格

規格	タイトル
ISO/IEC 8473	『*ISO CLNP: Connectionless Network Protocol (ISO-IP)*』。コネクションレス型モード ネットワーク サービスを提供するプロトコル。
ISO/IEC 9542	『*End System to Intermediate System Protocol (ESIS)*』。コネクションレス型モード ネットワーク サービス（ISO 8473）を提供するプロトコルとともに使用される、エンド システムから中継システムまでのルーティング交換プロトコル。
ISO/IEC 10589	『*IS-IS, Intermediate System-to-Intermediate System*』。コネクションレス型モード ネットワーク サービス（ISO 8473）を提供するプロトコルとともに使用される、中継システム間のドメイン内ルーティング情報交換プロトコル。

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 1700	『*Assigned Numbers*』
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 1997	『*BGP Communities Attribute*』
RFC 2042	『*Registering New BGP Attribute Types*』
RFC 2439	『*BGP Route Flap Dampening*』
RFC 2842	『*Capabilities Advertisement with BGP-4*』
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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。この 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。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/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

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。12.2(1) 以降のリリースで追加または変更された機能だけが、テーブルに示されています。

このテクノロジーの機能でここに記載されていない情報については、『BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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	12.2(8)T 12.2(33)SRB	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。 リリース 12.2(8)T では、この機能が次のプラットフォームで追加されました。 • Cisco 2600 シリーズ • Cisco 3600 シリーズ • Cisco 7100 シリーズ • Cisco 7200 シリーズ • Cisco 7500 シリーズ • Cisco uBR7200 シリーズ リリース 12.2(33)SRB では、この機能が Cisco 7600 シリーズで追加されました。 この機能によって、次の各コマンドが追加変更されています。**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** および**マルチプロトコル BGP**）、**redistribute**（**BGP** から **ISO ISIS**）、**redistribute**（**ISO ISIS** から **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**、**show bgp nsap summary**

用語集

AS：Autonomous System（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 レイヤ 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 レイヤ 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：International Organization for Standardization（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 アドレス：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（開放型システム間相互接続）。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。

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：Synchronous Optical Network。光ファイバ上で稼動するように設計された高速同期ネットワーク仕様です。

アドレス ファミリ：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。

ルーティング ドメイン：BGP の自律システムに相当する OSI 用語。

BGP リンク帯域幅

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）Link Bandwidth 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 external BGP（eBGP; 外部 BGP）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 アトリビュートは、拡張コミュニティ交換がイネーブルなとき、internal BGP（iBGP; 内部 BGP）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。

BGP リンク帯域幅機能の履歴

リリース	変更内容
12.2(2)T	この機能が追加されました。
12.2(14)S	この機能は、Cisco IOS Release 12.2(14)S に統合されました。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「BGP リンク帯域幅の機能情報」（P.10）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

マニュアルの内容

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。
- リンク帯域幅アトリビュート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、シスコ エクスプレス フォワーディングまたは分散シスコ エクスプレス フォワーディングがイネーブルにされ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イネーブルになります。この機能は、iBGP、eBGP マルチパス ロード バランシングおよび Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）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 アトリビュートは、**neighbor send-community** コマンドで拡張コミュニティ交換がイネーブルにされたとき、iBGP ピアに伝播します。

リンク帯域幅拡張コミュニティのアトリビュート

リンク帯域幅拡張コミュニティのアトリビュートは 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 Demilitarized Zone（DMZ; 非武装地帯）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アトリビュートは、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 Interior Gateway Protocol（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および確認」（P.3）（必須）

BGP リンク帯域幅の設定および確認

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**
5. **address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
6. **bgp dmzlink-bw**
7. **neighbor** *ip-address* **dmzlink-bw**
8. **neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**]
9. **end**
10. **show ip bgp** *ip-address* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*mask-length*]]
11. **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 モードなどの上位の特権レベル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。
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** **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 モードを開始します。
ステップ 5	**address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	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 6	**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 7	**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アトリビュートを含めるように 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 8	**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アトリビュートが伝播する iBGP ピア用に設定する必要があります。
ステップ 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。

	コマンドまたはアクション	目的
ステップ 10	**show ip bgp** *ip-address* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*mask-length*]] **例：** `Router# show ip bgp 10.0.0.0`	（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。 • 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 11	**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`	（任意）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

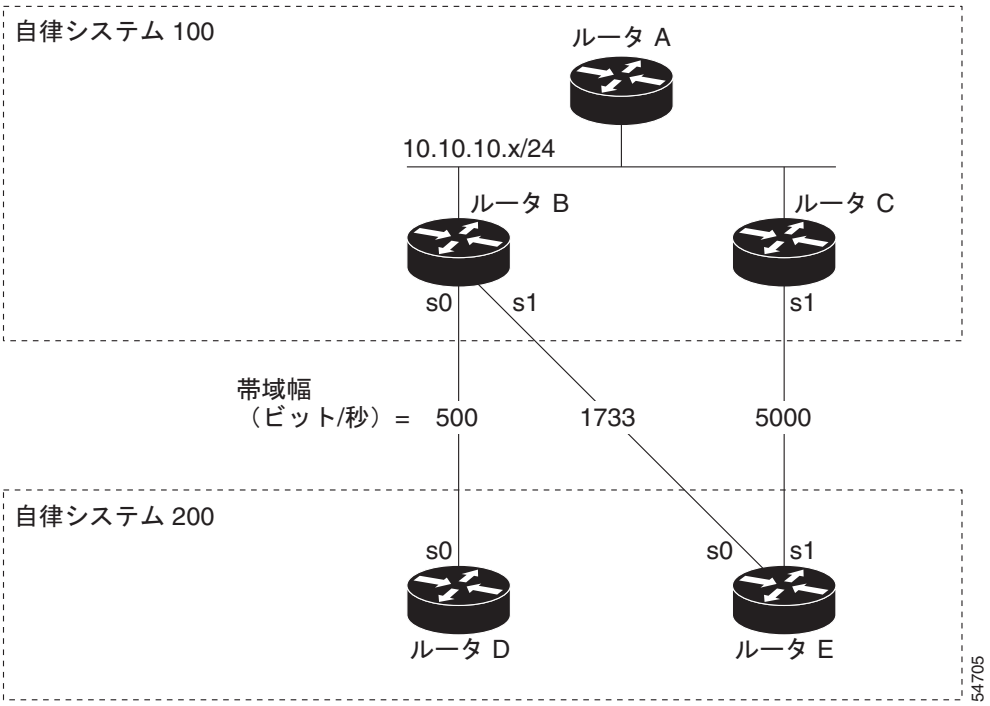
例：BGP リンク帯域幅設定の確認

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。図 1 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 バランシングがイネーブルになっており、トラフィックに比例してバランスされています。

（注） BGP リンク帯域幅機能は、出力点への単一のパスがある単純なトポロジに対して動作します。

注意 出力点へのロード バランシングが必要な場合は、BGP リンク帯域幅機能が正しく機能しないことがあります。

図 1　　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 アトリビュートを iBGP ネイバーと交換するようにルータ A を設定します。

```
RouterA(config)# router bgp 100
RouterA(config-router)# neighbor 10.10.10.2 remote-as 100
RouterA(config-router)# neighbor 10.10.10.2 update-source Loopback 0
RouterA(config-router)# neighbor 10.10.10.3 remote-as 100
RouterA(config-router)# neighbor 10.10.10.3 update-source Loopback 0
RouterA(config-router)# address-family ipv4
RouterA(config-router-af)# bgp dmzlink-bw
RouterA(config-router-af)# neighbor 10.10.10.2 activate
RouterA(config-router-af)# neighbor 10.10.10.2 send-community both
RouterA(config-router-af)# neighbor 10.10.10.3 activate
RouterA(config-router-af)# neighbor 10.10.10.3 send-community both
RouterA(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。

```
RouterB(config)# router bgp 100
RouterB(config-router)# neighbor 10.10.10.1 remote-as 100
RouterB(config-router)# neighbor 10.10.10.1 update-source Loopback 0
RouterB(config-router)# neighbor 10.10.10.3 remote-as 100
RouterB(config-router)# neighbor 10.10.10.3 update-source Loopback 0
RouterB(config-router)# neighbor 172.16.1.1 remote-as 200
RouterB(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
RouterB(config-router)# neighbor 172.16.2.2 remote-as 200
RouterB(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
RouterB(config-router)# address-family ipv4
RouterB(config-router-af)# bgp dmzlink-bw
```

```
RouterB(config-router-af)# neighbor 10.10.10.1 activate
RouterB(config-router-af)# neighbor 10.10.10.1 next-hop-self
RouterB(config-router-af)# neighbor 10.10.10.1 send-community both
RouterB(config-router-af)# neighbor 10.10.10.3 activate
RouterB(config-router-af)# neighbor 10.10.10.3 next-hop-self
RouterB(config-router-af)# neighbor 10.10.10.3 send-community both
RouterB(config-router-af)# neighbor 172.16.1.1 activate
RouterB(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
RouterB(config-router-af)# neighbor 172.16.2.2 activate
RouterB(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
RouterB(config-router-af)# maximum-paths ibgp 6
RouterB(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。

```
RouterC(config)# router bgp 100
RouterC(config-router)# neighbor 10.10.10.1 remote-as 100
RouterC(config-router)# neighbor 10.10.10.1 update-source Loopback 0
RouterC(config-router)# neighbor 10.10.10.2 remote-as 100
RouterC(config-router)# neighbor 10.10.10.2 update-source Loopback 0
RouterC(config-router)# neighbor 172.16.3.30 remote-as 200
RouterC(config-router)# neighbor 172.16.3.30 ebgp-multihop 1
RouterC(config-router)# address-family ipv4
RouterC(config-router-af)# bgp dmzlink-bw
RouterC(config-router-af)# neighbor 10.10.10.1 activate
RouterC(config-router-af)# neighbor 10.10.10.1 send-community both
RouterC(config-router-af)# neighbor 10.10.10.1 next-hop-self
RouterC(config-router-af)# neighbor 10.10.10.2 activate
RouterC(config-router-af)# neighbor 10.10.10.2 send-community both
RouterC(config-router-af)# neighbor 10.10.10.2 next-hop-self
RouterC(config-router-af)# neighbor 172.16.3.3 activate
RouterC(config-router-af)# neighbor 172.16.3.3 dmzlink-bw
RouterC(config-router-af)# maximum-paths ibgp 6
RouterC(config-router-af)# maximum-paths 6
```

BGP リンク帯域幅の確認

ここで、ルータ A、ルータ B、およびルータ C 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最良パスがインストールされているかを確認します。各リンクの帯域幅は、各ルートとともに表示されます。

```
RouterB# 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 に入力して、iBGP を通じてリンク帯域幅拡張コミュニティがルータ A に伝播しているかを確認します。出口リンクは、ルータ B およびルータ C にあります。出力には、BGP のルーティング テーブルの最良パスとして、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。

```
RouterA# 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。

```
RouterA# 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
```

次の作業

MPLS-VPN 機能の中で、eBGP と iBGP の両方を対象とする BGP マルチパス ロード シェアリングの詳細については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_ebgp_ibgp.html

iBGP マルチパス ロード シェアリング機能に関する詳細については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_multi_load.html

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	参照先
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、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP 設定作業	「*BGP Feature Roadmap*」モジュール
CEF 設定作業	「Cisco Express Forwarding Overview」モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	プラットフォームおよび Cisco IOS リリースでサポートされる MIB のリストを入手して、MIB モジュールをダウンロードするには、次の URL にある Cisco.com の Cisco MIB Web サイト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
draft-ramachandra-bgp-ext-communities-09.txt	『*BGP Extended Communities Attribute*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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 リンク帯域幅の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 1　　<モジュール タイトルに基づいたフレーズ> の機能情報

機能名	リリース	機能情報
BGP リンク帯域幅	12.2(2)T 12.2(14)S	この機能は、自律システムの出口リンクの帯域幅を拡張コミュニティとしてアドバタイズします。このリンク帯域幅拡張コミュニティ リンク アトリビュートは、拡張コミュニティ交換がイネーブルなとき、internal BGP（iBGP; 内部 BGP）ピアに伝播します。 この機能に関する詳細については、次の各項を参照してください。 • 「BGP リンク帯域幅の概要」（P.2） • 「リンク帯域幅拡張コミュニティのアトリビュート」（P.3） • 「BGP リンク帯域幅機能の利点」（P.3） 次のコマンドが、導入または変更されました。**router bgp**、**address-family ipv4**、**address-family ipv4**、**bgp dmzlink-bw**、**neighbor**、**show ip bgp**、**show ip route**。

iBGP のマルチパス ロード シェアリング

この機能モジュールでは、internal BGP（iBGP; 内部 BGP）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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「iBGP のマルチパス ロード シェアリングの機能情報」（P.10）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

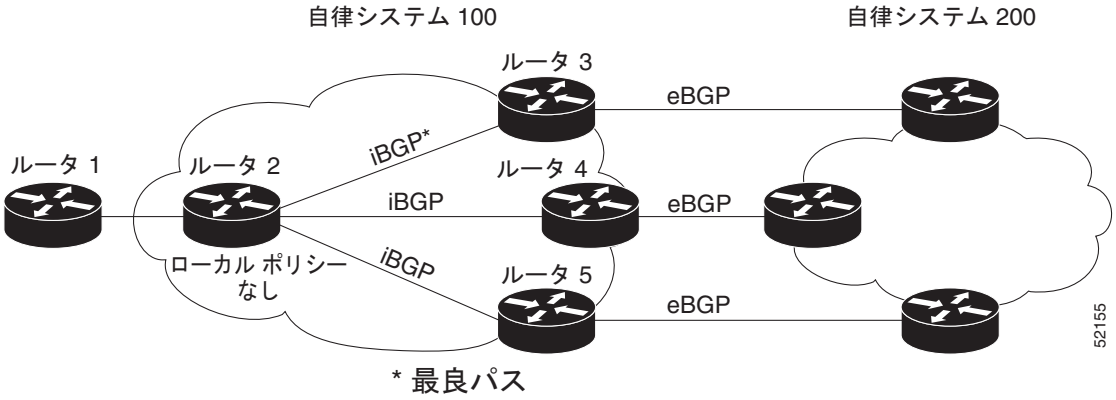
iBGP のマルチパス ロード シェアリングの制約事項

- ルート リフレクタの制約：複数の iBGP のパスがルーティング テーブルにインストールされていると、ルート リフレクタは、パスの 1 つ（1 つのネクストホップ）だけに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 シェアリング機能は、Cisco IOS Release 12.2(14)S の次のプラットフォームでサポートされます。
  - Cisco 7200 シリーズ
  - Cisco 7400 シリーズ
  - Cisco 7500 シリーズ

機能概要

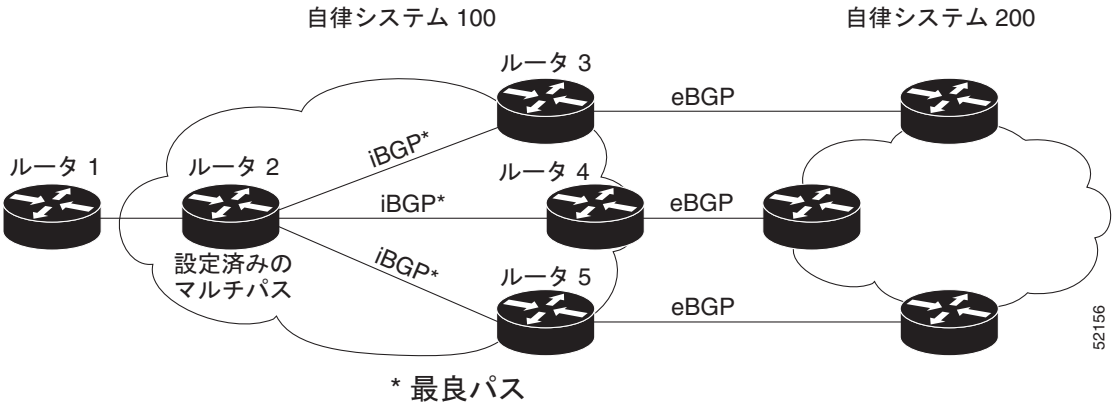
ローカル ポリシーが設定されていない Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）対応ルータが複数の Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着達可能性情報）を同じ宛先の内部 BGP（iBGP）から受信すると、このルータは 1 つの iBGP パスを最良パスとして選択します。この最良パスは、次にこのルータの IP ルーティング テーブルにインストールされます。たとえば、図 1 では、自律システム 200 へのパスは 3 つありますが、ルータ 2 は、自律システム 200 へのパスの 1 つを最良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 1　　1 つの最良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



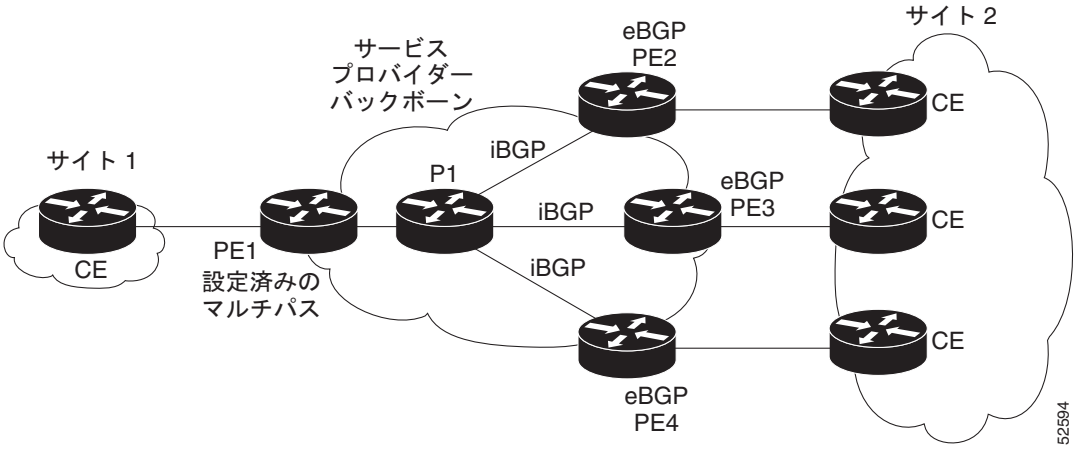
iBGP のマルチパス ロード シェアリング機能を使用すると、BGP 対応ルータがイネーブルになり、複数の iBGP パスを宛先への最良パスとして選択できます。この最良パスまたはマルチパスは、次にこのルータの IP ルーティング テーブルにインストールされます。たとえば、図 2 のルータ 2 で、ルータ 3、4 および 5 へのパスがマルチパスとして設定され、自律システム 200 に到達するために使用でき、結果として自律システム 200 への負荷が均等に負担されます。

図 2　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 Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）と同様に機能します。たとえば、図 3 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 3　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。

- すべてのアトリビュートが同じである必要があります。アトリビュートには、加重、ローカル プリファレンス、自律システム パス（長さだけでなくアトリビュート全体）、発信元コード、Multi Exit Discriminator（MED）、および Interior Gateway Protocol（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 つを最良パスに指定し、この最良パスをそのネイバーにアドバタイズします。

利点

複数の iBGP の最良パスを設定すると、ルータがイネーブルになり、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ます。

関連する機能およびテクノロジー

iBGP のマルチパス ロード シェアリング機能は、external BGP（eBGP; 外部 BGP）パスに対する BGP マルチパス サポートに類似していますが、iBGP のマルチパス ロード シェアリング機能は、eBGP パスではなく、内部に適用されます。

設定作業

iBGP のマルチパス ロード シェアリング機能の設定作業については、次の項目を参照してください。リスト内の各作業は、必須または任意のいずれかに識別されています。

- 「iBGP のマルチパス ロード シェアリングの設定」（必須）
- 「iBGP のマルチパス ロード シェアリングの確認」（任意）

iBGP のマルチパス 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
`Router(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 iBGP の最大パラレル ルート数を制御します。

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。

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アトリビュートを表示するか、**show ip bgp vpnv4 all** *ip-prefix* EXEC コマンドを入力して、MPLS VPN のネットワークのアトリビュートを表示します。

```
Router# 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

Router# 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。

```
Router# 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

Router# 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、ステップ 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
Router# **show ip bgp** *ip-prefix*	非 MPLS トポロジのネットワークのアトリビュートおよびマルチパスを表示します。
Router# **show ip bgp vpnv4 all** *ip-prefix*	MPLS VPN のネットワークのアトリビュートおよびマルチパスを表示します。
Router# **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。
Router# **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

ここでは、次の設定例について説明します。

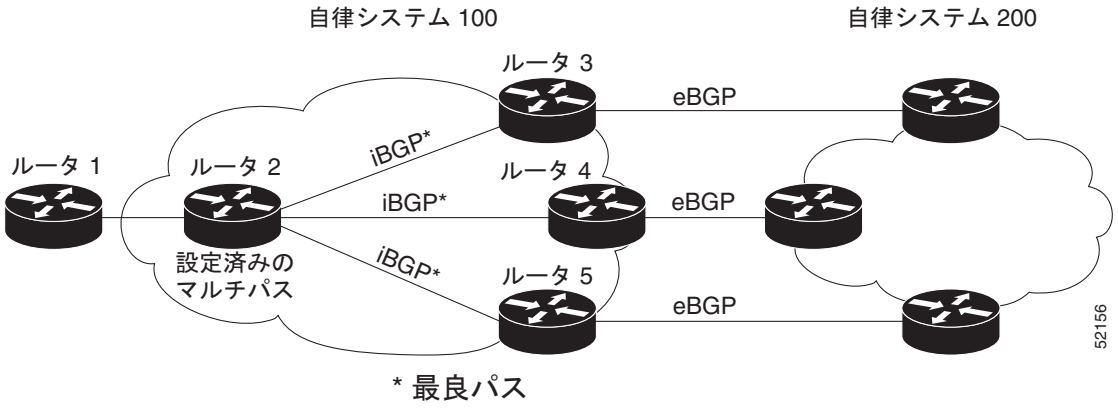
- 「非 MPLS トポロジの例」
- 「MPLS VPN トポロジの例」

設定例は両方とも、各パスの適切なアトリビュートが等しく、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。

非 MPLS トポロジの例

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（図 4 を参照）。

図 4　　非 MPLS トポロジの例



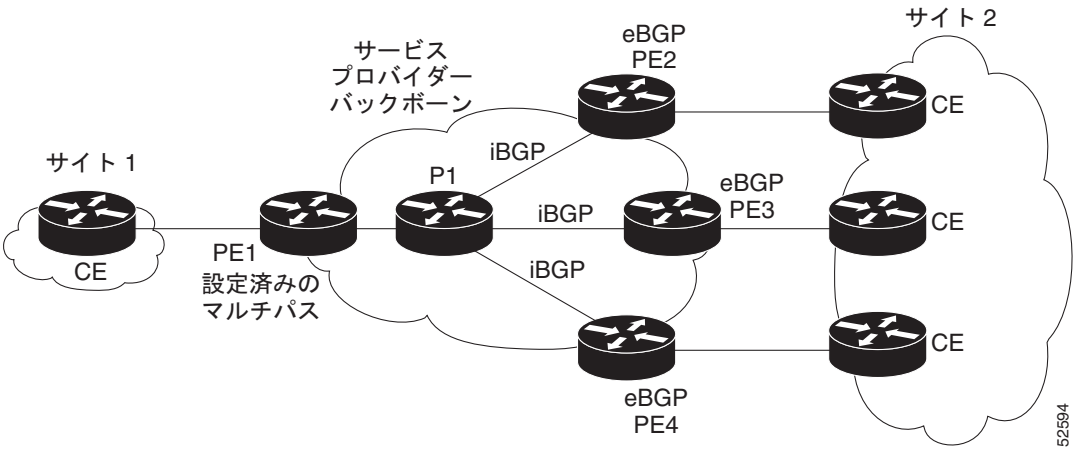
ルータ 2 の設定

```
router bgp 100
maximum-paths ibgp 3
```

MPLS VPN トポロジの例

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（図 5 を参照）。

図 5　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
```

参考資料

ここでは、iBGP のマルチパス ロード シェアリング機能に関する参考資料について説明します。

関連資料

関連項目	参照先
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
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	『*BGP Link Bandwidth*』
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	『*BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

新しいコマンド

- **maximum-paths ibgp**

変更されたコマンド

- **show ip bgp**
- **show ip bgp vpnv4**
- **show ip route**
- **show ip route vrf**

iBGP のマルチパス ロード シェアリングの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

このテクノロジーの機能でここに記載されていない情報については、『*BGP Features Roadmap*』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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	12.2(14)S 12.2(2)T	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 対応ルータがイネーブルになり、複数の iBGP パスを宛先への最良パスとして選択できます。 次のコマンドが導入または変更されました。**maximum-paths ibgp**、**show ip bgp**、**show ip bgp vpnv4**、**show ip route**、**show ip route vrf**。

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

external BGP（eBGP; 外部 BGP）および internal BGP（iBGP; 内部 BGP）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、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を使用するように設定された Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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 Provider Edge（PE; プロバイダー エッジ）ルータのために役立ちます。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリングの機能情報」（P.11）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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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 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 Routing and Forwarding（VRF; VPN ルーティング/転送）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 に対する BGP マルチパス ロード シェアリングに関する情報

MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能を設定するには、次の概念について理解する必要があります。

- 「eBGP および iBGP に対する BGP マルチパス ロード シェアリングの利点」（P.5）

eBGP と iBGP の間のマルチパス 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 つのパスを最良パスとして Routing Information Base（RIB; ルーティング情報ベース）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 はこの場合も最良パス アルゴリズムを使用して 1 つのマルチパスを最良パスとして選択し、その最良パスを BGP ピアにアドバタイズします。

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

マルチパス全体でのロード バランシングは CEF によって実行されます。CEF ロード バランシングは、パケット単位のラウンド ロビンまたはセッション単位（送信元と宛先のペア）を基準として設定されます。CEF については、『Cisco Express Forwarding Overview』のマニュアルを参照してください。

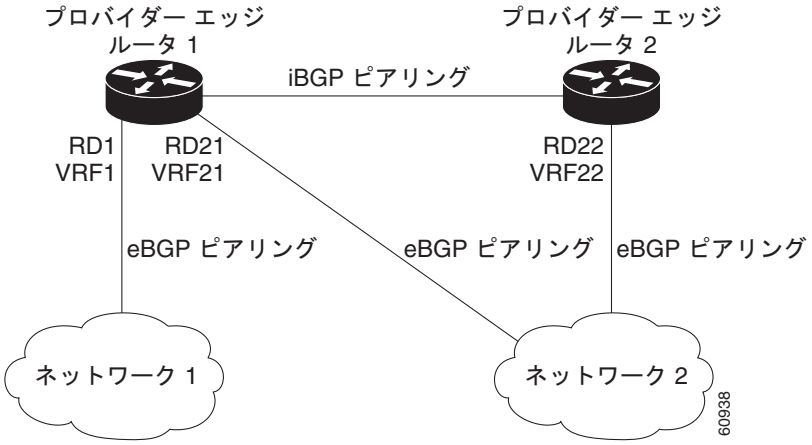
MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能は、IPv4 VRF アドレス ファミリ コンフィギュレーション モードだけでイネーブルにされます。この機能がイネーブルにされると、VRF にインポートされた eBGP パスまたは iBGP パスあるいはその両方でロード バランシングを実行できます。マルチパスの数は VRF 単位で設定されます。別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。

（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

図 1 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 1　サービス プロバイダー BGP MPLS ネットワーク

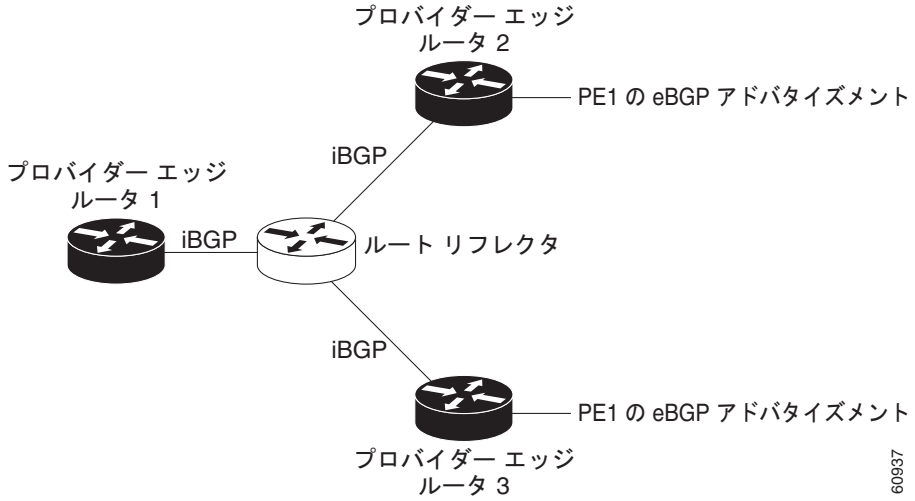


PE ルータ 1 には、MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能が設定でき、これによって、iBGP パスと eBGP パスの両方をマルチパスとして選択し、ネットワーク 1 の VRF にインポートできます。マルチパスは CEF によって使用され、ロード バランシングが実行されます。ネットワーク 2 から PE ルータ 1 および PE ルータ 2 に送信される IP トラフィックは、eBGP パスを経由して IP トラフィックとして送信されます。iBGP パスを経由して送信される IP トラフィックは MPLS トラフィックとして送信され、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クスは、Route Distinguisher（RD; ルート識別子）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

図 2 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 2　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 に対する BGP 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 に対する BGP マルチパス ロード シェアリングの設定方法

ここでは、次の手順について説明します。

- 「eBGP および iBGP へのマルチパス ロード シェアリングの設定」（P.5）
- 「eBGP および iBGP に対するマルチパス ロード シェアリングの確認」（P.6）

eBGP および iBGP へのマルチパス 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** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **ipv6** [**multicast** | **unicast**] | **vpnv4** [**unicast**]

5. **maximum-paths eibgp** *number* [**import** *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：** `Router> enable`	特権 EXEC モードなどの上位の特権レベル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。
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 プロセスを作成または設定します。
ステップ 4	**address-family ipv4 vrf** *vrf-name* **例：** `Router(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* [**import** *number*] **例：** `Router(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：** `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。

eBGP および iBGP に対するマルチパス ロード シェアリングの確認

この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 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：** `Router> enable`	特権 EXEC モードなどの上位の特権レベル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。
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：** `Router# 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：** `Router# 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：** `Router# 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 に対する BGP マルチパス ロード シェアリング機能の設定例

次に、この機能の設定方法および確認方法の例を示します。

- 「eBGP および iBGP のマルチパス ロード シェアリングを設定する例」（P.7）
- 「eBGP および iBGP のマルチパス ロード シェアリングを確認する例」（P.7）

eBGP および iBGP のマルチパス ロード シェアリングを設定する例

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。

```
Router(config)# router bgp 40000
 Router(config-router)# address-family ipv4 vrf RED
 Router(config-router-af)# maximum-paths eibgp 6
 Router(config-router-af)# end
```

eBGP および iBGP のマルチパス ロード シェアリングを確認する例

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。

```
Router# 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。

```
Router# 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 Link Bandwidth』を参照してください。

参考資料

MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリングに関連する情報については、次の参考資料を参照してください。

関連資料

関連項目	参照先
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、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP 設定作業	「BGP Features Roadmap」モジュール
総合的な BGP リンク帯域幅の設定例および作業	「BGP Link Bandwidth」モジュール
CEF 設定作業	「Cisco Express Forwarding Overview」モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	プラットフォームおよび Cisco IOS リリースでサポートされる MIB のリストを入手して、MIB モジュールをダウンロードするには、次の URL にある Cisco.com の Cisco MIB Web サイト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	タイトル
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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

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

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 12.2(1)、12.0(3)S、12.2(27)SBC、12.2(33)SRB、12.2(33)SXH、またはそれ以降のリリースで追加または変更された機能だけが表に示されています。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

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

機能名	リリース	機能の設定情報
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	12.0(24)S 12.2(14)S 12.2(18)SXE 12.2(4)T 15.0(1)S Cisco IOS XE 3.1.0SG	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、MPLS VPN を使用するように設定された BGP ネットワークで、eBGP パスおよび 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 PE ルータのために役立ちます。 この機能によって次のコマンドが導入または変更されました。**maximum-paths eibgp**

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

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、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

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「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の機能情報」（P.4）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

マニュアルの内容

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。

この機能には、次の利点があります。

- 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。

参考資料

マルチパス ロード シェアリングおよびパラレル ルートのコンフィギュレーションに関連する詳細情報については、次の資料を参照してください。

関連資料

関連項目	参照先
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、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
マルチパス ロード シェアリングを含む BGP 設定作業	『BGP Feature Roadmap』
eiBGP マルチパス ロード シェアリング	「BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN」モジュール
iBGP のマルチパス ロード シェアリング	「iBGP Multipath Load Sharing」モジュール

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/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機能の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 1　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の機能情報

機能名	リリース	機能情報
『Loadsharing IP Packets Over More Than Six Parallel Paths』	12.3(2)T、12.2(25)S、Cisco IOS XE 3.1.0SG	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、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。 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**

BGP ポリシー アカウンティング

機能履歴

リリース	変更内容
12.0(9)S	この機能が追加されました。
12.0(17)ST	この機能は、Cisco IOS Release 12.0(17)ST に統合されました。
12.2(13)T	この機能は、Cisco IOS Release 12.2(13)T に統合されました。
15.0(1)S	この機能は、Cisco IOS Release 15.0(1)S に統合されました。

このマニュアルでは、Cisco IOS Release 12.2(13)T の BGP ポリシー アカウンティング機能を説明します。ここでは、次の内容について説明します。

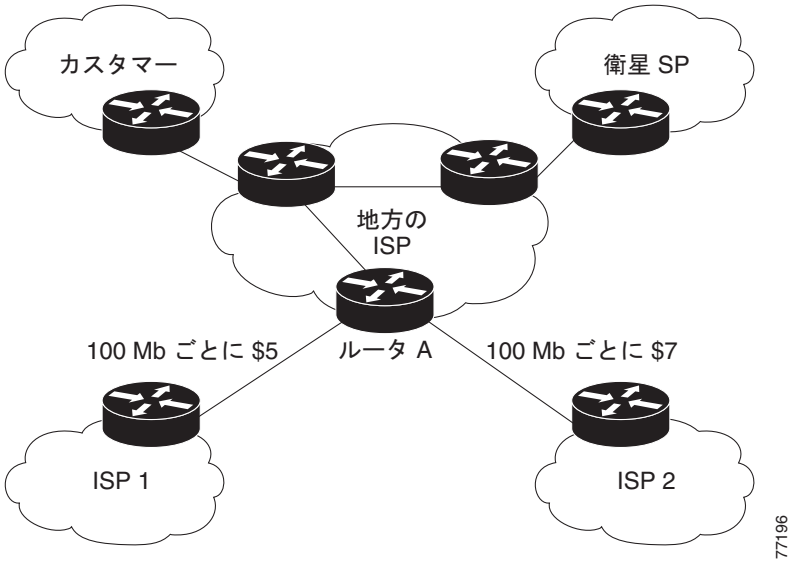
機能概要

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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 Internet Protocol（IP; インターネット プロトコル）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クスは、BGP アトリビュート、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。Service Provider（SP; サービス プロバイダー）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。図 1-1 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 1-1　　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、Internet Service Provider（ISP; インターネット サービス プロバイダー）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。

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。

関連する機能およびテクノロジー

BGP のコンフィギュレーション情報を確認するには、『*Cisco IOS IP Routing: BGP Configuration Guide*』の「Cisco BGP Features Roadmap」モジュールの章を参照してください。BGP コマンド情報を確認するには、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

追加の Cisco Express Forwarding（CEF）および Distributed CEF（dCEF）のコマンドおよびコンフィギュレーション情報は、『*Cisco IOS Switching Services Configuration Guide*』の「Cisco Express Forwarding Overview」モジュールおよび『*Cisco IOS Switching Command Reference*』に記載されています。

関連資料

- 『*Cisco IOS IP Routing: BGP Command Reference*』
- 『*Cisco IOS IP Switching Command Reference*』

サポート プラットフォーム

BGP ポリシー アカウンティング機能は、Cisco IOS Release 12.2(13)T をサポートする次のプラットフォームでサポートされています。

- Cisco 1400 シリーズ
- Cisco 1600 シリーズ
- Cisco 1700 シリーズ
- Cisco 2600 シリーズ
- Cisco 3600 シリーズ
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco 7500 シリーズ
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850
- Cisco ICS7750
- Cisco IGX 8400 URM
- Cisco MC3810
- Cisco MGX 8850
- Cisco uBR7200 シリーズ

プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

サポートされる標準、管理情報ベース（MIB）、コメント要求（RFC）

規格

この機能がサポートする新しい規格または変更された規格はありません。

MIB

- 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 Management Information Base（MIB; 管理情報ベース）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 IOS リリース、および機能セットの 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://tools.cisco.com/ITDIT/MIBS/servlet/index

Cisco MIB Locator で必要な MIB 情報がサポートされていない場合は、次の URL にある Cisco MIB ページにアクセスすれば、サポートされている MIB のリストを入手したり、MIB をダウンロードしたりできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れた場合や紛失した場合は、cco-locksmith@cisco.com に空メールを送信してください。自動チェックにより、ご使用の E メール アドレスが Cisco.com に登録されているか検証されます。チェックが成功した場合は、アカウントの詳細がランダムな新パスワードと一緒に E メールで送信されます。認証されたユーザは、次の URL に表示される指示に従うことで、Cisco.com にアカウントを構築できます。

https://tools.cisco.com/RPF/register/register.do

RFC

この機能がサポートする新しい Request for Comments（RFC; コメント要求）または変更された RFC はありません。

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。

設定作業

BGP ポリシー アカウンティング機能の設定作業については、次のセクションを参照してください。リスト内の各作業は、必須または任意のいずれかに識別されています。

- 「BGP ポリシー アカウンティングの一致基準の指定」（P.5）（必須）
- 「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イネーブル化」（P.5）（必須）
- 「BGP ポリシー アカウンティングの確認」（P.6）（任意）

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 アトリビュートの例です。

BGP ポリシー アカウンティングに使用する BGP アトリビュートを指定し、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。

	コマンド	目的
ステップ 1	`Router(config)# ip community-list` *community-list-number* {**permit** | **deny**} *community-number*	BGP のコミュニティ リストを作成して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	`Router(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。 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	`Router(config-route-map)# match community-list` *community-list-number* [**exact**]	BGP コミュニティを一致させます。
ステップ 4	`Router(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イネーブル化

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イネーブルにする前に、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イネーブル化されます。

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イネーブルにするには、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。

	コマンド	目的
ステップ 1	`Router(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。
ステップ 2	`Router(config-router)# table-map route-map-name`	ルーティング テーブルに入力された BGP プレフィクスを分類します。
ステップ 3	`Router(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	`Router(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	`Router(config-router)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	`Router(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	`Router(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	`Router(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	`Router(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イネーブルにします。

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。

ステップ 1 どのアカウンティング バケットが指定されたプレフィクスに割り当てられているかを学習するために、**detail** キーワードを指定して **show ip cef** EXEC コマンドを入力します。

この例では、プレフィクス 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）がこのプレフィクスに割り当てられていることが示されています。

```
Router# 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 ステップ 1 と同じプレフィクス（192.168.5.0）に対し、どのコミュニティが割り当てられているかを学習するために **show ip bgp** EXEC コマンドを入力します。

この例では、プレフィクス 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」がこのプレフィクスに割り当てられていることが示されています。

```
Router# 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。

```
LC-Slot7# 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

BGP ポリシー アカウンティング機能をモニタリングおよびメンテナンスするには、必要に応じて次のコマンドを EXEC モードで使用します。

コマンド	目的
Router# **show cef interface** [*type number*] **policy-statistics**	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。
Router# **show ip bgp** [*network*] [*network mask*] [**longer-prefixes**]	BGP ルーティング テーブル内のエントリを表示します。
Router# **show ip cef** [*network* [*mask*]] [**detail**]	Forwarding Information Base（FIB; 転送情報ベース）のエントリまたは FIB の概要を表示します。

設定例

ここでは、次の設定例について説明します。

- 「BGP ポリシー アカウンティングの一致基準の指定例」
- 「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イネーブル化の例」

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 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
```

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イネーブル化の例

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イネーブルにされ、**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
```

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、
http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP*

Routing: BGP Command Reference』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

- **bgp-policy**
- **set traffic-index**
- **show cef interface policy-statistics**
- **show ip bgp**
- **show ip cef**

用語集

AS：Autonomous System（自律システム）。独自の独立したルーティング ポリシーを持ち、単一権限により管理されるルーティング ドメインを指す 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。

dCEF：distributed Cisco Express Forwarding。

BGP コスト コミュニティ

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、internal BGP（iBGP; 内部 BGP）およびコンフェデレーション ピアには渡されますが、external BGP（eBGP; 外部 BGP）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、最良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、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）およびバックドア リンクを備えた多様な Enhanced Interior Gateway Routing Protocol（EIGRP; 拡張内部ゲートウェイ ルーティング プロトコル）Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP コスト コミュニティの機能情報」（P.12）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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 コミュニティ機能には次の制約事項が適用されます。

- 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 コミュニティは非遷移の拡張コミュニティ アトリビュートで、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 Point Of Insertion（POI; 挿入ポイント）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、その他のアトリビュート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 コミュニティ機能を設定するには、次の概念について理解する必要があります。

BGP コスト コミュニティの概要

コスト コミュニティは非遷移の拡張コミュニティ アトリビュートで、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 最良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 アトリビュートは、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。パスのプリファレンスは、コスト番号値により決定されます。最も低いコスト コミュニティ番号を持つパスが優先されます。コスト コミュニティ アトリビュート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、最良パス選択プロセスにより評価されます。2 つのパスに同一のコスト番号値が設定されている場合、パス選択プロセスにより最も低いコスト コミュニティ ID を持つパスが優先されます。コスト拡張コミュニティ アトリビュートは、**neighbor send-community** コマンドにより拡張コミュニティ交換がイネーブルになったときに iBGP ピアに伝播されます。

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 コミュニティはどのように最良パス選択プロセスに影響するか

BGP 最良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 アトリビュートの影響を受けます。デフォルトでは、POI は Interior Gateway Protocol（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 は最良パス選択プロセスを使用して、いずれのパスが最良パスであるかを決定します。最良パスは 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。ローカルの最良パス選択で POI が有効でない場合は、コスト コミュニティ アトリビュートは暗黙的に無視されます。

コスト コミュニティ アトリビュートを使用して、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次にその POI において最も低いコミュニティ ID を持つパスに進みます。

（注） パスにコスト コミュニティ アトリビュートが設定されていない場合、最良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 アトリビュートを適用することで、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ピアを起点とするパスまたは任意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、最良パス選択プロセス中の「タイ ブレーカ」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 最良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」（P.4）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 アトリビュートは、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 アトリビュートは、コスト コミュニティ アトリビュート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 ルートに伝送されます。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、最も高く設定された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 アトリビュート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 アトリビュートを伝送しない場合、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 アトリビュート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)

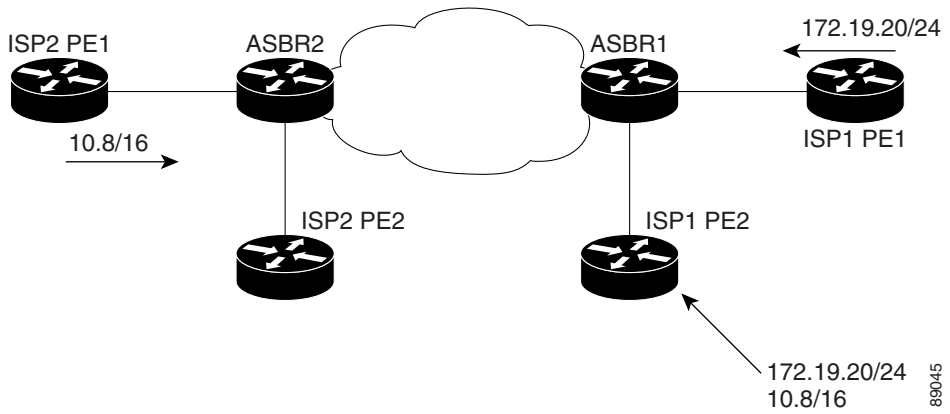
アドバタイズされる単一のパスには、次のように集約コスト コミュニティが含まれます。

- {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

図 1 に、エッジに 2 つの Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）がある Interior Gateway Protocol（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 1　　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 ロードシェアリングが設定されていない場合、BGP により最初に最良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 間のリンクは低速です。

コスト コミュニティ アトリビュート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 最良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。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）。

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「プレ最良パス」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 ルートに適用されます。「プレ最良パス」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、最良パス計算プロセスに作用します。コンフィギュレーションは必要ありません。Cisco IOS Release 12.0(27)S が Provider Edge（PE; プロバイダー エッジ）、Customer Edge（CE; カスタマーエッジ）、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 拠点に対してイネーブルになります。

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

ここでは、次の手順について説明します。

- 「BGP コスト コミュニティの設定」（P.6）
- 「BGP コスト コミュニティの設定確認」（P.7）

BGP コスト コミュニティの設定

コスト コミュニティを設定するには、このセクションの手順を実行してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **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：** `Router> enable`	特権 EXEC モードなどの上位の特権レベル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。
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	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *ip-address* **route-map** *map-name* {**in** | **out**} **例：** `Router(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：** `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 8	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] **例：** `Router(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：** `Router(config-route-map)# set extcommunity cost 1 100`	set 句を作成しコスト コミュニティ アトリビュートを適用します。 • 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。その他すべてのアトリビュートが等しい場合、最も低い*コスト値*を持つ cost community set 句が最良パス選択プロセスにより優先されます。 • コスト コミュニティ アトリビュートが設定されていないパスにはデフォルトの*コスト値*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：** `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。

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。「BGP コスト コミュニティの設定確認」（P.7）に出力の具体例を示します。

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 アトリビュートの評価をディセーブルにし、BGP 最良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 アトリビュート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。外部ピアから非遷移の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

次に、この機能のコンフィギュレーションおよび検証の例を示します。

- 「BGP コスト コミュニティ設定例」（P.8）
- 「BGP コスト コミュニティ検証例」（P.8）

BGP コスト コミュニティ設定例

次に、**set extcommunity cost** コマンドによるコンフィギュレーションの例を示します。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、最良パス選択プロセスにより優先されます。

```
Router(config)# router bgp 50000
Router(config-router)# neighbor 10.0.0.1 remote-as 50000
Router(config-router)# neighbor 10.0.0.1 update-source Loopback 0
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.1 activate
Router(config-router-af)# neighbor 10.0.0.1 route-map COST1 in
Router(config-router-af)# neighbor 10.0.0.1 send-community both
Router(config-router-af)# exit
Router(config)# route-map COST1 permit 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# set extcommunity cost 1 100
```

BGP コスト コミュニティ検証例

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 アトリビュートのステータスおよびアトリビュートが表示されます。次の出力例は、表示される出力に類似しています。

```
Router# 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。

```
Router# 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。

```
Router# 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 アトリビュートを設定したパスを伝送するかを確認する際に使用できます。コスト コミュニティ アトリビュート情報は、「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。

```
Router# 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。

次の作業

EIGRP MPLS VPN PE-CE Site of Origin（SoO）機能についての詳細は、Cisco IOS Release 12.0(27)S で追加された『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。

参考資料

BGP コスト コミュニティ機能に関する詳細情報については、次の資料を参照してください。

関連資料

関連項目	参照先
BGP 最良パスの選択	『*BGP Best Path Selection Algorithm*』
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
設定作業および設定例を含む BGP モジュールおよび機能のロードマップ	『*BGP Features Roadmap*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	プラットフォームおよび Cisco IOS リリースでサポートされる MIB のリストを入手して、MIB モジュールをダウンロードするには、次の URL にある Cisco.com の Cisco MIB Web サイト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
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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

- **bgp bestpath cost-community ignore**
- **debug ip bgp updates**
- **set extcommunity cost**

BGP コスト コミュニティの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。このテーブルには、Cisco IOS Release 12.0(24)S、Cisco IOS Release 12.3(2)T、12.2(18)S またはそれ以降のリリースで導入または変更された新しい機能だけが記載されています。

このテクノロジーの機能でここに記載されていない情報については、『BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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 アトリビュートが導入されます。コスト コミュニティとは、非遷移の拡張コミュニティ アトリビュートで、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、最良パス選択プロセスに反映させることができます。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP コスト コミュニティの概要」（P.2） • 「BGP コスト コミュニティはどのように最良パス選択プロセスに影響するか」（P.3） • 「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」（P.4） • 「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」（P.4） • 「BGP コスト コミュニティ機能の設定方法」（P.5） • 「BGP コスト コミュニティ機能の設定例」（P.8） **bgp bestpath cost-community ignore**、**debug ip bgp updates**、**set extcommunity cost** の各コマンドが追加または変更されています。

表 1　BGP コスト コミュニティの機能情報 （続き）

機能名	リリース	機能情報
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「プレ最良パス」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。コンフィギュレーションは必要ありません。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 拠点に対してイネーブルになります。 次のセクションで、この機能に関する情報を参照できます。 • 「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」（P.5） 追加または変更されたコマンドはありません。

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 プレフィクスをグローバル ルーティング テーブルから Virtual Private Network（VPN; バーチャル プライベート ネットワーク）routing/forwarding（VRF; VPN ルーティング/転送）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。

このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの機能情報」（P.14）を参照してください。

プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの前提条件

- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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イネーブル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 プレフィクスは、VPNv4 VRF に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 プレフィクスおよび IPv4 マルチキャスト プレフィクスの両方がサポートされています。Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）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 プレフィクスは、標準の Cisco IOS 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 プレフィクスまたは IP プレフィ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

この機能は、Black Hole Routing（BHR; ブラック ホール ルーティング）をサポートするために設定できます。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 Denial of Service（DoS; サービス拒絶）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

この機能を使用すると、物理的な位置またはサービスのクラスに基づいてグローバル IP トラフィックを分類できます。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。

グローバル テーブルから VRF テーブルへの IP プレフィクスのインポート方法

ここでは、次の作業について説明します。

インポートする IPv4 IP プレフィクスの定義

IPv4 ユニキャストまたは IPv4 マルチキャストのプレフィクスは、標準の Cisco IOS 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：** `Router> enable`	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。
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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**] **例：** `Router(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：** `Router(config)# ip prefix-list COLORADO permit 10.24.240.0/22`	プレフィクス 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 ごとに 1000 のプレフィクスがインポートされます。各 VRF に対して、1 ～ 2,147,483,647 のプレフィクスを手動で設定できます。プレフィクス インポートの制限を手動で設定する場合は、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

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クスが受信と同時にインポートされます。

新しい syslog メッセージ

この機能によって、次の syslog メッセージが追加されています。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。

制約事項

- 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。
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 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：** `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`	インポート マップを作成し、グローバル ルーティング テーブルから IPv4 プレフィクスを VRF テーブルにインポートします。 • ユニキャスト プレフィクスまたはマルチキャスト プレフィクスを指定します。 • デフォルトでは、最大 1000 のプレフィクスがインポートされます。1 ～ 2,147,483,647 のプレフィクスの制限を指定するには、*prefix-limit* 引数を使用します。 • インポートするプレフィクスを定義するルート マップは、**map** キーワードの入力後に指定されます。 • この例では、UNICAST という名前のルート マップを通過する最大 1000 のユニキャスト プレフィクスをインポートするインポート マップを作成しています。
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`	ルートを、あるルーティング プロトコルから別のルーティング プロトコルに再配布する条件を定義したり、ポリシー ルーティングをイネーブルにしたりします。 • 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。

	コマンドまたはアクション	目的
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*]} **例：** `Router(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

この機能は、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。

ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）

ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）は任意に設定できます。ユニキャスト RPF は、送信元アドレスが Forwarding Information Base（FIB; 転送情報ベース）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 でイネーブルにされます。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。

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。
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のポリシー ルーティングに使用するルート マップを識別します。 • 設定例では、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 プレフィクス インポートの確認

次の作業の手順を実行すると、この機能で設定された VRF に関する情報が表示され、指定された VRF テーブルにグローバル IP プレフィクスがインポートされていることを確認できます。

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。

```
Router# 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クス インポート制限、インポートされた実際のプレフィクスの数、および個別のインポート プレフィクス エントリが表示されます。

```
Router# 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 プレフィクスをインポートしており、プレフィクス インポート リミットが 1000 であることを示します。

```
Router# 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 プレフィクス インポートに対する BGP サポートの設定例

ここでは、次の設定例について説明します。

- 「グローバル IP プレフィクス インポートの設定：例」（P.10）
- 「グローバル IP プレフィクス インポートの確認：例」（P.10）

グローバル IP プレフィクス インポートの設定：例

次に、IP プレフィクス 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
```

グローバル IP プレフィクス インポートの確認：例

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。

次の例は **show ip vrf** コマンドの出力であり、UNICAST という名前のインポート ルート マップが IPv4 ユニキャストをインポートしており、プレフィクス インポート リミットが 1000 であることを示します。

```
Router# 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
```

次の例は **show ip bgp vpnv4** コマンドの出力であり、インポート ルート マップ名、プレフィクス インポート制限、インポートされたプレフィクスの実際の数、および個別のインポート エントリを示します。

```
Router# 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
```

参考資料

次のセクションでは、グローバル テーブルから VRF テーブルへの IP プレフィクスのインポートに対する BGP サポート機能に関連する参照資料について説明します。

関連資料

関連項目	参照先
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*』
BGP 機能のロードマップと、機能およびコンフィギュレーション モジュールへのリンク	『BGP Features Roadmap』
MPLS レイヤ 3 VPN の設定作業	『Configuring MPLS Layer 3 VPNs』
ポリシーベース ルーティングを使用した VRF 選択	『Directing MPLS VPN Traffic Using Policy-Based Routing』
送信元 IP アドレスに基づく VRF の選択	『MPLS VPN— VRF Selection Based on Source IP Address』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

- **debug ip bgp import**
- **import ipv4**
- **ip verify unicast vrf**

グローバル テーブルから VRF テーブルへの IP プレフィクス インポートに対する BGP サポートの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　グローバル テーブルから VRF テーブルへの IP プレフィクス 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 プレフィクスのインポートに対する BGP サポート	12.0(29)S 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.3(14)T 15.0(1)S	グローバル テーブルから VRF テーブルへの IP プレフィ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。 この機能によって、**debug ip bgp import**、**import ipv4**、**ip verify unicast vrf** の各コマンドが追加または変更されています。

BGP のネイバーごとの SoO 設定

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。Cisco IOS Release 12.4(9)T、12.2(33)SRA、12.2(31)SB2、およびこれら以前のリリースでは、SoO 値は、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。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。Cisco IOS Release 12.4(24)T では、4 バイト自律システム番号の asdot 形式に限りサポートが追加されました。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP のネイバーごとの SoO 設定の機能情報」（P.19）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

- 「BGP のネイバーごとの SoO 設定の機能情報」（P.19）

- 「BGP のネイバーごとの SoO 設定の機能情報」（P.19）

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（CEF）がご使用のネットワークでイネーブル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

BGP ネイバーの SoO 値を設定する前に、次の概念を理解しておく必要があります。

- 「Site of Origin BGP コミュニティ アトリビュート」（P.2）
- 「4 バイト自律システム番号に対する BGP サポート」（P.2）
- 「BGP によるネイバーごとの Site of Origin の設定」（P.3）
- 「BGP のネイバーごとの Site of Origin の利点」（P.4）

Site of Origin BGP コミュニティ アトリビュート

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 アトリビュートです。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。

4 バイト自律システム番号に対する BGP サポート

Cisco IOS Release 12.4(24)T では、RFC 5396 の『*Textual Representation of Autonomous System (AS) Numbers*』で説明されているとおり、4 バイト自律システム番号のサポートが追加されました。
Cisco IOS Release 12.4(24)T では、4 バイト自律システム番号の Cisco による実装は、設定形式、正規表現一致、および出力表示として asdot 表記（1.2 など）だけを使用し、asplain 形式はサポートしません。

Cisco IOS Release 12.2(33)SRE、12.2(33)XNE、およびこれら以降のリリースでは、デフォルト形式として asplain 形式を使用する 4 オクテット（4 バイト）自律システム番号に対する BGP サポートが導入されました。デフォルトの asplain 形式は、65536 などの 10 進数値を使用しますが、4 バイト自律システム番号を asplain 形式と asdot 形式の両方で設定できます。デフォルトの **show** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、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。

4 バイト自律システム番号に関する設定例については、「BGP ピア ポリシー テンプレートを使用し、4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.16）または「BGP ネイバー コマンドおよび 4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.17）を参照してください。

BGP 自律システム番号形式の Cisco による実装の詳細については、「Cisco BGP Overview」モジュールを参照してください。

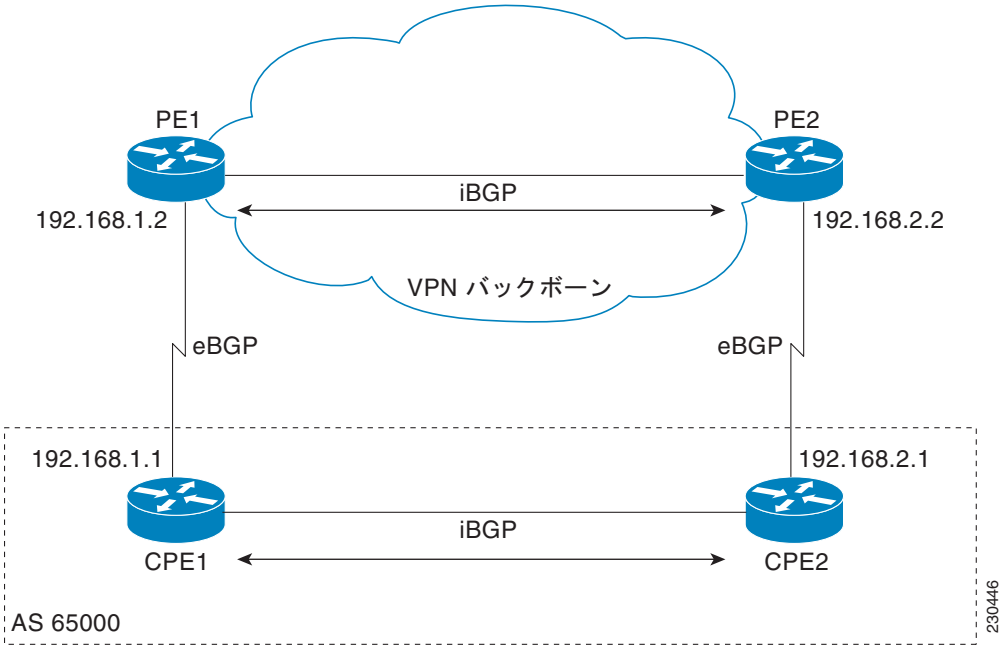
BGP によるネイバーごとの Site of Origin の設定

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 Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）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。

BGP ネイバーに対する SoO 値の設定は、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の入り口である Provider Edge（PE; プロバイダー エッジ）ルータで実行されます。SoO がイネーブルになると、プレフィクスの SoO タグが Customer Premises Equipment（CPE; 顧客宅内機器）用に設定された SoO タグと一致しない場合だけ PE ルータがプレフィクスを CPE に転送します。たとえば、図 1 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 がプレフィクスを PE1 に送信すると、PE1 は、このプレフィクスに 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 1　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

Cisco IOS Release 12.4(11)T、12.2(33)SRB、および 12.2(33)SB 以前のリリースでは、SoO 拡張コミュニティ アトリビュートは、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。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される 2 つの新しいコマンドの導入により、SoO 値の設定が簡素化されます。

BGP のネイバーごとの SoO の設定方法

BGP ネイバーに SoO 値を設定するには、次のリストの最初の作業およびその次の 3 つの作業のいずれかを実行する必要があります。最後の 3 つの作業は、相互に排他的な関係です。これらのうち 1 つだけを実行する必要があります。

- 「CEF の確認および VRF インスタンスの設定」（P.4）
- 「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」（P.8）
- 「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」（P.11）
- 「BGP ピア グループを使用したネイバーごとの SoO 値の設定」（P.13）

CEF の確認および VRF インスタンスの設定

次の作業を図 1 の両方の PE ルータで実行し、仮想ルーティング/転送（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、CEF がイネーブルであることが確認された後、SOO_VRF という名前の VRF インスタンスが設定されます。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。

ルート識別子

Route Distinguisher（RD; ルート識別子）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 プレフィクスをグローバルに固有の VPN-IPv4 プレフィクスに変更するために、RD が IPv4 プレフィ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

手順の概要

1. **enable**
2. **show ip cef**
3. **configure terminal**
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **route-target** {**import** | **both**} *route-target-ext-community*
7. **route-target** {**export** | **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：** `Router> enable`	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。
ステップ 2	**show ip cef** **例：** `Router# show ip cef`	CEF がイネーブルであることを確認します。 • CEF は、ほとんどの Cisco IOS リリースで、デフォルトでイネーブルになっています。 • CEF がイネーブルでない場合、**ip cef** コマンドをグローバル コンフィギュレーション モードで入力します。一部のプラットフォームでは、このコマンドとともに追加のキーワードが必要です。詳細については、『*Cisco IOS IP Switching Command Reference*』を参照してください。
ステップ 3	**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 4	**ip vrf** *vrf-name* **例：** `Router(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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 6	**route-target** {**export** | **both**} *route-target-ext-community* **例：** `Router(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、ステップ 7 を参照してください。
ステップ 7	**route-target** {**import** | **both**} *route-target-ext-community* **例：** `Router(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：** `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 9	**interface** *type number* **例：** `Router(config)# interface Ethernet 1/0`	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、イーサネット インターフェイス 1/0 が設定されます。
ステップ 10	**ip vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] **例：** `Router(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 がイーサネット インターフェイス 1/0 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：** `Router(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、イーサネット インターフェイス 1/0 が IP アドレス 192.168.1.2 によって設定されます。

	コマンドまたはアクション	目的
ステップ 12	**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 13	**show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*] **例：** `Router# 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。

```
Router# show ip vrf

Name                                     Default RD          Interfaces
SOO_VRF                                  1:1                 Eth1/0
```

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

次の作業を図 1 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、図 1 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。

4 バイト自律システム番号に関する設定例については、「BGP ピア ポリシー テンプレートを使用し、4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.16）を参照してください。

（注） 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。

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、「Configuring a Basic BGP Network」モジュールを参照してください。

前提条件

この作業は、「CEF の確認および VRF インスタンスの設定」（P.4）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。

制約事項

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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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。

	コマンドまたはアクション	目的
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）。 – 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、キーワード **unicast** 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 プレフィクスを指定するには、**multicast** キーワードを使用します。 • 後続する 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 インスタンス名を指定するには、**vrf** キーワードと *vrf-name* 引数を使用します。
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クスをローカル ルータと交換します。

	コマンドまたはアクション	目的
ステップ 10	**neighbor** *ip-address* **inherit peer-policy** *policy-template-name* **例：** `Router(config-router-af)# neighbor 192.168.1.1 inherit peer-policy SOO_POLICY`	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、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

次の作業を図 1 のルータ PE2 で実行し、**neighbor** コマンドを使用して、図 1 のルータ CPE2 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。

4 バイト自律システム番号に関する設定例については、「BGP ネイバー コマンドおよび 4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.17）を参照してください。

（注） 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。

前提条件

この作業は、「CEF の確認および VRF インスタンスの設定」（P.4）で説明された作業が適切な変更を加えてインターフェイスおよび IP アドレスに対し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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**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、キーワード **unicast** 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 プレフィクスを指定するには、**multicast** キーワードを使用します。 • 後続する 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 インスタンス名を指定するには、**vrf** キーワードと *vrf-name* 引数を使用します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(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。
ステップ 6	**neighbor** *ip-address* **activate** **例：** `Router(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 グループがステップ 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、このステップは行わないでください。たとえば、BGP ピア グループは、ステップ 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。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **soo** *extended-community-value* **例：** `Router(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：** `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 グループを使用したネイバーごとの SoO 値の設定

この作業を図 1 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、図 1 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。

（注） 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。

前提条件

この作業は、「CEF の確認および VRF インスタンスの設定」（P.4）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。

制約事項

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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**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、キーワード **unicast** 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 プレフィクスを指定するには、**multicast** キーワードを使用します。 • 後続する 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 インスタンス名を指定するには、**vrf** キーワードと *vrf-name* 引数を使用します。
ステップ 5	**neighbor** *peer-group-name* **peer-group** **例：** `Router(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：** `Router(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：** `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。

	コマンドまたはアクション	目的
ステップ 8	**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：** `Router(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：** `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 のネイバーごとの SoO 設定の設定例

ここでは、次の設定例について説明します。

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：例

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。CEF がイネーブルであることを確認し、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。アドレス ファミリ IPv4 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。

```
show ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface Ethernet 1/0
 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
```

BGP ピア ポリシー テンプレートを使用し、4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例

次に、ピア ポリシー テンプレートを作成し、4 バイト自律システム番号（asdot 形式の 1.2）を使用して 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。アドレス ファミリ IPv4 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。この例では、Cisco IOS Release 12.4(24)T、または以降のリリースが必要です。

```
router bgp 1.2
 template peer-policy SOO_POLICY
  soo 1.2:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

次に、ピア ポリシー テンプレートを作成し、4 バイト自律システム番号（asplain 形式の 65538）を使用して 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。アドレス ファミリ IPv4 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。この例では、Cisco IOS Release 12.2(33)SRE、12.2(33)XNE、または以降のリリースが必要です。

```
router bgp 65538
 template peer-policy SOO_POLICY
  soo 65538:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 65550
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

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：例

次に、BGP ネイバーに SoO 値を設定する方法の例を示します。CEF がイネーブルであることを確認後、SOO_VRF という名前の VRF インスタンスが設定され、ネイバーがアドレス ファミリ IPv4 VRF の下で特定され、SoO 値がこのネイバーに設定されます。

```
show ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface Ethernet 1/0
 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
```

BGP ネイバー コマンドおよび 4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例

次に、BGP ネイバーに SoO 値を設定する方法の例を示します。この例では、すべての BGP ネイバー、ルート ターゲット、および SoO 値が 4 バイト自律システム番号を asplain 形式で使用します。CEF がイネーブルであることが確認された後、SOO_VRF という名前の VRF インスタンスがルート ターゲットによって設定されます。BGP ルータ セッションでネイバーがアドレス ファミリ IPv4 VRF の下で特定され、SoO 値がこのネイバーに設定されます。この例では、Cisco IOS Release 12.4(24)T、または以降のリリースが必要です。

```
show ip cef
ip vrf SOO_VRF
 rd 100:200
 route-target export 1.14:1
 route-target import 1.14:1
 exit
interface Ethernet 1/0
 ip vrf forwarding SOO_VRF
 ip address 192.168.2.2 255.255.255.0
 exit
router bgp 1.2
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.2.1 remote-as 1.14
  neighbor 192.168.2.1 activate
  neighbor 192.168.2.1 soo 1.14:1
  end
```

BGP ピア グループを使用したネイバーごとの SoO 値の設定：例

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。CEF がイネーブルであることを確認後、SOO_VRF という名前の VRF インスタンスが設定され、BGP ピア グループがアドレス ファミリ IPv4 VRF の下に設定され、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。

```
show ip cef
ip vrf SOO_VRF
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit
interface Ethernet 1/0
 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 の概要を表示するには、「Cisco BGP Overview」モジュールに進みます。
- 基本的な BGP 機能の作業を実行するには、「Configuring a Basic BGP Network」モジュールに進みます。
- BGP の拡張機能の作業を実行するには、「Configuring Advanced BGP Features」モジュールに進みます。
- BGP ネイバー セッションのオプションを設定するには、「Configuring BGP Neighbor Session Options」モジュールに進みます。
- 内部 BGP 作業を実行するには、「Configuring Internal BGP Features」モジュールに進みます。

参考資料

ここでは、ネイバーごとの SoO 設定に対する BGP サポート機能に関連する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands 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*』
IP 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、コマンド履歴、使用上の注意事項、例）	『*Cisco IOS IP Switching Command Reference*』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 1 に、この機能のリリース履歴を示します。

このテクノロジーの機能でここに記載されていないものについては、『BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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	12.2(33)SB 12.2(33)SRB 12.4(11)T	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。Cisco IOS Release 12.4(9)T、12.2(33)SRA、12.2(31)SB2、およびこれら以前のリリースでは、SoO パラメータは、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。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。 次のコマンドがこの機能によって導入されました。**neighbor soo**、**soo**。
4 バイト ASN に対する BGP サポート	12.0(32)S12 12.0(32)SY8 12.2(33)SRE 12.2(33)XNE 12.4(24)T	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、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）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す。 Cisco IOS Release 12.0(32)SY8、12.2(33)SRE、および 12.2(33)XNE では、4 バイト自律システム番号の Cisco による実装は、自律システム番号のデフォルトの正規表現一致および出力表示形式として asplain 形式を使用しますが、RFC 5396 で説明されているように、4 バイト自律システム番号を asplain 形式と asdot 形式の両方に設定できます。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** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「4 バイト自律システム番号に対する BGP サポート」（P.2） • 「BGP ピア ポリシー テンプレートを使用し、4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.16） • 「BGP ネイバー コマンドおよび 4 バイト自律システム番号を使用したネイバーごとの SoO 値の設定：例」（P.17） 次のコマンドがこの機能によって変更されました。**bgp asnotation dot**、**bgp confederation identifier**、**bgp confederation peers**、**clear ip bgp**、**ip bgp-community new-format**、**ip extcommunity-list**、**match source-protocol**、**neighbor local-as**、**neighbor remote-as**、**neighbor soo**、**redistribute**（IP）、**router bgp**、**set as-path**、**set extcommunity**、**set origin**、**soo**、および自律システム番号を表示するすべての **show ip bgp** コマンド。

BGP ネクストホップ伝播

BGP ネクストホップ伝播機能により、ネットワークの設計およびマイグレーションを行うときの柔軟性が高まります。BGP ネクストホップ伝播機能では、反映されたルートのネクストホップ アトリビュートをルート リフレクタによって変更でき、ネクストホップ アトリビュートを変更せずに Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）によって external BGP（eBGP; 外部 BGP）マルチホップ ピアにアップデートを送信できます。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP ネクストホップ伝播の機能情報」（P.11）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

BGP ネクストホップ伝播の前提条件

- BGP ピアリングが確立され、ネクストホップにアクセス可能である必要があります。

BGP ネクストホップ伝播の制約事項

- BGP ネクストホップ伝播は、マルチホップ eBGP ピア間だけで設定できます。直接接続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
  ```

- この機能がルート リフレクタ クライアントに対してイネーブルにされているときは、**neighbor next-hop-self** コマンドを使用してルート リフレクタのネクストホップ アトリビュートを変更しないでください。ルート リフレクタで **neighbor next-hop-self** コマンドを使用すると、eBGP ピアから学習したルートのネクストホップ アトリビュートだけが変更され、ルート リフレクタ クライアントから反映された意図したルートは変更されません。ルートを反映するときにネクストホップ アトリビュートを変更するには、アウトバウンド ルート マップを使用します。

ネクストホップ伝播に関する情報

ここでは次の概念について説明します。

- 「BGP ネクストホップ伝播の概要」（P.2）
- 「BGP ネクストホップ伝播の利点」（P.2）

BGP ネクストホップ伝播の概要

BGP ネクストホップ伝播機能により、ネットワークの設計およびマイグレーションを行うときの柔軟性が高まります。BGP ネクストホップ伝播機能では、反映されたルートのネクストホップ アトリビュートをルート リフレクタによって変更でき、ネクストホップ アトリビュートを変更せずに 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。

注意 ルート リフレクタの BGP アトリビュート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、または接続の損失が発生する可能性があります。ルート リフレクタの BGP アトリビュートの設定は、経験豊富なネットワーク オペレータだけが行う必要があります。

この機能を internal BGP（iBGP; 内部 BGP）マルチパス ロード シェアリング機能とあわせて設定すると、アウトバウンド ルート マップを使用して BGP ルート リフレクタを転送パスに含めることができます。

BGP ネクストホップ伝播の利点

BGP ネクストホップ伝播機能によって、次の作業を実行できます。

- ルート リフレクタを転送パスに含めます。これを iBGP マルチパス ロード シェアリング機能と一緒に使用してロード バランシングを設定できます。

- eBGP ピアにルートをアドバタイズするとき、ネクストホップ アトリビュートを変更しないことによって、プロバイダー間の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を設定します。
- eBGP ピアのネクストホップ計算をオフにします。この機能は、ラベル スイッチド パスのエンドツーエンド接続の設定に役立ちます。

BGP ネクストホップ伝播の設定方法

ここでの最初の 2 つの作業は必須で、3 番目の作業は任意です。

- 「ルート リフレクタの設定」（P.3）（必須）
- 「ルート リフレクタ クライアントの設定」（P.5）（必須）
- 「BGP ネクストホップ伝播の確認」（P.7）（任意）

ルート リフレクタの設定

ここでは、次の作業を完了します。

- ルート マップを作成して、ルート リフレクタ クライアントにアドバタイズされるネクストホップを設定します。ルート マップはアウトバウンド ルートだけに適用されます。
- ルート リフレクタ クライアントとの eBGP ピアリングを設定します。

制約事項

この機能がルート リフレクタ クライアントに対してイネーブルにされているときは、**neighbor next-hop-self** コマンドを使用してルート リフレクタのネクストホップ アトリビュートを変更しないでください。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **set ip next-hop** *ip-address* [**peer-address**]
5. **exit**
6. **router bgp** *as-number*
7. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
8. **neighbor** *ip-address* **activate**
9. **neighbor** *ip-address* **ebgp-multihop** *ttl*
10. **neighbor** *ip-address* **route-reflector-client**
11. **neighbor** *ip-address* **route-map** *map-tag* **in** | **out**
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。
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** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map NEXTHOP`	ルート マップ コンフィギュレーション モードを開始して、ルート マップを作成または設定します。 • 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* [*peer-address*] **例：** `Router(config-route-map)# set ip next-hop 172.16.0.1`	ネクストホップを指定します。
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 6	**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 7	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **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	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 10.0.0.100 activate`	アドレス ファミリ ピアとの情報の交換をイネーブルにします。
ステップ 9	**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 10	**neighbor** *ip-address* **route-reflector-client** **例：** `Router(config-router-af)# neighbor 10.0.0.100 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。

	コマンドまたはアクション	目的
ステップ 11	**neighbor** *ip-address* **route-map** *map-name* **out** **例：** `Router(config-router-af)# neighbor 10.0.0.100 route-map NEXTHOP out`	ルート マップを発信ルートに適用します。
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。

例

次に、グローバル コンフィギュレーション モードから開始して、ローカル ルータをルート リフレクタに設定し、10.0.0.100 マルチホップ ピアをルート リフレクタ クライアントに設定する例を示します。ルート マップが作成され、アドバタイズされるネクストホップを 172.16.0.1 に設定します。

```
route-map NEXTHOP
 set ip next-hop 172.16.0.1
 exit
router bgp 65535
 address-family ipv4
 neighbor 10.0.0.100 activate
 neighbor 10.0.0.100 ebgp-multihop 255
 neighbor 10.0.0.100 route-reflector-client
 neighbor 10.0.0.100 route-map NEXTHOP out
 end
```

次の作業

この設定を完了するには、**neighbor next-hop-unchanged** コマンドをルート リフレクタ クライアントに設定します。詳細については、次のセクションに進みます。

ルート リフレクタ クライアントの設定

ここでは、次の作業を完了します。

- ルート リフレクタとの eBGP ピアリングを設定します。
- next-hop-unchanged を伝播するようにルート リフレクタ クライアントを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **activate**
6. **neighbor** *ip-address* **ebgp-multihop** *ttl*
7. **neighbor** *ip-address* **next-hop-unchanged**
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。
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 65412`	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** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **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 5	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 192.168.0.1 activate`	アドレス ファミリ ピアとの情報の交換をイネーブルにします。
ステップ 6	**neighbor** *ip-address* **ebgp-multihop** *ttl* **例：** `Router(config-router-af)# neighbor 192.168.0.1 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 7	**neighbor** *ip-address* **next-hop-unchanged** **例：** `Router(config-router-af)# neighbor 192.168.0.1 next-hop-unchanged`	ルータを設定して、ネクストホップ アトリビュートを変更せずに BGP ピアに BGP アップデートを送信するように設定します。
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 モードを開始します。

例

次に、グローバル コンフィギュレーション モードから開始して、ローカル ルータ（ルート リフレクタ クライアント）を設定し、ルート リフレクタとのピアリングの確立および next-hop-unchanged の伝播を行う例を示します。

```
router bgp 65412
 address-family ipv4
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.1 ebgp-multihop 255
 neighbor 192.168.0.1 next-hop-unchanged
 end
```

次の作業

次のセクションに進んで、BGP ネクストホップ伝播機能の設定を確認するために使用できるコマンドを参照します。

BGP ネクストホップ伝播の確認

BGP ネクストホップ伝播機能の設定は、**show ip bgp neighbors** EXEC コマンドで確認できます。

手順の概要

1. **enable**
2. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | {**paths** *regexp*} | **dampened-routes** | **received prefix-filter**]]
3. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-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：** `Router> enable`	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。
ステップ 2	**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 接続についての情報を表示します。出力には BGP ネクストホップ伝播機能のステータスが表示されます。
ステップ 3	**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。表示される出力には、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。

BGP ネクストホップ伝播の設定例

次に、この機能を設定する例を示します。

- 「ルート リフレクタ：例」（P.8）
- 「ルート リフレクタ クライアント：例」（P.8）

ルート リフレクタ：例

次に、グローバル コンフィギュレーション モードから開始して、ローカル ルータをルート リフレクタに設定し、10.0.0.100 マルチホップ ピアをルート リフレクタ クライアントに設定する例を示します。ルート マップが作成され、アドバタイズされるネクストホップを 172.16.0.1 に設定します。

```
route-map NEXTHOP
 set ip next-hop 172.16.0.1
 exit
router bgp 65535
 address-family ipv4
 neighbor 10.0.0.100 activate
 neighbor 10.0.0.100 ebgp-multihop 255
 neighbor 10.0.0.100 route-reflector-client
 neighbor 10.0.0.100 route-map NEXTHOP out
 end
```

ルート リフレクタ クライアント：例

次に、グローバル コンフィギュレーション モードから開始して、ローカル ルータ（ルート リフレクタ クライアント）を設定し、ルート リフレクタとのピアリングの確立および next-hop-unchanged の伝播を行う例を示します。

```
router bgp 65412
 address-family ipv4
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.1 ebgp-multihop 255
 neighbor 192.168.0.1 next-hop-unchanged
 end
```

参考資料

次のセクションでは、BGP ネクストホップ伝播機能に関連する参考資料を示します。

関連資料

関連項目	参照先
BGP コマンドおよび設定作業：BGP ネクストホップ伝播機能は BGP ルーティング プロトコルの拡張機能です。BGP、ルート リフレクタ、経路集約、およびフィルタリングの設定に関する情報。	• 『*Cisco IOS IP Routing: BGP Command Reference*』 • 「Configuring Internal BGP Features」モジュール
iBGP マルチパス ロードシェアリング：内部 BGP（iBGP）マルチパス ロードシェアリング設定およびコマンド リファレンス情報。	• 『iBGP Multipath Load Sharing』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にアクセスしてコマンド検索ツールを使用するか、『*Cisco IOS Master Commands List*』を参照してください。

- **neighbor next-hop-unchanged**

BGP ネクストホップ伝播の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 12.2(1)、12.0(3)S、12.2(27)SBC、12.2(33)SRB、12.2(33)SXH、またはそれ以降のリリースで追加または変更された機能だけが表に示されています。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　BGP ネクストホップ伝播の機能情報

機能名	リリース	機能の設定情報
BGP ネクストホップ伝播	12.0(22)S 12.0(16)ST 12.2 12.2(14)S 15.0(1)S	BGP ネクストホップ伝播機能により、ネットワークの設計およびマイグレーションを行うときの柔軟性が高まります。BGP ネクストホップ伝播機能では、反映されたルートのネクストホップ アトリビュートをルート リフレクタによって変更でき、ネクストホップ アトリビュートを変更せずに Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）によって external BGP（eBGP; 外部 BGP）マルチホップ ピアにアップデートを送信できます。 この機能によって次のコマンドが追加または変更されました。**neighbor next-hop-unchanged**

BGP ルータ ID の VRF 単位の割り当て

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 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、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に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP ルータ ID の VRF 単位での割り当てに関する機能情報」（P.26）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

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（CEF; シスコ エクスプレス フォワーディング）または distributed CEF（dCEF; 分散 CEF）がイネーブル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 を使用して VRF 単位でルータ ID を割り当てるには、次の概念を理解する必要があります。

- 「BGP ルータ ID」（P.2）
- 「VRF 単位でのルータ ID の割り当て」（P.2）

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最良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、最良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 Release 12.2(31)SB2、12.2(33)SRA、12.2(33)SXH、12.4(20)T、およびこれ以降のリリースでは、各 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）routing/forwarding（VRF; VPN ルーティング/転送）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。

BGP ルータ ID の VRF 単位での割り当ての設定方法

各 VRF に BGP ルータ ID を設定するには、主に 2 つの方法があります。VRF 単位で BGP ルータ ID を手動で設定するには、まず、次に示される最初の 3 つの作業を実行する必要があります。自動的に BGP ルータ ID を各 VRF に割り当てるには、最初の作業と 4 番目の作業を実行する必要があります。ここでは、次の作業について説明します。

- 「VRF インスタンスの設定」（P.3）
- 「VRF インスタンスとインターフェイスの関連付け」（P.4）
- 「VRF 単位での BGP ルータ ID の手動設定」（P.7）
- 「VRF 単位での BGP ルータ ID の自動割り当て」（P.11）

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、Route Distinguisher（RD; ルート識別子）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。

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 プレフィクスをグローバルに固有の VPN-IPv4 プレフィクスに変更するために、RD が IPv4 プレフィ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

前提条件

この作業は、CEF または dCEF をイネーブルにし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。
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」（P.3）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 拡張コミュニティとの間でルーティング情報のインポートとエクスポートの両方を実行するには、**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 拡張コミュニティとの間でルーティング情報のインポートとエクスポートの両方を実行するには、**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 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。

（注） **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。

前提条件

- この作業は、CEF または dCEF をイネーブルにし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」（P.3）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。
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。

	コマンドまたはアクション	目的
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`	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 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 がシリアル インターフェイス 2/0 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。
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 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。

前提条件

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」（P.3）および「VRF インスタンスとインターフェイスの関連付け」（P.4）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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 ファミリをディセーブルにします。 **（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イネーブルにします。
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 アトリビュートが 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 アトリビュートが 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 がイネーブルに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 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。

	コマンドまたはアクション	目的
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 アトリビュート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追加しない場合は、**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に存在する外部ピアへの BGP 接続の受け入れと試行を行います。 • 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。
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`	自動サマライズをディセーブルにし、サブプレフィクス 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 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することをイネーブルにします。
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。	—

	コマンドまたはアクション	目的
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。 **（注）** この例では、この作業に適用される構文だけが使用されます。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。

前提条件

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」（P.3）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。
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* **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 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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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。

	コマンドまたはアクション	目的
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 ファミリをディセーブルにします。 **（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イネーブルにします。
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。
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。

	コマンドまたはアクション	目的
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 アトリビュートが 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 アトリビュートが 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：** `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 がイネーブルに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 アトリビュート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追加しない場合は、**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。

	コマンドまたはアクション	目的
ステップ 25	**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に存在する外部ピアへの BGP 接続の受け入れと試行を行います。 • 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 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クスをすべて再アドバタイズできるように、Provider Edge（PE; プロバイダー エッジ）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`	自動サマライズをディセーブルにし、サブプレフィクス 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 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することをイネーブルにします。
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。 **（注）** この例では、この作業に適用される構文だけが使用されます。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

ここでは、次の設定例について説明します。

- 「VRF 単位での BGP ルータ ID の手動設定：例」（P.17）
- 「VRF 単位での BGP ルータ ID の自動割り当て：例」（P.20）

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
!
interface Ethernet0/0
 ip vrf forwarding vrf_trans
 ip address 172.22.1.1 255.255.0.0
```

```
!
interface Ethernet1/0
 ip vrf forwarding vrf_user
 ip address 172.23.1.1 255.255.0.0
!
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」（P.20）
- 「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」（P.21）
- 「VRF 単位で自動割り当てされるルータ ID」（P.22）

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

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
!
interface Ethernet0/0
 ip vrf forwarding vrf_trans
 ip address 172.22.1.1 255.0.0.0
!
interface Ethernet1/0
 ip vrf forwarding vrf_user
 ip address 172.23.1.1 255.0.0.0
!
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」（P.17）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

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
!
interface Ethernet0/0
 ip vrf forwarding vpn1
 ip address 172.22.1.1 255.0.0.0
!
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
Ethernet0/0            172.22.1.1      YES NVRAM  up                    up
Ethernet1/0            unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial3/0              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
                                                        Ethernet0/0
VRF session is established:
```

VRF 単位で自動割り当てされるルータ ID

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** コマンドの出力を使用すると、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
!
interface Ethernet0/0
 ip vrf forwarding vrf_trans
 ip address 172.22.1.1 255.0.0.0
!
interface Ethernet1/0
 ip vrf forwarding vrf_user
 ip address 172.23.1.1 255.0.0.0
!
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 ?
```

参考資料

次の項では、BGP ルータ ID の VRF 単位での割り当て機能に関連する参照資料を紹介します。

関連資料

関連項目	参照先
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*』
設定作業および設定例を含む BGP モジュールおよび機能のロードマップ	『BGP Features Roadmap』
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*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドについては、http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_book.html の『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup でコマンド検索ツールを使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html で『*Cisco IOS Master Command List, All Releases*』を参照してください。

- **bgp router-id**
- **show ip bgp vpnv4**

BGP ルータ ID の VRF 単位での割り当てに関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　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 単位の割り当て	12.2(31)SB2 12.2(33)SRA 12.2(33)SXH 12.4(20)T 15.0(1)S	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。 この機能では、**bgp router-id** コマンド、**show ip bgp vpnv4** コマンドが追加または変更されています。

L2VPN アドレス ファミリに対する BGP サポート

Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）アドレス ファミリに対する Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）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 Routing Information Base（RIB; ルーティング情報ベース）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

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「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」（P.14）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、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。

目次

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、VPN、Virtual Private LAN Service（VPLS; バーチャル プライベート LAN サービス）、および Multiprotocol Layer Switching（MPLS; マルチプロトコル レイヤ スイッチング）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 モードで使用された場合、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 ファミリに対する BGP サポートを設定するには、次の概念について理解する必要があります。

L2VPN アドレス ファミリ

Cisco IOS Release 12.2(33)SRB およびそれ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。L2VPN は、IP Security（IPsec; IP セキュリティ）または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）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 Routing Information Base（RIB; ルーティング情報ベース）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。プレフィクスおよびパス情報は L2VPN データベースに保存され、最良パスが 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 バーチャル プライベート LAN サービス（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 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 サポートの設定方法

ここでは、次の作業について説明します。

- 「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」（P.4）

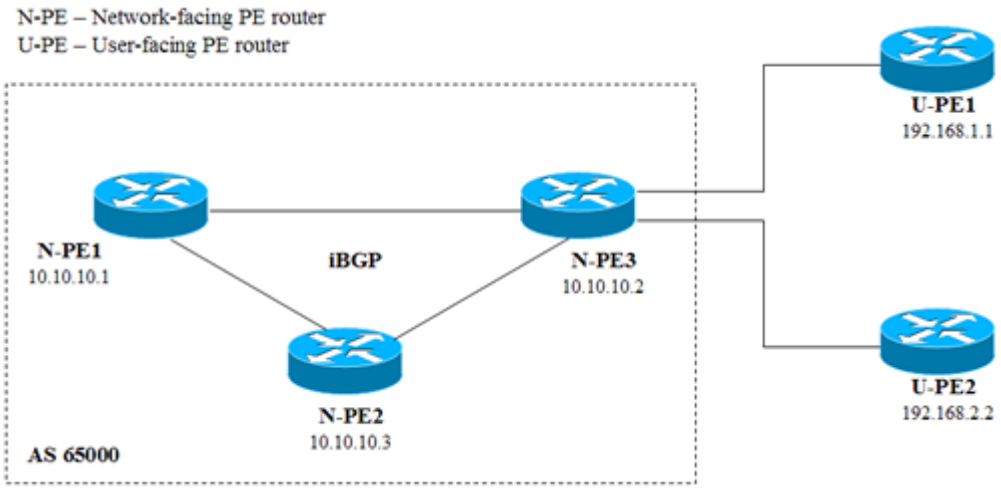
BGP および L2VPN アドレス ファミリを使用した VPLS オートディスカバリの設定

特定の VPLS のメンバーである各 Provider Edge（PE; プロバイダー エッジ）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 Release 12.2(33)SRB では、エンドポイント プロビジョニング情報が含まれる個別の L2VPN RIB とともに、BGP L2VPN アドレス ファミリが導入されました。BGP は、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。データベースは、Layer 2（L2）VFI が設定されるたびに更新されます。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。

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 に必要な疑似配線のフル メッシュを形成するよう VPLS 疑似配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 図 1 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、「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：例」（P.9）を参照してください。

図 1　　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 図 1 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 が入力して、この作業の手順を検証します。

新しい Virtual Forwarding Instance（VFI）に対して Route Reflector（RR; ルート リフレクタ）ノードがプロビジョニングされると、BGP は L2VPN Address Family Identifier（AFI; アドレス ファミリ識別子）からの現在のテーブル全体を L2VPN xconnect データベースに対してアナウンスし、Virtual Circuit（VC; 仮想回線）がアクティブであることを確認します。

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

前提条件

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. ステップ 4 ～ステップ 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. ステップ 13 ～ステップ 14 を繰り返して、他の BGP ネイバーを設定します。
16. **address-family l2vpn** [**vpls**]
17. **neighbor** {*ip-address* | *peer-group-name*} **activate**
18. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
19. ステップ 17 ～ステップ 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。
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配線で使用する 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。 • *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	ステップ 4 ～ステップ 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。	—

	コマンドまたはアクション	目的
ステップ 9	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
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 ファミリをディセーブルにします。 **（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 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イネーブルにします。
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	ステップ 13 ～ステップ 14 を繰り返して、他の BGP ネイバーを設定します。	—

	コマンドまたはアクション	目的
ステップ 16	**address-family l2vpn** [**vpls**] **例：** `Router(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** キーワードでは、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* | *peer-group-name*} **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、次のステップの **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 アトリビュートが 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 アトリビュートが 10.10.10.1 のネイバーに送信されます。
ステップ 19	ステップ 17 ～ステップ 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、VPLS のメイン マニュアルで「*VPLS Autodiscovery: BGP Based*」機能に関する項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

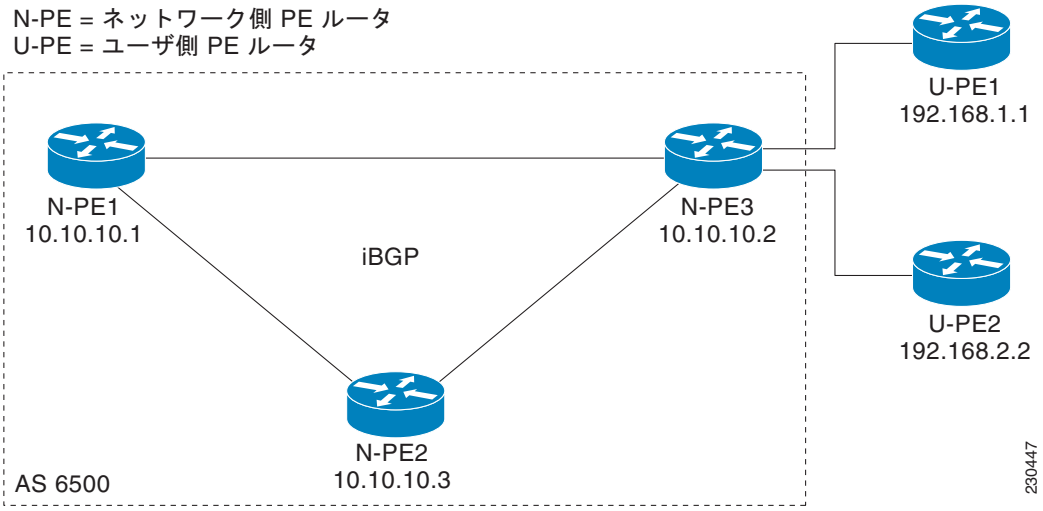
ここでは、次の設定例を示します。

- 「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：例」（P.9）

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：例

この設定例では、図 2 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 2　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 Ethernet0/0
 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 Ethernet0/0
 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 Loopback 1
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 update-source Loopback 1
!
 address-family l2vpn vpls
 neighbor 10.10.10.1 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 Ethernet0/0
 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 Loopback 1
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 update-source Loopback 1
!
 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
```

関連情報

VPLS オートディスカバリの設定の詳細については、「*VPLS Autodiscovery: BGP Based*」機能を参照してください。

その他の参考資料

ここでは、L2VPN アドレス ファミリに対する BGP サポート機能に関連する参考資料について説明します。

関連資料

関連項目	参照先
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 Overview」 *モジュール*
BGP 基本作業の設定	「Configuring a Basic BGP Network」 *モジュール*

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB 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、および機能セットの 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
この機能によってサポートされる新しい RFC または変更された RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その Cisco IOS ソフトウェア リリース トレインの以降のリリースでもその機能はサポートされます。

表 1　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	12.2(33)SRB	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 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。 Cisco IOS Release 12.2(33)SRB プラットフォームでは、この機能は Cisco 7600 プラットフォームに追加されました。 次のコマンドが、この機能によって導入または変更されました。**address-family l2vpn**、**clear ip bgp l2vpn**、**show ip bgp l2vpn**。

ピアごとの受信ルートに対する BGP 4 MIB サポート

このモジュールでは、ピアごとの受信ルートに対する BGP 4 MIB サポート機能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（簡易ネットワーク管理プロトコル（SNMP）コマンドを使用して）照会する機能を提供する新しいテーブルを CISCO-BGP4-MIB に導入します。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「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」（P.8）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、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。

目次

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。

機能の概要

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新しいテーブルを 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-speaking 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。

- プレフィクス
- プレフィクス長
- ピア アドレス

bgp4PathAttrTable は最初にプレフィ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 Routing Information Base（RIB; ルーティング情報ベース）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
  - プレフィクス
  - プレフィクス長

  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

表 1 に、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 1　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 レイヤ 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 レイヤ 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 レイヤ アドレスを表します。
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 レイヤ アドレスのタイプについては、表 2 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、表 3 を参照してください。

AFI と SAFI

表 2 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。表 2 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 2　AFI と SAFI

AFI	SAFI	Type
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 Route Distinguisher（RD; ルート識別子）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

表 3 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、表 1 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 3　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 レイヤ 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。

表 3　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 （続き）

テーブルまたはオブジェクト（またはインデックス）	説明
cbgpRouteAggregatorAddrType	cbgpRouteAggregatorAddr オブジェクトに格納されるネットワーク レイヤ 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 レイヤ 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。

利点

SNMP クエリー機能の向上

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した。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した。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。

設定作業

なし

設定例

なし

その他の参考資料

次の項では、ピアごとの受信ルートに対する BGP 4 MIB サポートに関する参考資料を説明します。

関連資料

関連項目	参照先
BGP の MIB の設定	『*Configuring Advanced BGP Features*』
BGP コマンド	『*Cisco IOS IP Routing: BGP Command Reference*』
SNMP サポートの設定	『*Configuring SNMP Support*』
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』の「SNMP Commands」

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/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

表 4 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS Release 12.2(1)、12.0(3)S、12.2(27)SBC、12.2(33)SRB、12.2(33)SXH、またはそれ以降のリリースで追加または変更された機能だけが表に示されています。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その Cisco IOS ソフトウェア リリース トレインの以降のリリースでもその機能はサポートされます。

表 4　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	機能の設定情報
『BGP 4 MIB Support for per-Peer Received Routes』	12.0(21)S 12.2(14)S 12.2(28)SB 15.0(1)S	この機能は、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新しいテーブルを CISCO-BGP4-MIB に導入します。 この機能によって導入または変更されたコマンドはありません。

用語集

AFI : Address Family Identifier（AFI; 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 レイヤ 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 : 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 レイヤ 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（MIB; 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 レイヤ到達可能性情報）。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 プレフィクスを伝送できます。

RIB：Routing Information Base（RIB）。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。属性で伝送されるネットワーク レイヤ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（SNMP; 簡易ネットワーク管理プロトコル）。TCP/IP ネットワークでほぼ独占的に使用されているネットワーク管理プロトコル。SNMP では、ネットワーク デバイスを監視および制御し、設定、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できます。

snmpwalk：**snmpwalk** コマンドは、Simple Network Management Protocol（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：Virtual Private Network（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。

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

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「BGP 低速ピアの検出と軽減のための機能情報」（P.22）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

目次

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*がイネーブルになります。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、低速ピアより速くコンバージできます。（**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

単に BGP 低速ピアを検出するには、次のタスクを実行します。

- 「低速ピアの検出」（P.5）

BGP 低速ピアの影響を減らし、アップデート グループの他のピアを低速にならないように動作させるには、次の 1 つ以上のタスクを実行します。

- 「ピアをスタティック低速ピアとしてマークする」（P.8）（任意）
- 「ダイナミック低速ピア保護の設定」（P.11）（任意）
- 「ダイナミック低速ピアに関する出力の表示」（P.16）（任意）
- 「ダイナミック低速ピアを通常のピアとして回復」（P.16）（任意）

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」（P.11）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」（P.5）
- 「ネイバー レベルでのダイナミック低速ピアの検出」（P.6）
- 「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」（P.7）

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：** `Router> enable`	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。
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。
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 秒から 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。
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。
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」（P.9）
- 「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」（P.9）

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。
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。
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」（P.11）
- 「ネイバー レベルでのダイナミック低速ピアの設定」（P.13）
- 「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」（P.14）

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タスクを実行します）。

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 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。
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。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *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 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。デフォルト値は 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」（P.16）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（コンバージする）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。
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。デフォルト値は 300 です。

	コマンドまたはアクション	目的
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」（P.16）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（コンバージする）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。

	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	**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。 • 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。デフォルト値は 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」（P.16）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（コンバージする）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。

	コマンドまたはアクション	目的
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。
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

このタスクで 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。
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、次のタスクで **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」（P.8）のいずれかのタスクに示すコマンドの **no** 形式を使用します。

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。
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。 • ***** 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

ここでは、次の BGP 低速ピア設定例について説明します。

- 「例：スタティック低速ピア」（P.18）
- 「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」（P.18）
- 「例：ネイバー レベルでのダイナミック低速ピア」（P.18）
- 「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」（P.18）
- 「例：ピア グループを使用したダイナミック低速ピア」（P.19）

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	参照先
Syslog メッセージと **logging console** コマンド	『*Cisco IOS XE Network Management Command Reference*』
BGP ピア ポリシー テンプレート	『*Cisco IOS XE IP Routing: BGP Configuration* Guide 』の「Configure a Basic BGP Network」モジュール

MIB

MIB	MIB 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、および機能セットの 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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 低速ピアの検出と軽減のための機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　BGP 低速ピアの機能情報

機能名	リリース	機能情報
BGP 低速ピア	Cisco IOS 15.0(1)S	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、ネットワークの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。 次のコマンドが変更されました。 • **clear ip bgp** • **show ip bgp neighbors** • **show ip bgp summary** 次のコマンドが導入されました。 • **bgp slow-peer detection** • **bgp slow-peer split-update-group dynamic** • **neighbor slow-peer detection** • **neighbor slow-peer split-update-group dynamic** • **neighbor slow-peer split-update-group static** • **slow-peer detection** • **slow-peer split-update-group dynamic** • **slow-peer split-update-group static**

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

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 サポート機能により、プロバイダー エッジ（PE）ルータは Customer Edge（CE; カスタマー エッジ）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、Route Processor（RP; ルート プロセッサ）スイッチオーバー中または PE ルータに対する定期的な In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）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 NonStop Forwarding（NSF; ノンストップ フォワーディング）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（SSO の BGP 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 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

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「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」（P.16）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

目次

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 サポート機能の前提条件

- このマニュアルでは、BGP が動作するようにネットワークが設定されていることを前提としています。
- このマニュアルでは、Multiprotocol Layer Switching（MPLS; マルチプロトコル レイヤ スイッチング）レイヤ 3 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）が設定されていることを前提としています。
- このマニュアルでは、NSF および SSO の概念および作業について精通していることを前提としています。

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 サポート機能に関する情報

BGP NSR with SSO 機能を設定するには、次の概念を理解しておく必要があります。

BGP NSR with SSO の概要

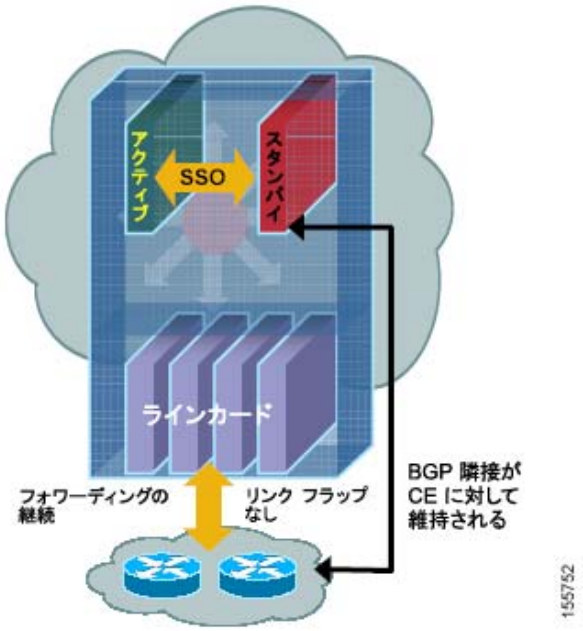
Cisco IOS Release 12.2(28)SB で BGP NSR with SSO が導入される以前は、BGP NSF に参加している隣接デバイスが NSF 対応であるか、または（BGP グレースフル リスタート メカニズムをサポートするようにデバイスを設定して）NSF 認識として設定する必要がありました。そのため、BGP NSF ではすべての隣接デバイスを BGP グレースフル リスタートをサポートする Cisco IOS ソフトウェア バージョンへアップグレードする必要がありました。ただし、多くの MPLS VPN 展開では、BGP グレースフル リスタートをサポートしておらず、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 Exterior BGP（eBGP; 外部 BGP）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、High Availability（HA; ハイ アベイラビリティ）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（図 1 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 Route Reflector（RR; ルート リフレクタ）との Internal BGP（iBGP; 内部 BGP）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 1　　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：BGP NSR with SSO により、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 HA の展開および利点が拡張されます。
- エッジにおけるハイ アベイラビリティ 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 ルータ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 ルータでの調整や 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 ルータとのグレースフル 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 フォワーディングを継続して 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）による無停止ルーティング（NSR）に対する BGP サポート機能の設定方法

ここでは、次の手順について説明します。

- 「BGP NSR with SSO をサポートする PE ルータの設定」（P.4）（必須）
- 「NSR with SSO の BGP サポートの確認」（P.10）（任意）

BGP NSR with SSO をサポートする PE ルータの設定

PE ルータが CE ルータとの BGP 状態を維持し、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 フォワーディングを継続できるようにするには、次の作業を実行します。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。

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 ルータでこのセクションの次のいずれかの作業を実行します。

- 「BGP NSR with SSO をサポートするピアの設定」（P.5）
- 「BGP NSR with SSO をサポートするピア グループの設定」（P.6）
- 「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」（P.8）

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、「Configuring a Basic BGP Network」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 モードの設定の詳細については、『*Stateful Switchover*』マニュアルで「Configuring SSO」作業を参照してください。
- PE ルータでグレースフル リスタートがイネーブルである必要があります。グレースフル リスタートの設定の詳細については、「Configuring Advanced BGP Features」モジュールを参照してください。

（注） 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。

- CE ルータは、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、『*Cisco IOS IP Routing: BGP Configuration Guide*』の「Configuring a Basic BGP Network」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

BGP ピアで BGP NSR with SSO をサポートするように設定する場合は、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. **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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] **例：** `Router(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。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4 vrf** *vrf-name* **例：** `Router(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：** `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。
ステップ 7	**neighbor** *ip-address* **ha-mode sso** **例：** `Router(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	BGP NSR with SSO 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：** `Router(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されたネイバーは、ユニキャスト アドレス プレフィクスだけを交換します。
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 vpnv4 all sso summary** **例：** `Router# 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

BGP ピア グループで BGP NSR with SSO をサポートするように設定する場合は、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. **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：** `Router> enable`	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。
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`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp graceful-restart [restart-time** *seconds*`]` `[`**stalepath-time** *seconds*`]` **例：** `Router(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	**address-family ipv4 vrf** *vrf-name* **例：** `Router(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：** `Router(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 7	**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。
ステップ 8	**neighbor** *ip-address* **peer-group** *peer-group-name* **例：** `Router(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：** `Router(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	BGP NSR with SSO 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：** `Router(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 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、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：** `Router# 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

BGP ピア セッション テンプレートで BGP NSR with SSO をサポートするように設定する場合は、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. **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：** `Router> enable`	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。
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	**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	**ha-mode sso** **例：** `Router(config-router-stmp)# ha-mode sso`	BGP NSR with SSO 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：** `Router(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：** `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。
ステップ 8	**show ip bgp template peer-session** [*session-template-name*] **例：** `Router# 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 テンプレートの詳細については、『*Cisco IOS IP Routing: BGP Configuration Guide*』の「Configuring a Basic BGP Network」の章を参照してください。

NSR with SSO の BGP サポートの確認

BGP NSR with SSO サポートを確認する場合は、このオプション作業を実行します。

手順の概要

1. **enable**
2. **show ip bgp vpnv4 all sso summary**
3. **show ip bgp vpnv4 all neighbors**

手順の詳細

ステップ 1 **enable**

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。

```
Router> enable
```

ステップ 2 **show ip bgp vpnv4 all sso summary**

このコマンドは、SSO モードである 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。

```
Router# show ip bgp vpnv4 all sso summary

   Stateful switchover support enabled for 40 neighbors
```

ステップ 3 **show ip bgp vpnv4 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 vpnv4 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 がイネーブルかディセーブルかを示します。[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。

```
Router# show ip bgp vpnv4 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: VPNv4 Unicast
   Translates address family IPv4 Unicast for VRF vrf1
   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。

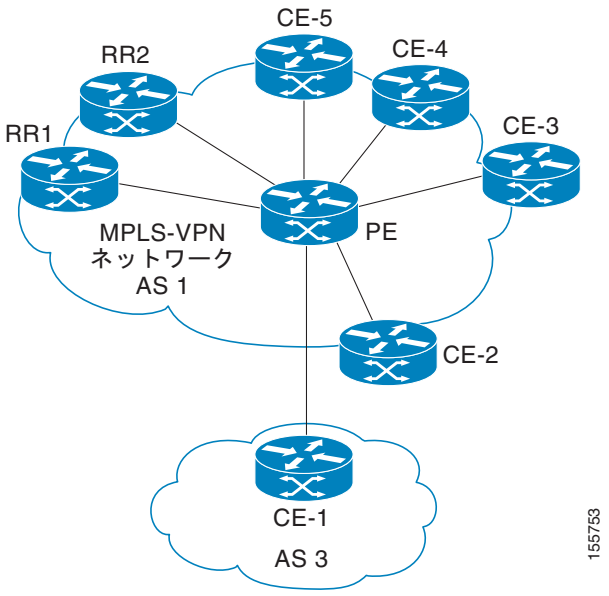
ステートフル スイッチオーバー（SSO）による無停止ルーティング（NSR）に対する BGP サポート機能の設定例

BGP NSR with SSO の設定：例

図 2 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 2　BGP NSR with SSO のトポロジ例



RR1 の設定

次の例では、図 2 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、図 2 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 ipv4 vrf ce-1
 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、図 2 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	参照先
BGP の概念と設定作業	「Cisco BGP Overview」モジュール
BGP コマンド：コマンド構文、コマンド モード、コマンド履歴、コマンド デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
BGP NSF 認識の概念、設定作業、および例	「Configuring Advanced BGP Features」モジュール
ISSU の概念、設定作業、および例	「Cisco In Service Software Upgrade Process」モジュール
MPLS レイヤ 3 VPN の概念および設定作業	「Configuring MPLS Layer 3 VPNs」モジュール
MPLS レイヤ 3 VPN コマンド：コマンド構文、コマンド モード、コマンド履歴、コマンド デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
SSO の概念、設定作業、および例	『*Stateful Switchover*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB 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、および機能セットの 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
draft-ietf-idr-restart-06.txt	『*Graceful Restart Mechanism for BGP*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

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

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 1　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
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	12.2(28)SB 15.0(1)S	ステートフル スイッチオーバー（SSO）による無停止ルーティング（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 Customer Edge（CE; カスタマー エッジ）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、Route Processor（RP; ルート プロセッサ）スイッチオーバー中または PE ルータに対する定期的な In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）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 NonStop Forwarding（NSF; ノンストップ フォワーディング）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：RT 制約ルート配布の設定

BGP: RT 制約ルート配布は、Route Reflector（RR; ルート リフレクタ）が RR および 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ためにサービス プロバイダが Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Layer 3 Virtual Private Networks（L3VPN; レイヤ 3 バーチャル プライベート ネットワーク）で使用する機能です。ルーティング アップデートを減らすことにより、リソースを節約できます。RR、Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）、PE が伝送するルートは少なくなります。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

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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、「BGP：RT 制約ルート配布の機能情報」（P.19）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。

目次

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。

- MPLS VPN
- Route Distinguisher（RD; ルート識別子）
- Route Target（RT; ルート ターゲット）
- Multiprotocol BGP（MBGP; マルチプロトコル BGP）

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 VPNv4 と VPNv6 のルート アドバタイズメントのみが制限されます。

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、その結果リソースが大量に消費されます。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。

図 1 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 1　PE での不要なルーティング アップデート

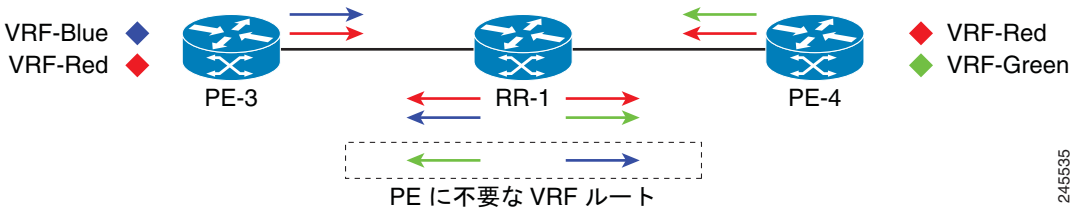


図 1 に示すとおり、PE は次のように不要なルートを受信しています。

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るだけでなく、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。図 2 に、RR に不要なルートが送信される場合の例を示します。

図 2　RR での不要なルーティング アップデート

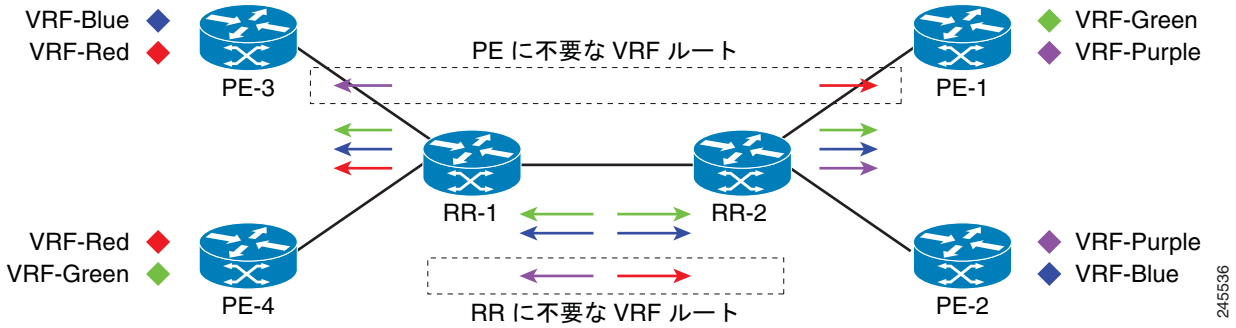


図 2 に示すとおり、RR-1 と RR-2 は次のように不要なルーティング アップデートを受信しています。

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 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 を隔離します。PE と Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）は、受信した VPN ルートをフィルタリングして、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すると、受信側で不要なルートが除外されます。これによりリソースが節約され、そのような VPN ルート アップデートが最初から生成されないようになります。

ARTF は VPN Network Layer Reachability Information（NLRI; ネットワーク層到達可能性情報）が RR から VPN を必要としない PE に伝播されないようにするためのメカニズムです。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、新しい Subsequent Address Family Identifier（SAFI）である BGP RT-Constrain 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 制約ルート配布のしくみ

「BGP：RT 制約ルート配布により解決できる問題」（P.2）で説明したように不要なルートをフィルタリング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 Network Layer Reachability Information（NLRI; ネットワーク層到着可能性情報）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。

図 3 に、RT Constraint（RTC; RT 制約）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 3　PE と RR の間での RTC NLRI とフィルタの交換

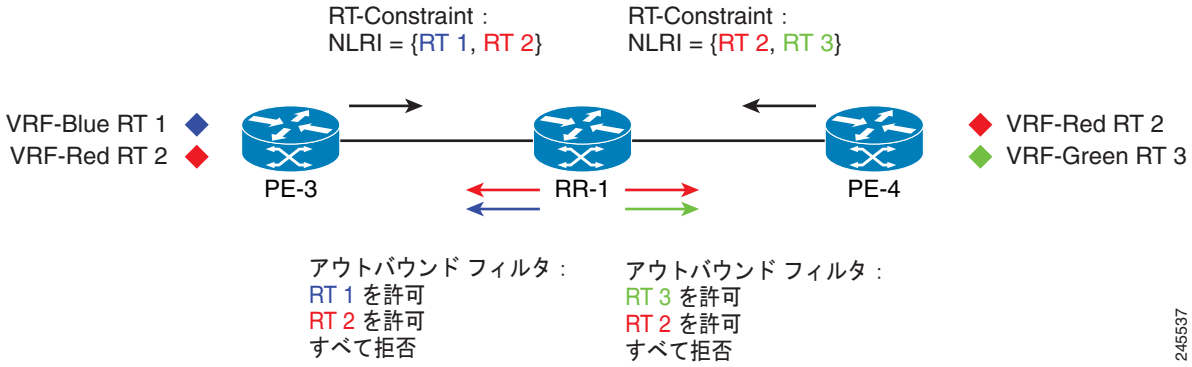


図 3 に示すとおり、PE と RR の間では次の情報交換が行われます。

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 プレフィクス

RT 制約 NLRI の形式は、長さが 12 バイトのプレフィクスで、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。最初の例では、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の例

RT 制約ルート配布のプロセスを示すため、この例では PE1 に接続されている AS 100 に 2 つの CE ルータを設置してあります。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 Route Reflector（RR; ルート リフレクタ）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 Constrain（RTC; RT 制約）プレフィクス 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 PE2 のアウトバウンド フィルタにインストールします。
7. RR には RT を許可または拒否するフィルタがあります（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. PE1 はアップデート パケットを RR に送信します。RR はフィルタを参照し、アウトバウンド パケットが許可されることを確認します。

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** コマンドで **neighbor default-originate** コマンドを設定します。

RT 制約ルート配布の設定方法

BGP：RT 制約ルート配布を設定するには、次の作業を実行します。最初の 3 つの作業は MPLS 環境で一般的なものです。最後の作業は、指定した BGP ネイバーと自動 RT フィルタ情報を交換するためのものです。

- 「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」（P.6）（必須）
- 「MPLS VPN カスタマーの接続」（P.8）（必須）
- 「PE での RT 制約の設定」（P.12）（必須）
- 「RR での RT 制約の設定」（P.13）（必須）

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 Multiprotocol BGP（MP-BGP; マルチプロトコル 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. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **address-family vpnv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	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。
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 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：** `Router(config-router)# no bgp default ipv4-unicast`	（任意）IPv4 ユニキャスト アドレス ファミリをすべてのネイバーでディセーブルにします。 • 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：** `Router(config-router)# neighbor pp.0.0.1 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(config-router)# 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	**address-family 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、標準 VPNv4 アドレス プレフィクスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィクスを指定します。

	コマンドまたはアクション	目的
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** **例：** `Router(config-router-af)# neighbor pp.0.0.1 send-community extended`	コミュニティ アトリビュートが BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(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 10	**end** **例：** `Router(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、ネイバーが稼動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** *x.x.x.x* **events** コマンドを入力します。ここで、*x.x.x.x* 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」（P.8）（必須）
- 「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」（P.10）（必須）
- 「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」（P.10）（必須）

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

Virtual Routing and Forwarding（VPN Routing and Forwarding; VPN ルーティング/転送）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：** `Router> enable`	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。
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 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：** `Router(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 プレフィクスに追加され、VPN IPv4 プレフィ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。
ステップ 5	**route-target** {**import** |**export** | **both**} *route-target-ext-community* **例：** `Router(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 アトリビュートが、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：** `Router(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 マップとして使用するルート マップを指定します。
ステップ 7	**exit** **例：** `Router(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：** `Router> enable`	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。
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 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* 引数には、設定するインターフェイスのタイプを指定します。 • *number* 引数には、ポート、コネクタ、またはインターフェイス カード番号を指定します。
ステップ 4	**ip vrf forwarding** *vrf-name* **例：** `Router(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** `Router(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：** `Router> enable`	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。
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 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：** `Router(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 プレフィクスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィクスを指定します。 • **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：** `Router(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：** `Router(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：** `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。
ステップ 8	**end** **例：** `Router(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. **end**
7. **show ip bgp rtfilter all**
8. **show ip bgp rtfilter all summary**
9. **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：** `Router> enable`	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。
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** *as-number* **例：** `Router(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：** `Router(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：** `Router(config-router-af)# neighbor 10.0.0.1 activate`	指定した BGP ネイバーとの自動 RT フィルタ情報を交換できるようにします。
ステップ 6	**end** **例：** `Router(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 7	**show ip bgp rtfilter all** **例：** `Router# 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 8	**show ip bgp rtfilter all summary** **例：** `Router# 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。
ステップ 9	**show ip bgp vpnv4 all** **例：** `Router# 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*} **send-community extended**
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client**

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：** `Router> enable`	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。
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 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：** `Router(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*} **send-community extended** **例：** `Router(config-router-af)# neighbor pp.0.0.1 send-community extended`	コミュニティ アトリビュートが 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 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(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 7	**neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** **例：** `Router(config-router-af)# neighbor 10.0.0.2 route-reflector-client`	指定した BGP ネイバーでの RT 制約をイネーブルにします。 • **neighbor route-reflector-client** コマンドを設定すると、ルータは自動的にデフォルトの RT フィルタを送信し、PE がすべての VPN ルートを RR に送信するように要求します（「デフォルトの RT フィルタ」（P.6）を参照してください）。そのため、**neighbor default-originate** コマンドを設定する必要はありません。
ステップ 8	**end** **例：** `Router(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。

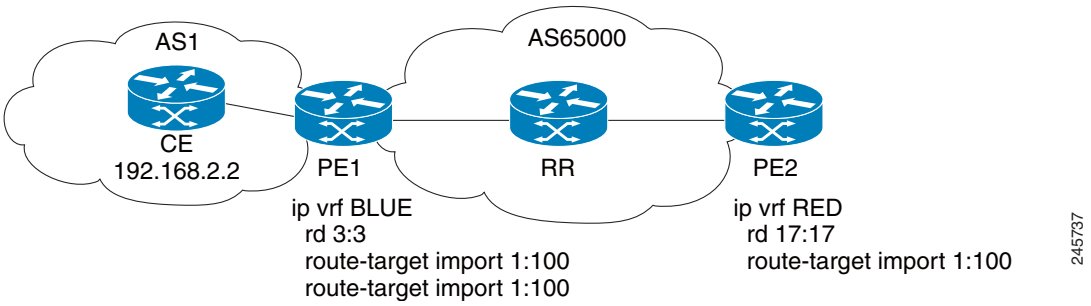
	コマンドまたはアクション	目的
ステップ 9	**show ip bgp rtfilter all** **例：** `Router# show ip bgp rtfilter all`	（任意）すべての BGP RT フィルタ情報を表示します。
ステップ 10	**show ip bgp rtfilter all summary** **例：** `Router# show ip bgp rtfilter all summary`	（任意）BGP RT フィルタのサマリー情報を表示します。
ステップ 11	**show ip bgp vpnv4 all** **例：** `Router# show 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、図 4 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 4　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 1
 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
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.6.6 remote-as 1
 neighbor 192.168.6.6 update-source Loopback0
 neighbor 192.168.7.7 remote-as 1
 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 192.168.7.7 activate
  neighbor 192.168.7.7 send-community extended
  neighbor 192.168.7.7 route-reflector-client
 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
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.2.2 remote-as 1
 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	参照先
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*』
L3VPNs とルート ターゲット	『*Cisco IOS MPLS Configuration Guide*』の「Configuring MPLS Layer 3 VPNs」
MPLS コマンド	『*Cisco IOS Multiprotocol Label Switching Command Reference*』

MIB

MIB	MIB リンク
—	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 4360	『*BGP Extended Communities Attribute*』
RFC 4684	『*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*』
RFC 5291	『*Outbound Route Filtering Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 1　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	15.1(1)S	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**