



## BGP の拡張機能の設定

このモジュールでは、さまざまな拡張ボーダー ゲートウェイ プロトコル (BGP) 機能の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 に対する双方向フォワーディング検出 (BFD) 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。

### 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュール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 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および 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> からアクセスします。Cisco.com のアカウントは必要ありません。

### 内容

- 「[BGP の拡張機能を設定するための前提条件](#)」(P.2)
- 「[BGP の拡張機能を設定するための制約事項](#)」(P.2)
- 「[BGP の拡張機能の設定に関する情報](#)」(P.2)
- 「[BGP の拡張機能の設定方法](#)」(P.14)
- 「[BGP の拡張機能を設定するための設定例](#)」(P.50)
- 「[次の作業](#)」(P.59)
- 「[その他の参考資料](#)」(P.59)
- 「[BGP の拡張機能を設定するための機能情報](#)」(P.61)



## 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せん。
- 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

- 「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.8)
- 「BGP 用の双方向フォワーディング検出 (BFD)」(P.9)
- 「BGP MIB サポート」(P.9)
- 「MTR に対する BGP サポート」(P.12)

## 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。同じ組織内の BGP ピアは、内部 BGP (iBGP) ピアリング セッションを通じて、ルーティング情報を交換します。内部 BGP ピアに関する詳細については、『Cisco IOS IP Routing Configuration Guide』の『Configuring Internal BGP Features』の章を参照してください。



(注)

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

## 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](#)」 (P.3)
- 「[BGP スキャナのデフォルトの動作](#)」 (P.3)
- 「[選択的 BGP ネクストホップ ルート フィルタリング](#)」 (P.3)

### BGP ネクストホップ アドレス トラッキング

BGP ネクストホップ アドレス トラッキング機能は、サポート Cisco ソフトウェア イメージがインストールされている場合はデフォルトでイネーブルになっています。BGP ネクストホップ アドレス トラッキングはイベント ドリブです。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。

### 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 属性に適用されるプレフィックスの長さを設定できます。ルート マップは BGP 最良パスの計算中に使用され、BGP プレフィックスのネクストホップ属性が記載されたルーティング テーブル内のルートに適用されます。ネクストホップ ルートがルート マップの評価に失敗した場合は、ネクストホップ ルートは到達不能とマークされます。このコマンドはアドレス ファミリ単位で実行されるため、異なるアドレス ファミリ内のネクストホップ ルートでは別のルート マップを適用できます。



(注) **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 Next\_Hop 属性

Next\_Hop 属性は、宛先への BGP ネクストホップとして使用されるネクストホップ IP アドレスを示します。ルータは、再帰的ルックアップによってルーティング テーブルで BGP ネクストホップを検索します。外部 BGP (eBGP) では、ネクストホップはアップデートを送信したピアの IP アドレスです。内部 BGP (iBGP) は、内部で生成されたルートのプレフィックスをアドバタイズしたピアの IP アドレスを、ネクストホップのアドレスとして設定します。eBGP から学習した iBGP へのルートのいずれかがアドバタイズされた場合、Next\_Hop 属性は変更されません。

ルータが BGP ルートを使用するためには、BGP ネクストホップの IP アドレスが到達可能でなければなりません。到着可能性情報は通常 IGP によって提供され、IGP での変更はネットワーク バックボーンを介したネクストホップアドレスの転送に影響を与える可能性があります。

## 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」 (P.4)
- 「NSF のシスコ エクスプレス フォワーディング」 (P.5)
- 「NSF のための BGP グレースフル リスタート」 (P.5)
- 「BGP NSF 認識」 (P.6)
- 「ネイバーごとの BGP グレースフル リスタート」 (P.7)
- 「BGP ピア セッション テンプレート」 (P.7)

## 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 認識であるを見なします。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。それから CEF はラインカードに新しい FIB 情報を更新します。



(注) 現在、EIGRP では NSF 認識だけがサポートされます。

## NSF のシスコ エクスプレス フォワーディング

NSF の重要な要素はパケット転送です。シスコのネットワークング デバイスでは、パケットの転送は CEF によって行われます。CEF は FIB を維持し、スイッチオーバー時に最新だった FIB 情報を使用して、スイッチオーバー中のパケットの転送を続行します。この機能により、スイッチオーバー中のトラフィックの中断を短くします。

通常の NSF 操作中に、アクティブな 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。既存または新規エントリは、リフレッシュされた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。転送情報はラインカードまたはコンバージェンス中の転送エンジンで更新されます。RIB が収束すると、RP が信号通知を行います。ソフトウェアは、現在のスイッチオーバー エポックよりも前のエポックを持った FIB および隣接エントリをすべて削除します。これで、FIB は最新のルーティング プロトコル転送情報となります。

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 テーブルの再構築に役立てるために、NSF 認識 ネイバー デバイスがステート情報を送信するように要求します。



(注) NSF 動作の場合、ルーティング プロトコルは、ルーティング情報を再構築している間にパケットを送り続ける CEF によって異なります。

## NSF のための BGP グレースフル リスタート

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。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した場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応ルータと BGP ピア (NSF 認識ピア) の両方が、セッションの確立時に OPEN メッセージでグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を交換しない場合、セッションはグレースフル リスタート対応になりません。

RP のスイッチオーバー中に BGP セッションが切断された場合、NSF 認識 BGP ピアは、NSF 対応ルータに関連付けられたすべてのルートを失効とマーキングします。ただし、所定の時間内は、引き続きこれらのルートを転送の決定に使用します。この機能により、新しくアクティブになった RP が BGP ピアとのルーティング情報のコンバージェンスを待機している間にパケットが消失することを防ぐことができます。

RP のスイッチオーバーが発生した後、NSF 対応ルータは BGP ピアとのセッションを再確立します。新しいセッションの確立時に、NSF 対応ルータが再起動したことを識別する新しいグレースフルリスタートメッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピアの間で交換されます。この交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、RIB と FIB を新しい転送情報で更新します。NSF 認識デバイスは、ネットワーク情報を使用して失効したルートを BGP テーブルから削除します。この後 BGP プロトコルが完全に収束します。

BGP ピアがグレースフルリスタート機能をサポートしていない場合、OPEN メッセージのグレースフルリスタート機能は無視されますが NSF 対応デバイスを使用して BGP セッションを確立します。この機能により、NSF 非認識（つまり NSF 機能のない）BGP ピアとの相互運用が可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフルリスタート機能を使用できません。

## BGP NSF 認識

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構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

## BGP ピア セッション テンプレート

ピア セッション テンプレートは、一般的な BGP セッション コマンドの設定をグループ化して、セッションの設定要素を共有するネイバーのグループに適用するために使用されます。異なるアドレス ファミリー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、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 ファミリー、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。

BGP ピア セッション テンプレートを使用して BGP グレースフル リスタートをイネーブルまたはディセーブルにするには、『[BGP ピア セッション テンプレートを使用した BGP グレースフル リスタートのイネーブル化とディセーブル化](#)』 (P.24) を参照してください。

## 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、ルートステータスは履歴からダンプに変更されます。
- ダンプステータス：この状態では、ルートフラップが非常に頻繁に発生したため、ルータはこのルートを BGP ネイバーにアドバタイズしなくなります。
- 抑制限度：ペナルティがこの制限を超えるとルートは抑制されます。デフォルト値は 2000 です。
- 半減期：ルートにペナルティが割り当てられると、半減期期間（デフォルトでは 15 分）後にペナルティは半減されます。ペナルティを小さくするプロセスは 5 秒ごとに発生します。
- 再使用制限：フラッピングルートのペナルティが減少し、この再使用制限を下回ると、ルートの抑制は解除されます。つまり、ルートは再び BGP テーブルに追加され、フォワーディングに再び使用されます。デフォルトの再使用制限は 750 です。ルートの抑制中止プロセスは、10 秒経過ごとに発生します。10 秒ごとに、ルータは、現在抑制が解除されているルートを検索して、アドバタイズします。
- 最大抑制制限：この値は、ルートを抑止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 Release 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 はあらゆるメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、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 に関する詳細については、『Cisco IOS IP Routing: BFD Configuration Guide』の『[Bidirectional Forwarding Detection](#)』モジュール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.10)
- 「BGP ルートが受信したルートのサポート」 (P.10)
- 「BGP プレフィクスしきい値の通知サポート」 (P.10)
- 「VPNv4 ユニキャストアドレス ファミリ ルートのサポート」 (P.11)
- 「cbgpPeerTable サポート」 (P.11)

### 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 *cbgpPrfexixMaxThresholdClear* 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*

`cbgpPrfexMaxThresholdClear` 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](#)」 (P.12)
- 「[BGP 下の MTR コマンドライン インターフェイス \(CLI\) 階層](#)」 (P.12)
- 「[クラス固有のトポロジの BGP セッション](#)」 (P.13)
- 「[BGP を使用したトポロジの変換](#)」 (P.13)
- 「[BGP を使用したトポロジのインポート](#)」 (P.13)

### 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 プロセスの範囲を設定すると、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」 (P.14)
- 「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.20)
- 「BGP ルート ダンプニングの設定」 (P.35)
- 「BFD を使用した BGP コンバージェンス時間の短縮」 (P.38)
- 「BGP MIB サポートのイネーブル化」 (P.41)
- 「MTR に対する BGP サポートの設定」 (P.42)

## 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」 (P.14)
- 「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」 (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」 (P.17)

## 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 ファミリーと VPNv4 アドレス ファミリーではデフォルトでイネーブルになっています。Cisco IOS Release 12.2(33)SB6 以降では、BGP ネクストホップ アドレス トラッキングは、VPNv6 アドレス ファミリーでネクストホップが IPv6 ネクストホップ アドレスにマッピングされる IPv4 アドレスである場合は、デフォルトで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*] | *vpn*v4 [*unicast*] | *vpn*v6 [*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	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<code>configure terminal</code>  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	<code>router bgp autonomous-system-number</code>  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	<code>address-family ipv4 [[mdt   multicast   tunnel   unicast [vrf vrf-name]   vrf vrf-name]   vpnv4 [unicast]   vpnv6 [unicast]]</code>  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。 <ul style="list-style-type: none"><li>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。</li></ul>
ステップ5	<code>no bgp nexthop trigger enable</code>  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。 <ul style="list-style-type: none"><li>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。</li><li>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。</li></ul>
ステップ6	<code>end</code>  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。

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。

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	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<code>configure terminal</code>  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	<code>router bgp autonomous-system-number</code>  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	<code>address-family ipv4 [[mdt   multicast   tunnel   unicast [vrf vrf-name]   vrf vrf-name]   vpnv4 [unicast]]</code>  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。 <ul style="list-style-type: none"><li>• 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。</li></ul>
ステップ 5	<code>bgp nexthop trigger delay delay-timer</code>  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。 <ul style="list-style-type: none"><li>• 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。</li><li>• <code>delay-timer</code> 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。</li><li>• この例では、20 秒の遅延間隔を設定します。</li></ul>
ステップ 6	<code>end</code>  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。 **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。 **set** コマンドやその他の **match** コマンドはサポートされません。

**bgp nexthop** コマンドの使用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.51) を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf vrf-name**]
5. **bgp nexthop route-map** *map-name*
6. **exit**
7. **exit**
8. **ip prefix-list** *list-name* [**seq seq-value**] {**deny network/length** | **permit network/length**} [**ge ge-value**] [**le le-value**]
9. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
10. **match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*]
11. **exit**
12. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
13. **end**
14. **show ip bgp** [*network*] [*network-mask*]

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>プロンプトが表示されたら、パスワードを入力します。</li> </ul>
ステップ2	<b>configure terminal</b>  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	<b>router bgp</b> <i>autonomous-system-number</i>  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
<p><b>ステップ 4</b> <code>address-family ipv4 [unicast   multicast   vrf vrf-name]</code></p> <p><b>例 :</b> Router(config-router)# address-family ipv4 unicast</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>unicast</b> 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、<b>address-family ipv4</b> コマンドに <b>unicast</b> 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。</li> <li>• <b>multicast</b> 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。</li> <li>• <b>vrf</b> キーワードと <i>vrf-name</i> 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。</li> </ul>
<p><b>ステップ 5</b> <code>bgp nexthop route-map map-name</code></p> <p><b>例 :</b> Router(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
<p><b>ステップ 6</b> <code>exit</code></p> <p><b>例 :</b> Router(config-router-af)# exit</p>	<p>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。</p>
<p><b>ステップ 7</b> <code>exit</code></p> <p><b>例 :</b> Router(config-router)# exit</p>	<p>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。</p>
<p><b>ステップ 8</b> <code>ip prefix-list list-name [seq seq-value] {deny network/length   permit network/length} [ge ge-value] [le le-value]</code></p> <p><b>例 :</b> Router(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
<p><b>ステップ 9</b> <code>route-map map-name [permit   deny] [sequence-number]</code></p> <p><b>例 :</b> Router(config)# route-map CHECK-NEXTHOP deny 10</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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 <b>match</b> 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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 10	<pre>match ip address prefix-list prefix-list-name [ prefix-list-name...]</pre> <p><b>例:</b> Router(config-route-map)# match ip address prefix-list FILTER25</p>	<p>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。</p> <ul style="list-style-type: none"> <li>プレフィクス リストの名前を指定するには、<i>prefix-list-name</i> 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。</li> </ul> <p><b>(注)</b> この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『<a href="#">Cisco IOS IP Routing: BGP Command Reference</a>』を参照してください。</p>
ステップ 11	<pre>exit</pre> <p><b>例:</b> Router(config-route-map)# exit</p>	<p>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。</p>
ステップ 12	<pre>route-map map-name [permit   deny] [sequence-number]</pre> <p><b>例:</b> Router(config)# route-map CHECK-NEXTHOP permit 20</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 13	<pre>end</pre> <p><b>例:</b> Router(config-route-map)# end</p>	<p>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。</p>
ステップ 14	<pre>show ip bgp [network] [network-mask]</pre> <p><b>例:</b> Router# show ip bgp</p>	<p>BGP ルーティング テーブル内のエントリを表示します。</p> <ul style="list-style-type: none"> <li>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。</li> </ul> <p><b>(注)</b> この例では、このタスクに適用可能な構文だけが使用されています。詳細については、『<a href="#">Cisco IOS IP Routing: BGP Command Reference</a>』を参照してください。</p>

## 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.20)
- 「BGP NSF 認識タイマーの設定」 (P.22)
- 「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.24)
- 「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せん。NSF 認識はデフォルトではイネーブルになっておらず、BGP NSF に関与するすべてのネイバーで設定する必要があります。



(注)

BGP グレースフル リスタート機能をイネーブルにするには、リスタート タイマーと失効パス タイマーの設定は不要です。デフォルト値はほとんどのネットワーク構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

### 制限事項

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.9) 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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>router bgp autonomous-system-number</code>  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	<code>bgp graceful-restart [restart-time seconds] [stalepath-time seconds]</code>  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 セッションが確立された後でこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。  • このコマンドは、再起動ルータとそのすべてのピア (NSF 対応と NSF 認識) で使用してください。
ステップ 5	<code>end</code>  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ダバタイズする 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。設定できる BGP グレースフル リスタート タイマーは 2 つあります。任意の **restart-time** キーワードと *seconds* 引数は、BGP OPEN メッセージを受信するまでピア ルータが失効したルートを削除するために待機する時間の長さを決定します。デフォルト値は 120 秒です。任意の **stalepath-time** キーワードと *seconds* 引数は、再起動ルータから End Of Record (EOR) メッセージを受信した後で失効したルートを削除するまでルータが待機する時間の長さを決定します。デフォルト値は 360 秒です。



(注) BGP グレースフル リスタート機能をイネーブルにするには、リスタート タイマーと失効パス タイマーの設定は不要です。デフォルト値はほとんどのネットワーク構成にとって最適な値であり、これらの値は経験豊富なネットワーク オペレータのみが調整すべきです。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp *autonomous-system-number***
4. **bgp graceful-restart [restart-time *seconds*]**
5. **bgp graceful-restart [stalepath-time *seconds*]**
6. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<b>configure terminal</b>  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	<b>router bgp <i>autonomous-system-number</i></b>  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
<p><b>ステップ 4</b> <code>bgp graceful-restart [restart-time seconds]</code></p> <p><b>例：</b>  Router(config-router)# <code>bgp graceful-restart restart-time 130</code></p>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>restart-time</b> 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。</li> <li>• 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。</li> </ul> <p>(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、『<a href="#">Cisco IOS IP Routing: BGP Command Reference</a>』を参照してください。</p>
<p><b>ステップ 5</b> <code>bgp graceful-restart [stalepath-time seconds]</code></p> <p><b>例：</b>  Router(config-router)# <code>bgp graceful-restart stalepath-time 350</code></p>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>stalepath-time</b> 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。</li> <li>• 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。</li> </ul> <p>(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、『<a href="#">Cisco IOS IP Routing: BGP Command Reference</a>』を参照してください。</p>
<p><b>ステップ 6</b> Router(config-router)# <code>end</code></p> <p><b>例：</b>  Router(config-router)# <code>end</code></p>	<p>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。</p>

## 次の作業

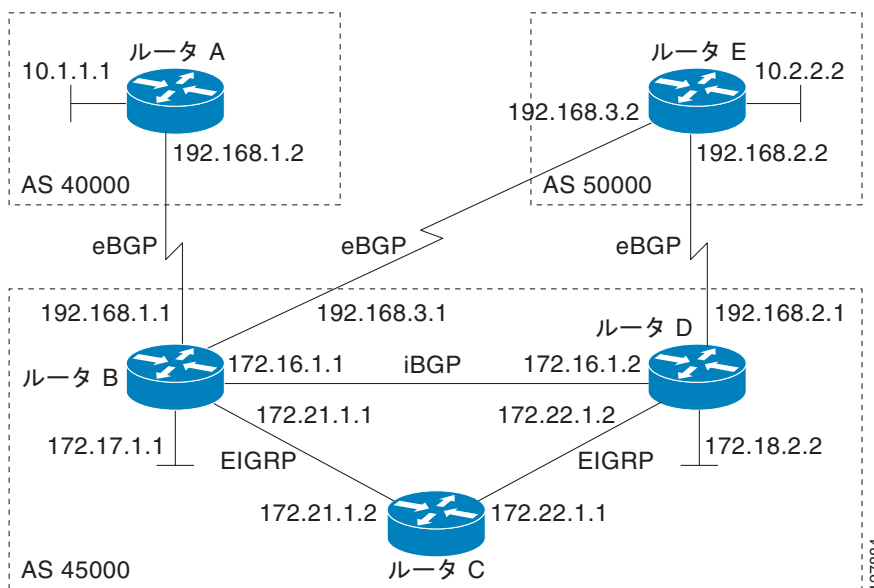
BGP セッションの確立後に `bgp graceful-restart` コマンドを実行する場合は、グレースフル リスタート機能を交換する前に、`clear ip bgp *` コマンドを実行するかルータをリロードすることによって、ピアセッションをリセットする必要があります。BGP セッションのリセットと `clear ip bgp` コマンドの使用に関する詳細については、『[Configuring a Basic BGP Network](#)』モジュールを参照してください。

## 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.22) 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。

### 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。

### 制限事項

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	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<code>configure terminal</code>  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	<code>router bgp <i>autonomous-system-number</i></code>  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	<code>template peer-session <i>session-template-name</i></code>  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。 <ul style="list-style-type: none"><li>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。</li></ul>

	コマンドまたはアクション	目的
ステップ 5	<pre>ha-mode graceful-restart [disable]</pre> <p>例 :</p> <pre>Router(config-router-stmp)# ha-mode graceful-restart</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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、<b>disable</b> キーワードを使用します。</li> <li>• 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。</li> <li>• 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。</li> </ul>
ステップ 6	<pre>exit-peer-session</pre> <p>例 :</p> <pre>Router(config-router-stmp)# exit-peer-session</pre>	<p>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。</p>
ステップ 7	<pre>template peer-session session-template-name</pre> <p>例 :</p> <pre>Router(config-router)# template peer-session S2</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 8	<pre>ha-mode graceful-restart [disable]</pre> <p>例 :</p> <pre>Router(config-router-stmp)# ha-mode graceful-restart disable</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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、<b>disable</b> キーワードを使用します。</li> <li>• 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。</li> <li>• 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。</li> </ul>
ステップ 9	<pre>exit-peer-session</pre> <p>例 :</p> <pre>Router(config-router-stmp)# exit-peer-session</pre>	<p>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。</p>
ステップ 10	<pre>bgp log-neighbor-changes</pre> <p>例 :</p> <pre>Router(config-router)# bgp log-neighbor-changes</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。</li> </ul>
ステップ 11	<pre>neighbor ip-address remote-as autonomous-system-number</pre> <p>例 :</p> <pre>Router(config-router)# neighbor 192.168.1.2 remote-as 40000</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 12	<pre>neighbor ip-address inherit peer-session session-template-number</pre> <p>例:</p> <pre>Router(config-router)# neighbor 192.168.1.2 inherit peer-session S1</pre>	<p>ピア セッション テンプレートを継承します。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 13	<pre>neighbor ip-address remote-as autonomous-system-number</pre> <p>例:</p> <pre>Router(config-router)# neighbor 192.168.3.2 remote-as 50000</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 14	<pre>neighbor ip-address inherit peer-session session-template-number</pre> <p>例:</p> <pre>Router(config-router)# neighbor 192.168.3.2 inherit peer-session S2</pre>	<p>ピア セッション テンプレートを継承します。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 15	<pre>end</pre> <p>例:</p> <pre>Router(config-router)# end</pre>	<p>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。</p>
ステップ 16	<pre>show ip bgp template peer-session [session-template-number]</pre> <p>例:</p> <pre>Router# show ip bgp template peer-session</pre>	<p>(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。</p> <ul style="list-style-type: none"> <li><code>session-template-name</code> 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。</li> </ul>
ステップ 17	<pre>show ip bgp neighbors [ip-address [received-routes   routes   advertised-routes   paths [regex]   dampened-routes   flap-statistics   received prefix-filter   policy [detail]]]</pre> <p>例:</p> <pre>Router# show ip bgp neighbors 192.168.1.2</pre>	<p>(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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

## 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 multiseession capable
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
  Graceful Restart Capability: advertised
  Multiseession 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 multiseession 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 ファミリー 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 [regex] | 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	<p><code>enable</code></p> <p>例： Router&gt; enable</p>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> <li>• プロンプトが表示されたら、パスワードを入力します。</li> </ul>
ステップ 2	<p><code>configure terminal</code></p> <p>例： Router# configure terminal</p>	<p>グローバル コンフィギュレーション モードを開始します。</p>
ステップ 3	<p><code>router bgp autonomous-system-number</code></p> <p>例： Router(config)# router bgp 45000</p>	<p>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。</p>
ステップ 4	<p><code>address-family ipv4 [unicast   multicast   vrf vrf-name]</code></p> <p>例： Router(config-router)# address-family ipv4 unicast</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>unicast</b> 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、<b>address-family ipv4</b> コマンドに <b>unicast</b> 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。</li> <li>• <b>multicast</b> 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。</li> <li>• <b>vrf</b> キーワードと <b>vrf-name</b> 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。</li> </ul>
ステップ 5	<p><code>neighbor ip-address remote-as autonomous-system-number</code></p> <p>例： Router(config-router-af)# neighbor 172.21.1.2 remote-as 45000</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>

	コマンドまたはアクション	目的
ステップ6	<pre>neighbor ip-address activate</pre> <p><b>例:</b> Router(config-router-af)# neighbor 172.21.1.2 activate</p>	<p>ネイバーが IPv4 アドレス ファミリのプレフィックスをローカルルータと交換できるようにします。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ7	<pre>neighbor ip-address ha-mode graceful-restart [disable]</pre> <p><b>例:</b> Router(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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、<b>disable</b> キーワードを使用します。</li> <li>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。</li> <li>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。</li> </ul>
ステップ8	<pre>end</pre> <p><b>例:</b> Router(config-router-af)# end</p>	<p>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。</p>
ステップ9	<pre>show ip bgp neighbors [ip-address [received-routes   routes   advertised-routes   paths [regex]   dampened-routes   flap-statistics   received prefix-filter   policy [detail]]]</pre> <p><b>例:</b> Router# show ip bgp neighbors 172.21.1.2</p>	<p>(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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

## 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* [*regex*]  
| *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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<b>configure terminal</b>  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	<b>router bgp <i>autonomous-system-number</i></b>  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
<p><b>ステップ 4</b> <code>address-family ipv4 [unicast   multicast   vrf vrf-name]</code></p> <p><b>例 :</b> Router(config-router)# address-family ipv4 unicast</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>unicast</b> 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、<b>address-family ipv4</b> コマンドに <b>unicast</b> 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。</li> <li>• <b>multicast</b> 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。</li> <li>• <b>vrf</b> キーワードと <i>vrf-name</i> 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。</li> </ul>
<p><b>ステップ 5</b> <code>neighbor peer-group-name peer-group</code></p> <p><b>例 :</b> Router(config-router-af)# neighbor PG1 peer-group</p>	<p>BGP ピア グループを作成します。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
<p><b>ステップ 6</b> <code>neighbor peer-group-name remote-as autonomous-system-number</code></p> <p><b>例 :</b> Router(config-router-af)# neighbor PG1 remote-as 45000</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
<p><b>ステップ 7</b> <code>neighbor peer-group-name ha-mode graceful-restart [disable]</code></p> <p><b>例 :</b> Router(config-router-af)# neighbor PG1 ha-mode graceful-restart disable</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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、<b>disable</b> キーワードを使用します。</li> <li>• BGP セッションが確立された後でこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。</li> <li>• 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。</li> </ul>
<p><b>ステップ 8</b> <code>neighbor ip-address peer-group peer-group-name</code></p> <p><b>例 :</b> Router(config-router-af)# neighbor 172.16.1.2 peer-group PG1</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>



	コマンドまたはアクション	目的
ステップ9	<pre>end</pre> <p>例:</p> <pre>Router(config-router-af)# end</pre>	アドレスファミリー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ10	<pre>show ip bgp neighbors [ip-address [received-routes   routes   advertised-routes   paths [regex]   dampened-routes   flap-statistics   received prefix-filter   policy [detail]]]</pre> <p>例:</p> <pre>Router# show ip bgp neighbors 172.16.1.2</pre>	<p>(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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>

## 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 [regex] | 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 [regex] | 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およびメンテナンス」(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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>router bgp as-number</code>  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	<pre>address-family ipv4 [unicast   multicast   vrf vrf-name]</pre> <p>例 :</p> <pre>Router(config-router)# address-family ipv4 unicast</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>unicast</b> 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、<b>address-family ipv4</b> コマンドに <b>unicast</b> 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。</li> <li>• <b>multicast</b> 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。</li> <li>• <b>vrf</b> キーワードと <b>vrf-name</b> 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。</li> </ul>
ステップ 5	<pre>bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]</pre> <p>例 :</p> <pre>Router(config-router-af)# bgp dampening 30 1500 10000 120</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <i>half-life</i>、<i>reuse</i>、<i>suppress</i>、および <i>max-suppress-time</i> 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。</li> <li>• 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、<b>route-map</b> キーワードと <i>map-name</i> 引数を使用します。</li> </ul>
ステップ 6	<pre>end</pre> <p>例 :</p> <pre>Router(config-router-af)# end</pre>	<p>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。</p>

## 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

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** [*regex* *regex*] [*filter-list* *access-list*] [*ip-address* *mask*] [*longer-prefix*]
3. **clear ip bgp flap-statistics** [*neighbor-address* [*ipv4-mask*]] [*regex* *regex*] [*filter-list* *extcom-number*]
4. **show ip bgp dampened-paths**
5. **clear ip bgp** [*ipv4* {*multicast* | *unicast*}] [*ipv6* {*multicast* | *unicast*}] [*vpn4* *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 ファミリー プレフィックスのルート 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。インターフェイスで BFD を設定して、BFD プロセスを開始します。BFD プロセスの開始時に、隣接データベースにはエントリは作成されません。言い換えれば、BFD 制御パケットは送受信されません。適用可能なルーティングプロトコルの BFD サポートを設定すると、隣接作成が実行されます。BGP コンバージェンス時間を短縮するために BGP に対する BFD サポートを実装するには、最初の 2 つの作業を設定する必要があります。3 番目の作業は、BFD のモニタまたはトラブルシューティングに役立つ任意の作業です。

- 「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)
- 「Catalyst 7600 シリーズ ルータのモニタリングとトラブルシューティング」(P.41)

『Configuring BGP Neighbor Session Options』の章の「Configuring BFD for BGP IPv6 Neighbors」の項も参照してください。

### 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爾にする必要があります。
- BFD を配置する前に、ルータで BGP を設定する必要があります。使用しているルーティングプロトコルの高速コンバージェンスを実装する必要があります。高速コンバージェンスの設定については、お使いのバージョンの Cisco IOS ソフトウェアの IP ルーティングのマニュアルを参照してください。

### 制限事項

- 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、どちらの BFD ピアも 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 のネイバーは 1 ホップ以内に限定されます。マルチホップのコンフィギュレーション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.9) 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 BFD セッションパラメータを設定することによって、インターフェイスで BFD を設定する方法を示します。BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**

4. **bfd interval milliseconds min\_rx milliseconds multiplier interval-multiplier**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>enable</b>  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	<b>configure terminal</b>  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	<b>interface type number</b>  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	<b>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</b>  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	<b>end</b>  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 は、関連するすべてのルータで実行する必要があります。
- BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「[インターフェイスでの BFD セッションパラメータの設定](#)」(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 [regex] | 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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>router bgp autonomous-system-number</code>  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	<code>neighbor ip-address fall-over bfd</code>  例： Router(config-router)# neighbor 172.16.10.2 fall-over bfd	フェールオーバーに対する BFD サポートをイネーブルにします。
ステップ 5	<code>end</code>  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	<code>show bfd neighbors [details]</code>  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	<code>show ip bgp neighbors [ip-address [received-routes   routes   advertised-routes   paths [regex]   dampened-routes   flap-statistics   received prefix-filter   policy [detail]]]</code>  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。



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

Catalyst 7600 シリーズ ルータのモニタリングとトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

### 手順の概要

1. `enable`
2. `show bfd neighbors [details]`
3. `debug bfd [event | packet | ipc-error | ipc-event | oir-error | oir-event]`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<code>show bfd neighbors [details]</code>  例： Router# show bfd neighbors details	(任意) BFD 隣接関係データベースを表示します。 <ul style="list-style-type: none"><li>• <b>details</b> キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。</li></ul>
ステップ 3	<code>debug bfd [event   packet   ipc-error   ipc-event   oir-error   oir-event]</code>  例： Router# debug bfd packet	(任意) BFD パケットのデバッグ情報を表示します。

### 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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>snmp-server enable traps bgp</code> [[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。  • <b>state-changes</b> 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。 • <b>all</b> 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。 • <b>backward-trans</b> 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。 • <b>limited</b> 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。 • <b>threshold</b> キーワードと <b>prefix</b> 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	<code>exit</code>  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。

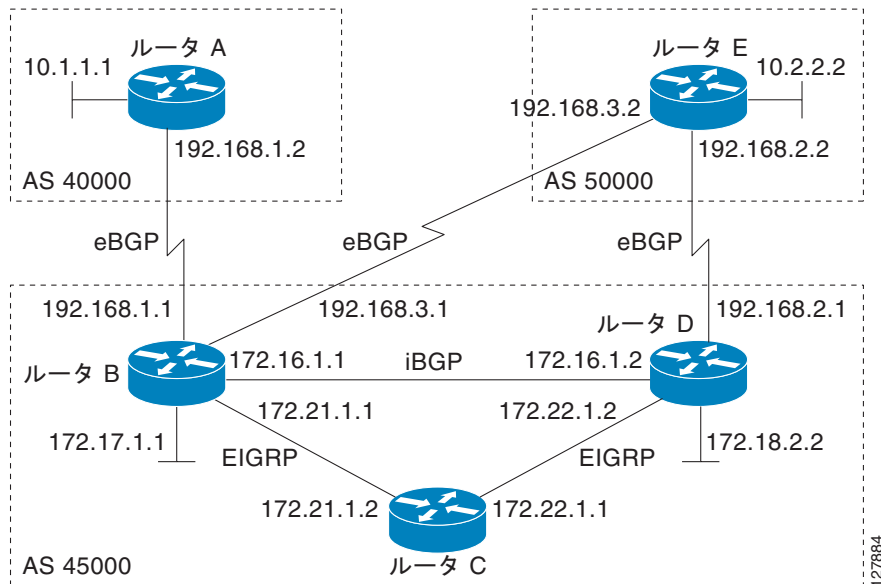
- 「[BGP を使用した MTR トポロジのアクティブ化](#)」 (P.42)
- 「[BGP を使用した MTR トポロジからのルートのインポート](#)」 (P.47)

## 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.12) 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。

## 制限事項

- 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	<b>enable</b>  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	<b>configure terminal</b>  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
<p><b>ステップ 3</b> <code>router bgp autonomous-system-number</code></p> <p><b>例 :</b> Router(config)# router bgp 45000</p>	<p>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。</p>
<p><b>ステップ 4</b> <code>scope {global   vrf vrf-name}</code></p> <p><b>例 :</b> Router(config-router)# scope global</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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、<b>global</b> キーワードを使用します。</li> <li>• 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、<b>vrf</b> キーワードと <i>vrf-name</i> 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。</li> </ul>
<p><b>ステップ 5</b> <code>neighbor {ip-address   peer-group-name}</code> <code>remote-as autonomous-system-number</code></p> <p><b>例 :</b> Router(config-router-scope)# neighbor 172.16.1.2 remote-as 45000</p>	<p>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。</p>
<p><b>ステップ 6</b> <code>neighbor {ip-address   peer-group-name}</code> <code>transport {connection-mode {active   passive}  </code> <code>path-mtu-discovery   multi-session  </code> <code>single-session}</code></p> <p><b>例 :</b> Router(config-router-scope)# neighbor 172.16.1.2 transport multi-session</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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、<b>connection-mode</b> キーワードを使用します。</li> <li>• 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、<b>path-mtu-discovery</b> キーワードを使用します。</li> <li>• 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、<b>multi-session</b> キーワードを使用します。</li> <li>• 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、<b>single-session</b> キーワードを使用します。</li> </ul>

コマンドまたはアクション	目的
<p><b>ステップ7</b> <code>address-family ipv4 [mdu   multicast   unicast]</code></p> <p><b>例:</b> Router(config-router-scope)# address-family ipv4</p>	<p>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。</p> <ul style="list-style-type: none"> <li>IPv4 MDT アドレス プレフィクスを指定するには、<b>mdu</b> キーワードを使用します。</li> <li>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、<b>multicast</b> キーワードを使用します。</li> <li>IPv4 ユニキャスト アドレス ファミリを指定するには、<b>unicast</b> キーワードを使用します。デフォルトでは、<b>address-family ipv4</b> コマンドに <b>unicast</b> 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。</li> <li>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。</li> </ul>
<p><b>ステップ8</b> <code>topology {base   topology-name}</code></p> <p><b>例:</b> Router(config-router-scope-af)# topology VIDEO</p>	<p>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。</p>
<p><b>ステップ9</b> <code>bgp tid number</code></p> <p><b>例:</b> Router(config-router-scope-af-topo)# bgp tid 100</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
<p><b>ステップ10</b> <code>neighbor ip-address activate</code></p> <p><b>例:</b> Router(config-router-scope-af-topo)# neighbor 172.16.1.2 activate</p>	<p>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。</p> <p><b>(注)</b> 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。</p>
<p><b>ステップ11</b> <code>neighbor {ip-address   peer-group-name} translate-topology number</code></p> <p><b>例:</b> Router(config-router-scope-af-topo)# neighbor 172.16.1.2 translate-topology 200</p>	<p>(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。</p> <ul style="list-style-type: none"> <li>ルータ上のトポロジを識別するために、<i>number</i> 引数にトポロジ ID を入力します。</li> </ul>
<p><b>ステップ12</b> <code>end</code></p> <p><b>例:</b> Router(config-router-scope-af-topo)# end</p>	<p>(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。</p>

コマンドまたはアクション	目的
<b>ステップ 13</b> <code>clear ip bgp topology</code> <i>{*   topology-name}</i> <i>{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]}</i> <i>[in [prefix-filter]   out   soft [in [prefix-filter]   out]]</i>  <b>例：</b> Router# <code>clear ip bgp topology VIDEO 45000</code>	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。
<b>ステップ 14</b> <code>show ip bgp topology</code> <i>{*   topology}</i> <b>summary</b>  <b>例：</b> Router# <code>show ip bgp topology VIDEO summary</code>	(任意) トポロジに関する BGP 情報を表示します。  <ul style="list-style-type: none"> <li>ほとんどの標準の BGP キーワードと引数は、topology キーワードの後に入力できます。</li> </ul> <b>(注)</b> 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、『 <a href="#">Cisco IOS IP Routing: BGP Command Reference</a> 』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実ポートする場合は、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実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 ファミリー 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。

## 制限事項

- 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	<b>enable</b>  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	<b>configure terminal</b>  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
<p><b>ステップ 3</b> <code>ip prefix-list list-name [seq seq-value] {deny network/length   permit network/length} [ge ge-value] [le le-value]</code></p> <p><b>例:</b> Router(config)# ip prefix-list TEN permit 10.2.2.0/24</p>	<p>IP プレフィクス リストを設定します。</p> <ul style="list-style-type: none"> <li>この例では、プレフィクス リスト TEN は、<b>match ip address</b> 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。</li> </ul>
<p><b>ステップ 4</b> <code>route-map map-name [permit   deny] [sequence-number]</code></p> <p><b>例:</b> Router(config)# route-map 10NET</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
<p><b>ステップ 5</b> <code>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...]}</code></p> <p><b>例:</b> Router(config-route-map)# match ip address prefix-list TEN</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
<p><b>ステップ 6</b> <code>exit</code></p> <p><b>例:</b> Router(config-route-map)# exit</p>	<p>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。</p>
<p><b>ステップ 7</b> <code>router bgp autonomous-system-number</code></p> <p><b>例:</b> Router(config)# router bgp 50000</p>	<p>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。</p>
<p><b>ステップ 8</b> <code>scope {global   vrf vrf-name}</code></p> <p><b>例:</b> Router(config-router)# scope global</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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、<b>global</b> キーワードを使用します。</li> <li>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、<b>vrf</b> キーワードと <i>vrf-name</i> 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。</li> </ul>
<p><b>ステップ 9</b> <code>address-family ipv4 [mdt   multicast   unicast]</code></p> <p><b>例:</b> Router(config-router-scope)# address-family ipv4</p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 10	<pre>topology {base   topology-name}</pre> <p>例： Router(config-router-scope-af)# topology VIDEO</p>	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	<pre>import topology {base   topology-name} [route-map map-name]</pre> <p>例： Router(config-router-scope-af-topo)# import topology VOICE route-map 10NET</p>	(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。 <ul style="list-style-type: none"> <li>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、<b>route-map</b> キーワードを使用できます。</li> </ul>
ステップ 12	<pre>end</pre> <p>例： Router(config-router-scope-af-topo)# end</p>	(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](#)」(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.51)
- 「[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.51)
- 「[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.52)
- 「[BGP ルート ダンプニングの設定：例](#)」(P.53)
- 「[BGP MIB サポートのイネーブル化：例](#)」(P.56)
- 「[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)

### 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

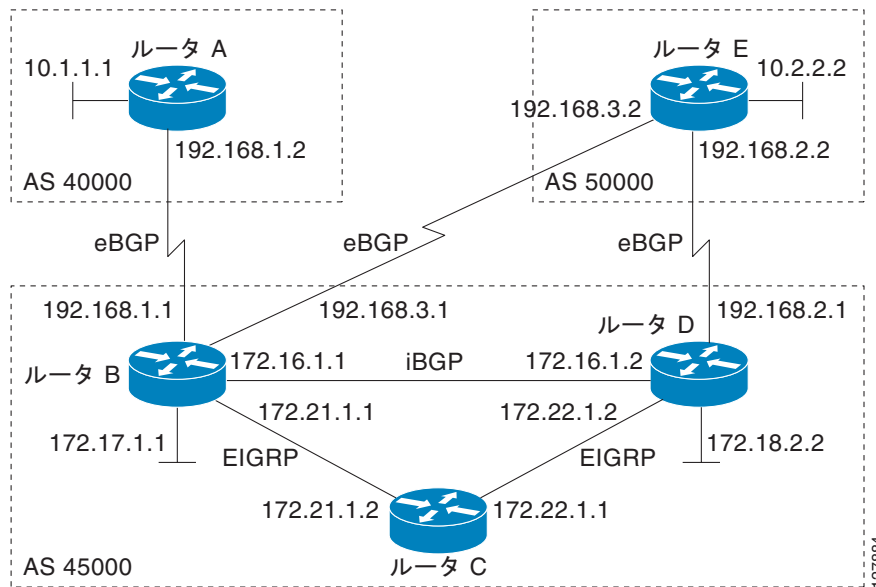


図 3 のルータ C にある個別の内部 BGP ネイバー 172.21.1.2 では BGP グレースフル リスタート機能はイネーブルになっているのに対して、図 3 のルータ D にある BGP ネイバー 172.16.1.2 では BGP グレースフル リスタートはディセーブルになっています。これは、ピアグループ PG1 のメンバであるためです。BGP グレースフル リスタートのディセーブル化は、ピアグループ PG1 のすべてのメンバについて設定されます。リスタート タイマーと失効パス タイマーは変更され、BGP セッションがリセットされます。

```

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
set dampening 15 750 2000 60
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

次の例は、ルータ A とルータ B で構成される単純な BGP ネットワークです。ルータ A のファストイーサネット インターフェイス 0/1 がルータ 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 モードから開始し、BFD の設定を示します。

### 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 からの **show bfd neighbors details** コマンドの出力で、BFD セッションが作成され、BFD サポートに対して BGP が登録されることを確認できます。この出力では、対応するコマンド出力が太字で表示されています。

### 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 のラインカードからの **show bfd neighbors details** コマンドの出力で、BFD セッションが作成されたことを確認できます。



(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** コマンドがラインカードで入力された場合、登録されたプロトコルは表示されません。

### 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** コマンドの出力で、BFD が BGP ネイバーに対してイネーブルになっていることを確認できます。

#### 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、次の設定例を示します。

- [「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」\(P.57\)](#)
- [「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」の項で、『[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。

## その他の参考資料

### 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	『 <a href="#">Cisco IOS IP Routing: BGP Command Reference</a> 』
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	『 <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a> 』の『 <a href="#">Cisco BGP Overview</a> 』モジュール
BGP の基本作業のコンセプトと設定の詳細。	『 <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a> 』の『 <a href="#">Configuring a Basic BGP Network</a> 』モジュール
SNMP 操作と SNMP 操作に関する情報	『 <a href="#">Cisco IOS Network Management Configuration Guide</a> 』の『 <a href="#">Configuring SNMP Support</a> 』の項

### 標準

標準	タイトル
MDT SAFI	『 <a href="#">MDT SAFI</a> 』

### 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、およびフィードバックの 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。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFC

RFC	タイトル
RFC 1657	『Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIPv2』
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
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>・テクニカル サポートを受ける</li> <li>・ソフトウェアをダウンロードする</li> <li>・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</li> <li>・ツールおよびリソースへアクセスする <ul style="list-style-type: none"> <li>- Product Alert の受信登録</li> <li>- Field Notice の受信登録</li> <li>- Bug Toolkit を使用した既知の問題の検索</li> </ul> </li> <li>・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</li> <li>・トレーニング リソースへアクセスする</li> <li>・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</li> </ul> <p>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。</p>	<p><a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a></p>

## 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情報については、『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。特定のコマンドに関する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、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、フィーチャ 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、特定の Cisco IOS ソフトウェア リリース トレインの中で特定の機能のサポートが導入された Cisco IOS ソフトウェア リリースだけを示します。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

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	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ネイバーごとの BGP グレースフルリスタート」(P.7)</li> <li>「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.24)</li> <li>「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)</li> <li>「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)</li> <li>「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.52)</li> </ul> <p>この機能によって、<b>ha-mode graceful-restart</b>、<b>neighbor ha-mode graceful-restart</b>、<b>show ip bgp neighbors</b> の各コマンドが導入または変更されました。</p>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「BGP MIB サポート」(P.9)</li> <li>「BGP MIB サポートのイネーブル化」(P.41)</li> <li>「BGP MIB サポートのイネーブル化：例」(P.56)</li> </ul> <p>この機能では、<b>snmp-server enable traps bgp</b> コマンドが導入されました。</p>

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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「BGP ノンストップ フォワーディング認識」 (P.4)</li> <li>• 「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.20)</li> <li>• 「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)</li> <li>• 「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.52)</li> <li>• 「BGP ルート ダンプニングの設定：例」 (P.53)</li> </ul> <p>この機能によって、<b>bgp graceful-restart</b>、<b>show ip bgp</b>、<b>show ip bgp neighbors</b> の各コマンドが導入または変更されました。</p>

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 の選択的アドレス トラッキング	12.4(4)T 12.2(33)SRB	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「選択的 BGP ネクストホップ ルート フィルタリング」(P.3)</li> <li>「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.17)</li> <li>「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.51)</li> </ul> <p>この機能によって、<b>bgp nexthop</b> コマンドおよび <b>neighbor fall-over</b> コマンドが変更されました。</p>
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	<p>双方向フォワーディング検出 (BFD) は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、さまざまなルーティングプロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。BGP 用の BFD を実装する主な利点は、再コンバージェンス時間が非常に短いことです。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「BGP 用の双方向フォワーディング検出 (BFD)」(P.9)</li> <li>「BFD を使用した BGP コンバージェンス時間の短縮」(P.38)</li> <li>「BGP ネットワークでの BFD の設定：例」(P.54)</li> </ul> <p>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。<b>bfd</b>、<b>neighbor fall-over</b>、<b>show bfd neighbors</b>、<b>show ip bgp neighbors</b>。</p>



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	<p>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差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層到着可能性情報 (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。</p> <p>12.2(33)SRB では、この機能は Cisco 7600 で導入されました。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「MTR に対する BGP サポート」 (P.12)</li> <li>• 「MTR に対する BGP サポートの設定」 (P.42)</li> <li>• 「BGP を使用した MTR トポロジのアクティブ化：例」 (P.56)</li> <li>• 「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)</li> </ul> <p>この機能によって、<b>address-family ipv4 (BGP)</b>、<b>bgp tid</b>、<b>clear ip bgp topology</b>、<b>import topology</b>、<b>neighbor translate-topology</b>、<b>neighbor transport</b>、<b>scope</b>、<b>show ip bgp topology</b>、<b>topology (BGP)</b> の各コマンドが導入または変更されました。</p>

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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「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)</li> <li>「BGP ネクストホップ アドレス トラッキングの設定」(P.14)</li> <li>「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)</li> <li>「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.51)</li> </ul> <p>この機能では、<b>bgp nexthop</b> コマンドが導入されました。</p>

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

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2005–2010 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2005–2012, シスコシステムズ合同会社.  
All rights reserved.