CHAPTER 8

拡張 BGP の設定

この章では、Cisco NX-OS スイッチでボーダー ゲートウェイ プロトコル（BGP）の拡張機能を設定する方法について説明します。

この章では、次の内容について説明します。

拡張 BGP の概要

BGP は、組織または自律システム（AS）間のループフリー ルーティングを実現する、ドメイン間ルーティング プロトコルです。Cisco NX-OS は BGP バージョン 4 をサポートしています。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応スイッチ（BGP ピア）との間で TCP セッションを確立するために、信頼できるトランスポート プロトコルとして TCP を使用します。外部組織に接続するときには、ルータが external BGP（eBGP; 外部 BGP）ピアリング セッションを作成します。同じ組織内の BGP ピアは、internal BGP（iBGP; 内部 BGP）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。

ここでは、次の内容について説明します。

ピア テンプレート

BGP ピア テンプレートを使用すると、共通のコンフィギュレーション ブロックを作成し、類似している BGP ピア間で再利用できます。各ブロックでは、ピアに継承させる一連の属性を定義できます。継承した属性の一部を上書きすることもできるので、非常に柔軟性のある方法で、繰り返しの多い BGP の設定を簡素化できます。

Cisco NX-OS は、3 種類のピア テンプレートを実装します。

- *peer-session* テンプレートでは、トランスポートの詳細、ピアのリモート AS 番号、セッション タイマーといった BGP セッション属性を定義します。peer-session テンプレートは、別の peer-session テンプレートから属性を継承することもできます（ローカル定義の属性によって、継承した peer-session 属性は上書きされます）。
- *peer-policy* テンプレートでは、着信ポリシー、発信ポリシー、フィルタ リスト、プレフィックス リストを含め、アドレス ファミリに依存する、ピアのポリシー要素を定義します。peer-policy テンプレートは、一連の peer-policy テンプレートからの継承が可能です。Cisco NX-OS は、継承設定のプリファレンス値で指定された順序で、これらの peer-policy テンプレートを評価します。最小値が大きい値よりも優先されます。
- *peer* テンプレートは、peer-session および peer-policy テンプレートからの継承が可能であり、ピアの定義を簡素化できます。peer テンプレートの使用は必須ではありませんが、peer テンプレートによって再利用可能なコンフィギュレーション ブロックが得られるので、BGP の設定を簡素化できます。

認証

BGP ネイバー セッションに認証を設定できます。この認証方式によって、ネイバーに送られる各 TCP セグメントに MD5 認証ダイジェストが追加され、不正なメッセージや TCP セキュリティ アタックから BGP が保護されます。

（注）　BGP ピア間で MD5 パスワードを一致させる必要があります。

ルート ポリシーおよび BGP セッションのリセット

BGP ピアにルート ポリシーを関連付けることができます。ルート ポリシーではルート マップを使用して、BGP が認識するルートを制御または変更します。着信または発信ルート アップデートに関するルート ポリシーを設定できます。ルート ポリシーはプレフィックス、AS_path 属性など、さまざまな条件で一致が必要であり、ルートを選択して受け付けるかまたは拒否します。ルート ポリシーでパス属性を変更することもできます。ルート ポリシーの詳細については、第 17 章「ポリシーベース ルーティングの設定」を参照してください。

BGP ピアに適用するルート ポリシーを変更する場合は、そのピアの BGP セッションをリセットする必要があります。Cisco NX-OS は、BGP ピアリング セッションのリセット方法として、次の 3 種類をサポートします。

- ハード リセット：ハード リセットでは、指定されたピアリング セッションが TCP 接続を含めて切断され、指定のピアからのルートが削除されます。このオプションを使用すると、BGP ネットワーク上のパケット フローが中断します。ハード リセットは、デフォルトでディセーブルです。
- ソフト再構成着信：ソフト再構成着信によって、セッションをリセットすることなく、指定されたピアのルーティング アップデートが開始されます。このオプションを使用できるのは、着信ルート ポリシーを変更する場合です。ソフト再構成着信の場合、ピアから受け取ったすべてのルートのコピーを保存したあとで、着信ルート ポリシーを介してルートが処理されます。着信ルート ポリシーをする場合、Cisco NX-OS は変更された着信ルート ポリシーを介して保存ルートを渡し、既存のピアリング セッションを切断することなく、ルート テーブルをアップデートします。ソフト再構成着信の場合、まだフィルタリングされていない BGP ルートの保存に、大量のメモリ リソースを使用する可能性があります。ソフト再構成着信は、デフォルトでディセーブルです。
- ルート リフレッシュ：ルート リフレッシュでは、着信ルート ポリシーの変更時に、サポートするピアにルート リフレッシュ要求を送信することによって、着信ルーティング テーブルがダイナミックにアップデートされます。リモート BGP ピアは新しいルート コピーで応答し、ローカル BGP スピーカが変更されたルート ポリシーでそれを処理します。Cisco NX-OS はピアに、プレフィックスの発信ルート リフレッシュを自動的に送信します。
- BGP ピアは、BGP ピア セッションの確立時に、BGP 機能ネゴシエーションの一部として、ルート リフレッシュ機能をアドバタイズします。ルート リフレッシュは優先オプションであり、デフォルトでイネーブルです。

（注） BGP はさらに、ルート再配布、ルート集約、ルート ダンプニングなどの機能にルート マップを使用します。ルート マップの詳細については、第 16 章「Route Policy Manager の設定」を参照してください。

eBGP

eBGP を使用すると、異なる AS からの BGP ピアを接続し、ルーティング アップデートを交換できます。外部ネットワークへの接続によって、自分のネットワークから他のネットワークへ、またインターネットを介して、トラフィックを転送できます。

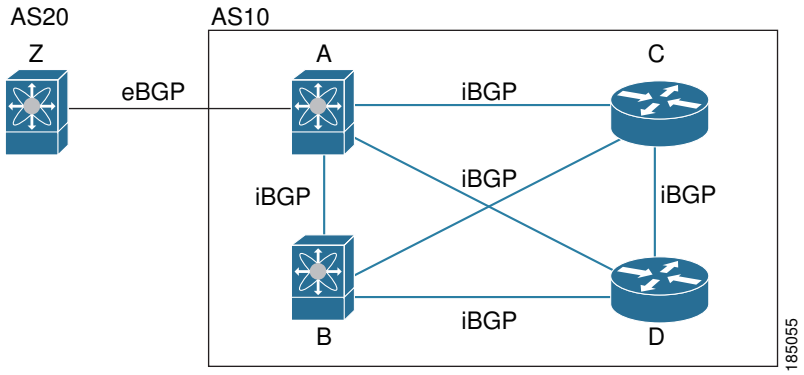
eBGP ピアリング セッションの確立には、ループバック インターフェイスを使用します。ループバック インターフェイスは、インターフェイス フラップが発生する可能性が小さいからです。インターフェイス フラップが発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フェールオーバー、AS パス属性のサイズ制限については、「eBGP の設定」（P.8-23）を参照してください。

iBGP

iBGP を使用すると、同じ AS 内の BGP ピアを接続できます。iBGP はマルチホーム BGP ネットワーク（同じ外部 AS に対して複数の接続があるネットワーク）に使用できます。

図 8-1 に、大きい BGP ネットワークの中の iBGP ネットワークを示します。

図 8-1　　iBGP ネットワーク



iBGP ネットワークはフルメッシュです。各 iBGP ピアは、ネットワーク ループを防止するために、他のすべての iBGP ピアに対して直接接続されています。

（注）　iBGP ネットワークでは別個のインテリア ゲートウェイ プロトコルを設定する必要があります。

ここでは、次の内容について説明します。

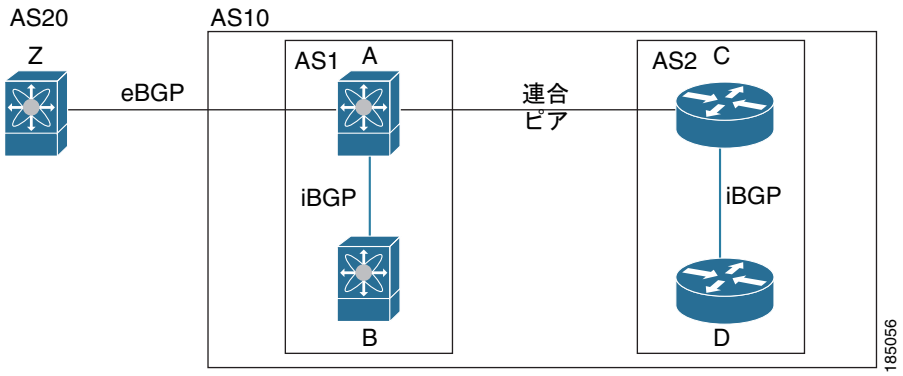
- 「AS 連合」（P.8-4）
- 「ルート リフレクタ」（P.8-5）

AS 連合

フルメッシュの iBGP ネットワークは、iBGP ピア数が増えるにしたがって複雑になります。AS を複数のサブ AS に分割し、それを 1 つの連合としてまとめることによって、iBGP メッシュを緩和できます。連合は、同じ AS 番号を使用して外部ネットワークと通信する、iBGP ピアからなるグループです。各サブ AS はその中ではフルメッシュであり、同じ連合内の他のサブ AS に対する少数の接続があります。

図 8-2 に、図 8-1 の BGP ネットワークを 2 つのサブ AS に分割し、1 つの連合にしたものを示します。

図 8-2　AS 連合



この例では、AS10 が 2 つの AS（AS1 および AS2）に分割されています。各サブ AS はフルメッシュですが、サブ AS 間のリンクは 1 つだけです。AS 連合を使用することによって、図 8-1 のフルメッシュ AS に比べて、リンク数を少なくできます。

ルート リフレクタ

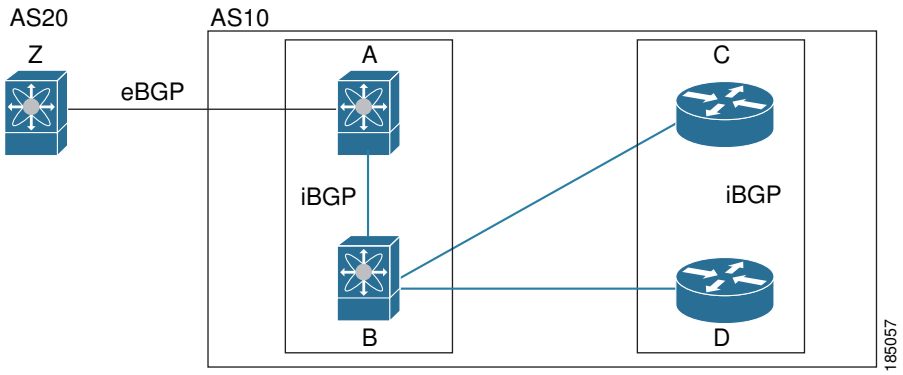
ルート リフレクタ構成を使用することによって、iBGP メッシュを緩和することもできます。ルート リフレクタは学習したルートをネイバーに渡すことで、すべての iBGP ピアをフルメッシュにしなくてもすむようにします。

図 8-1 に、メッシュの iBGP スピーカを 4 つ使用する（ルータ A、B、C、D）、単純な iBGP 構成を示します。ルート リフレクタを使用しなかった場合、外部ネイバーからルートを受け取ったルータ A は、3 つの iBGP ネイバーのすべてにルートをアドバタイズします。

ある iBGP ピアをルート リフレクタとして設定すると、そのピアが iBGP で学習したルートを一連の iBGP ネイバーに渡す役割を担います。

図 8-3 では、ルータ B がルート リフレクタです。ルータ A からアドバタイズされたルートを受信したルート リフレクタは、そのルートをルータ C および D にアドバタイズ（リフレクション）します。ルータ A からルータ C および D の両方にアドバタイズする必要がなくなります。

図 8-3　ルート リフレクタ



ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。ルート リフレクタのクライアント ピアとして動作するように、すべての iBGP ピアを設定する必要はありません。ただし、完全な BGP アップデートがすべてのピアに届くように、非クライアント ピアはフルメッシュとして設定する必要があります。

機能ネゴシエーション

BGP スピーカは機能ネゴシエーション機能を使用することによって、ピアがサポートする BGP 拡張機能について学習できます。機能ネゴシエーションによって、リンクの両側の BGP ピアがサポートする機能セットだけを BGP に使用させることができます。

BGP ピアが機能ネゴシエーションをサポートしない場合で、なおかつアドレス ファミリが IPv4 として設定されている場合、Cisco NX-OS は機能ネゴシエーションを行わずに、ピアとの新規セッションを試みます。他のマルチプロトコル設定（IPv6 など）の場合は、機能ネゴシエーションが不可欠です。

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上でのフラッピング ルートの伝播を最小限に抑える BGP 機能です。ルート フラップが発生するのは、使用可能ステートと使用不能ステートが短時間で次々切り替わる場合です。

AS1、AS2、および AS3 という 3 つの BGP AS からなるネットワークの場合について考えてみます。AS1 のルートがフラップした（使用不能になった）とします。ルート ダンプニングを使用しない場合、AS1 は AS2 に回収メッセージを送信します。AS2 は AS3 にその回収メッセージを伝達します。フラッピング ルートが再び発生すると、AS1 から AS2 にアドバタイズメント メッセージを送信し、AS2 は AS3 にそのアドバタイズメントを送信します。ルートの使用不能と使用可能が繰り返されると、AS1 は多数の回収メッセージおよびアドバタイズメント メッセージを送信することになり、それが他の AS に伝播します。

ルート ダンプニングによって、フラッピングを最小限に抑えることができます。ルート フラップが発生したとします。（ルート ダンプニングがイネーブルの）AS2 がルートにペナルティとして 1000 を割り当てます。AS2 は引き続き、ネイバーにルートの状態をアドバタイズします。ルート フラップが発生するたびに、AS2 がペナルティ値を追加します。ルート フラップが頻繁に発生して、ペナルティが設定可能な抑制限度を超えると、AS2 はフラップ回数に関係なく、ルートのアドバタイズを中止します。その結果、ルートが減衰（ダンプニング）します。

ルートに与えられたペナルティは、再使用限度に達するまで減衰します。その時点で、AS2 は再びルートをアドバタイズします。再使用限度が 50% になると、AS2 はそのルートのダンプニング情報を削除します。

（注） ルート ダンプニングがイネーブルの場合は、ピアのリセットによってルートが回収されても、リセット中の BGP にはペナルティは適用されません。

ロード シェアリングおよびマルチパス

BGP はルーティング テーブルに、同じ宛先プレフィックスに到達する複数の等コスト eBGP または iBGP パスを組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

BGP ベストパス アルゴリズムでは、次の属性が同じ場合に、等コスト パスと見なされます。

- 重量

- ローカル プリファレンス
- AS_path
- オリジン コード
- multi-exit discriminator（MED）
- BGP ネクスト ホップまでの IGP コスト

BGP はこれら複数のパスの中から、最適パスとして 1 つだけ選択し、そのパスを BGP ピアにアドバタイズします。

（注）　異なる AS 連合から受け取ったパスは、外部 AS_path 値およびその他の属性が同じ場合に、等コストパスと見なされます。

（注）　iBGP マルチパスに関してルート リフレクタを設定すると、ルート リフレクタが、選択された最適パスをピアにアドバタイズします。そのパスのネクスト ホップは変更されません。

ルート集約

集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 という固有性の強い 3 つのアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

アドバタイズするルートが少なくなるように、BGP ルート テーブルでは集約プレフィックスを使用します。

（注）　Cisco NX-OS は、自動ルート集約をサポートしません。

ルート集約はフォワーディング ループにつながる可能性があります。この問題を回避するために、集約アドレスのアドバタイズメントを生成するときに、BGP はローカル ルーティング テーブルに、その集約アドレスに対応するサマリー廃棄ルートを自動的に組み込みます。BGP はサマリー廃棄のアドミニストレーティブ ディスタンスを 220 に設定し、ルート タイプを廃棄に設定します。BGP はネクスト ホップ解決に廃棄ルートを使用しません。

BGP 条件付きアドバタイズメント

BGP 条件付きアドバタイズメントを使用すると、プレフィックスが BGP テーブルに存在するかどうかに基づいてルートをアドバタイズまたは撤回するように BGP を設定できます。この機能は、たとえば、BGP でいずれかのプロバイダーにプレフィックスをアドバタイズするようなマルチホーム ネットワーク（他のプロバイダーからの情報が存在しない場合のみ）で便利です。

AS1、AS2、および AS3 という 3 つの BGP AS からなるネットワークの例について考えてみます。この例で、AS1 と AS3 はインターネットと AS2 に接続しています。条件付きアドバタイズメントを使用しない場合、AS2 はすべてのルートを AS1 と AS3 の両方にプロパゲートします。条件付きアドバタイズメントを使用すれば、AS1 からのルートが存在しない場合のみ（たとえば AS1 へのリンクがダウンした場合）、特定のルートを AS3 にアドバタイズするように AS2 を設定できます。

BGP 条件付きアドバタイズメントでは、設定されたルート マップに一致する各ルートに、存在テストまたは非存在テストが追加されます。詳細については、「BGP 条件付きアドバタイズメントの設定」（P.8-31）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

BGP は、インストールされているルートのネクスト ホップ アドレスをモニタして、ネクスト ホップの到達可能性の確認、および BGP 最適パスの選択、インストール、検証を行います。BGP ネクストホップ アドレスのトラッキングを行うと、ネクストホップの到達可能性に影響を及ぼす可能性のあるルート変更が RIB で行われたときに確認プロセスをトリガーすることで、このようなネクストホップ到達可能性テストの速度が向上します。

ネクストホップ情報が変更されると、BGP は RIB から通知を受信します（イベント駆動型の通知）。BGP は、次のいずれかのイベントが発生したときに通知を受けます。

- ネクスト ホップが到達不能になった。
- ネクスト ホップが到達可能になった。
- ネクスト ホップへの完全な繰り返し IGP メトリックが変更される。
- ファースト ホップの IP アドレスまたはファースト ホップのインターフェイスが変更される。
- ネクスト ホップが接続された。
- ネクスト ホップが接続解除された。
- ネクスト ホップがローカル アドレスになった。
- ネクスト ホップが非ローカル アドレスになった。

（注）　到達可能性および繰り返しメトリック イベントは、最適パスの再計算をトリガーします。

RIB からのイベント通知は、クリティカルおよび非クリティカルとして分類されます。クリティカルおよび非クリティカル イベントの通知は、別々のバッチで送信されます。ただし、非クリティカル イベントが保留中であり、クリティカル イベントを読み込む要求がある場合は、非クリティカル イベントがクリティカル イベントとともに送信されます。

- クリティカル イベントは、ネクスト ホップの到達可能性（到達可能と到達不能）、接続性（接続と非接続）、および局在性（ローカルと非ローカル）に関係があります。これらのイベントの通知は遅延しません。
- 非クリティカル イベントには、IGP メトリックの変更のみが含まれます。

詳細については、「BGP ネクスト ホップ アドレス トラッキングの設定」（P.8-21）を参照してください。

ルートの再配布

スタティック ルートまたは他のプロトコルからのルートを再配布するように、BGP を設定できます。再配布を指定してルート ポリシーを設定し、BGP に渡されるルートを制御します。ルート ポリシーを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。詳細については、第 16 章「Route Policy Manager の設定」を参照してください。

BFD

この機能では、双方向フォワーディング検出（BFD）をサポートします。BFD は、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータ プレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

BGP の BFD は eBGP シングルホップ ピアおよび iBGP シングルホップ ピアでサポートされます。BFD を使用している iBGP シングルホップ ピアでは、ネイバー コンフィギュレーション モードで update-source オプションを設定する必要があります。BFD は他の iBGP ピアまたはマルチ ホップ eBGP ピアではサポートされていません。

BFD は、次のタイプのインターフェイスでサポートされます。

- L3 物理およびサブインターフェイス
- L3 ポートチャネルおよびサブインターフェイス
- SVI

BGP の BFD はポートチャネル上の認証またはリンクごとの BFD セッションはサポートしません。

詳細については、第 9 章「BGP の双方向フォワーディング検出の設定」を参照してください。

BGP の調整

BGP タイマーによって、さらにベストパス アルゴリズムの調整によって、BGP のデフォルト動作を変更できます。

ここでは、次の内容について説明します。

BGP タイマー

BGP では、ネイバー セッションおよびグローバル プロトコル イベントにさまざまなタイプのタイマーを使用します。確立されたセッションごとに、最低限 2 つのタイマーがあります。定期的にキープアライブ メッセージを送信するためのタイマー、さらに想定時間内にピアのキープアライブが届かなかった場合に、セッションをタイムアウトさせるためのタイマーです。また、個々の機能を処理するための、その他のタイマーがあります。これらのタイマーは通常、秒単位で設定します。タイマーには、異なる BGP ピアで同じタイマーが異なるタイミングでスタートするように、ランダム アジャストメントが組み込まれています。

ベストパス アルゴリズムの調整

オプションの設定パラメータによって、ベストパス アルゴリズムのデフォルト動作を変更できます。たとえば、アルゴリズムでの MED 属性およびルータ ID の扱い方を変更できます。

マルチプロトコル BGP

Cisco NX-OS の BGP は、複数のアドレス ファミリをサポートします。マルチプロトコル BGP（MP-BGP）は、アドレス ファミリに応じて異なるルート セットを伝送します。BGP ではたとえば、IPv4 ユニキャスト ルーティング用のルート セットを 1 つ、IPv4 マルチキャスト ルーティング用の

ルート セットを 1 つ、さらに IPv6 マルチキャスト ルーティング用のルート セットを 1 つ伝送できます。IP マルチキャスト ネットワークではリバース パス フォワーディング（RPF）のチェックに MP-BGP を使用できます。

（注）　マルチキャスト BGP ではマルチキャスト状態情報をプロパゲートしないため、プロトコル独立マルチキャスト（PIM）などのマルチキャスト プロトコルが必要です。

マルチプロトコル BGP 設定をサポートするには、ルータ アドレスファミリおよびネイバー アドレス ファミリの各コンフィギュレーション モードを使用します。MP-BGP では、設定されたアドレス ファミリごとに別々の RIB が維持されます（ユニキャスト RIB と、BGP のマルチキャスト RIB など）。

マルチプロトコル BGP ネットワークは下位互換性がありますが、マルチプロトコル拡張機能をサポートしない BGP ピアは、アドレス ファミリ ID 情報など、マルチプロトコル拡張機能が伝送するルーティング情報を転送できません。

拡張 BGP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BGP には、LAN Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。 （注）　レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP 機能をイネーブルにする必要があります（「BGP 機能のイネーブル化」（P.7-11）を参照）。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。
- ネイバー関係を作成しようとするピアに到達可能でなければなりません（Interior Gateway Protocol（IGP）、スタティック ルート、直接接続など）。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを明示的に設定する必要があります。

BGP に関する注意事項および制限事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- ダイナミック AS 番号プレフィックス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。

- AS 連合でプレフィックス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィックス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ Time-to-Live（TTL; 存続可能時間）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィックス設定オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。
- update-source を設定し、eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ルート マップを指定します。
- VRF 内で BGP ルータ ID を設定します。
- キープアライブおよびホールド タイマーの値を小さくすると、ネットワークでセッション フラップが発生する可能性があります。

デフォルト設定

表 8-1 に、BGP パラメータのデフォルト設定を示します。

表 8-1　デフォルトの BGP パラメータ

パラメータ	デフォルト
BGP 機能	ディセーブル
キープアライブ インターバル	60 秒
ホールド タイマー	180 秒

拡張 BGP の設定

ここでは、拡張 BGP の設定方法について説明します。内容は次のとおりです。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

BGP セッション テンプレートの設定

BGP セッション テンプレートを使用すると、類似した設定が必要な複数の BGP ピアで、BGP の設定を簡素化できます。BGP テンプレートによって、共通のコンフィギュレーション ブロックを再利用できます。先に BGP テンプレートを設定し、その後で BGP ピアにテンプレートを適用します。

BGP セッション テンプレートでは、継承、パスワード、タイマー、セキュリティなどのセッション属性を設定できます。

peer-session テンプレートは、別の peer-session テンプレートからの継承が可能です。第 3 のテンプレートから継承するように第 2 テンプレートを設定できます。さらに最初のテンプレートもこの第 3 のテンプレートから継承させることができます。この間接継承を続けることができる peer-session テンプレートの数は、最大 7 つです。

ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

（注）　テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、**default** 形式のコマンドを使用する必要があります。

手順の概要

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

5. **timers** *keepalive* ***hold***
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **inherit peer-session** *template-name*
9. （任意）**description** *text*
10. （任意）**show bgp peer-session** *template-name*
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *autonomous-system-number*
	
	Example:
	`switch(config)# router bgp 65536`
	`switch(config-router)#`
		BGP をイネーブルにして、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**template peer-session** *template-name*
	
	Example:
	`switch(config-router)# template peer-session BaseSession`
	`switch(config-router-stmp)#`
		peer-session テンプレート コンフィギュレーション モードを開始します。

ステップ 4	**password** *number password* **Example:** `switch(config-router-stmp)# password 0 test`	（任意）ネイバーにクリアテキスト パスワード *test* を追加します。パスワードは 3DES（タイプ 3 暗号形式）で保存および表示されます。
ステップ 5	**timers** *keepalive hold* **Example:** `switch(config-router-stmp)# timers 30 90`	（任意）peer-session テンプレートに BGP キープアライブおよびホールド タイマー値を追加します。 デフォルトのキープアライブ インターバルは 60 です。デフォルトのホールド タイムは 180 です。

ステップ 6	**exit**
	
	Example:
	`switch(config-router-stmp)# exit`
	`switch(config-router)#`
		peer-session テンプレート コンフィギュレーション モードを終了します。

ステップ 7	**neighbor** *ip-address* **remote-as** *as-number*
	
	Example:
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65536`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

	コマンド	目的

ステップ 8	**inherit peer-session** *template-name*
	
	Example:
	switch(config-router-neighbor)# inherit peer-session BaseSession
	switch(config-router-neighbor)
		ピアに peer-session テンプレートを適用します。

ステップ 9	**description** *text*
	
	Example:
	switch(config-router-neighbor)# description Peer Router A
	switch(config-router-neighbor)
		（任意）ネイバーの説明を追加します。

ステップ 10	**show bgp peer-session** *template-name* **Example:** switch(config-router-neighbor)# show bgp peer-session BaseSession	（任意）peer-policy テンプレートを表示します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config-router-neighbor)# copy running-config startup-config	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 3000 Series Command Reference,*』を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BaseSession
switch(config-router-stmp)# timers 30 90
switch(config-router-stmp)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# description Peer Router A
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# copy running-config startup-config
```

BGP peer-policy テンプレートの設定

peer-policy テンプレートを設定すると、特定のアドレス ファミリに対応する属性を定義できます。各 peer-policy テンプレートにプリファレンスを割り当て、指定した順序でテンプレートが継承されるようにします。ネイバー アドレス ファミリでは最大 5 つの peer-policy テンプレートを使用できます。

Cisco NX-OS は、プリファレンス値を使用して、アドレス ファミリの複数のピア ポリシーを評価します。プリファレンス値が最小のものが最初に評価されます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

peer-policy テンプレートでは、AS-path フィルタ リスト、プレフィックス リスト、ルート リフレクション、ソフト再構成など、アドレス ファミリ固有の属性を設定できます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

（注）　テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer-policy** *template-name*
4. **advertise-active-only**
5. **maximum-prefix** *number*
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **address-family** {**ipv4** | **ipv6**} {**multicast** | **unicast**}
9. **inherit peer-policy** *template-name preference*
10. （任意）**show bgp peer-policy** *template-name*
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	**template peer-policy** *template-name* **Example:** switch(config-router)# template peer-policy BasePolicy switch(config-router-ptmp)#	peer-policy テンプレートを作成します。
ステップ 4	**advertise-active-only** **Example:** switch(config-router-ptmp)# advertise-active-only	（任意）アクティブ ルートだけをピアにアドバタイズします。

	コマンド	目的
ステップ 5	**maximum-prefix** *number* **Example:** `switch(config-router-ptmp)# maximum-prefix 20`	（任意）このピアに認めるプレフィックスの最大数を設定します。

ステップ 6	**exit**
	
	Example:
	`switch(config-router-ptmp)# exit`
	`switch(config-router)#`
		peer-policy テンプレート コンフィギュレーション モードを終了します。

ステップ 7	**neighbor** *ip-address* **remote-as** *as-number*
	
	Example:
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65536`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

ステップ 8	**address-family** {**ipv4** | **ipv6**} {**multicast** | **unicast**}
	
	Example:
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		指定のアドレス ファミリに対しグローバル アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 9	**inherit peer-policy** *template-name preference* **Example:** `switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1`	ピア アドレス ファミリ設定に peer-policy テンプレートを適用し、このピア ポリシーのプリファレンス値を割り当てます。
ステップ 10	**show bgp peer-policy** *template-name* **Example:** `switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy`	（任意）peer-policy テンプレートを表示します。
ステップ 11	**copy running-config startup-config** **Example:** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 3000 Series Command Reference,*』を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

BGP peer-policy テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BasePolicy
switch(config-router-ptmp)# maximum-prefix 20
switch(config-router-ptmp)# exit
switch(config-router)# neighbor 192.168.1.1 remote-as 65536
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP peer テンプレートの設定

BGP peer テンプレートを設定すると、1 つの再利用可能なコンフィギュレーション ブロックで、セッション属性とポリシー属性を結合することができます。peer テンプレートも、peer-session または peer-policy テンプレートを継承できます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。ネイバーに設定できる peer テンプレートは 1 つだけですが、peer テンプレートは peer-session および peer-policy テンプレートを継承できます。

peer テンプレートは、eBGP マルチホップ TTL、最大プレフィックス数、ネクスト ホップ セルフ、タイマーなど、セッション属性およびアドレス ファミリ属性をサポートします。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

（注）　テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer** *template-name*
4. （任意）**inherit peer-session** *template-name*
5. （任意）**address-family** {**ipv4** | **ipv6**} {**multicast** | **unicast**}
6. （任意）**inherit peer** *template-name*
7. **exit**
8. （任意）**timers** *keepalive hold*
9. **exit**
10. **neighbor** *ip-address*
11. **inherit peer** *template-name*
12. （任意）**timers** *keepalive hold*
13. （任意）**show bgp peer-template** *template-name*
14. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 65536	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**template peer** *template-name* **Example:** switch(config-router)# template peer BasePeer switch(config-router-neighbor)#	peer テンプレート コンフィギュレーション モードを開始します。
ステップ 4	**inherit peer-session***n* *template-name* **Example:** switch(config-router-neighbor)# inherit peer-session BaseSession	（任意）peer テンプレートで peer-session テンプレートを継承します。
ステップ 5	**address-family** {**ipv4** | **ipv6**}{**multicast** | **unicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	（任意）指定のアドレス ファミリに対しグローバル アドレス ファミリ コンフィギュレーション モードを設定します。
ステップ 6	**inherit peer** *template-name* **Example:** switch(config-router-neighbor-af)# inherit peer BasePolicy	（任意）ネイバー アドレス ファミリ設定に peer テンプレートを適用します。
ステップ 7	**exit** **Example:** switch(config-router-neighbor-af)# exit switch(config-router-neighbor)#	BGP ネイバー アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 8	**timers** *keepalive hold* **Example:** switch(config-router-neighbor)# timers 45 100	（任意）ピアに BGP タイマー値を追加します。 これらの値によって、peer-session テンプレート、BaseSession のタイマー値が上書きされます。
ステップ 9	**exit** **Example:** switch(config-router-neighbor)# exit switch(config-router)#	BGP peer テンプレート コンフィギュレーション モードを終了します。
ステップ 10	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

	コマンド	目的
ステップ 11	**inherit peer** *template-name* **Example:** switch(config-router-neighbor)# inherit peer BasePeer	peer テンプレートを継承します。
ステップ 12	**timers** *keepalive hold* **Example:** switch(config-router-neighbor)# timers 60 120	（任意）このネイバーに BGP タイマー値を追加します。 これらの値によって、peer テンプレートおよび peer-session テンプレートのタイマー値が上書きされます。
ステップ 13	**show bgp peer-template** *template-name* **Example:** switch(config-router-neighbor-af)# show bgp peer-template BasePeer	（任意）peer テンプレートを表示します。
ステップ 14	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 3000 Series Command Reference,*』を参照してください。

BGP peer テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer BasePeer
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

プレフィックス ピアリングの設定

BGP では IPv4 および IPv6 の両方のプレフィックスを使用したピア セットの定義がサポートされます。この機能を使用すると、各ネイバーを設定に追加する必要がありません。

プレフィックス ピアリングを定義する場合は、プレフィックスとともにリモート AS 番号を指定する必要があります。プレフィックス ピアリングが設定されている許容最大ピア数を超えない場合、BGP はプレフィックスおよび AS から接続するピアを受け付けます。

プレフィックス ピアリングに含まれている BGP ピアが切断されると、Cisco NX-OS は定義されているプレフィックス ピア タイムアウト値まで、ピア構造を維持します。この場合、そのプレフィックス ピアリングのすべてのスロットを他のピアが使い果たした結果、ブロックされるという危険性を伴わずに、確立されたピアのリセットまたは再接続が可能になります。

BGP プレフィックス ピアリング タイムアウト値を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
timers prefix-peer-timeout *value* **Example:** switch(config-router-neighbor)# timers prefix-peer-timeout 120	プレフィックス ピアリングのタイムアウト値を設定します。指定できる範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。

ピアの最大数を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-peers *value* **Example:** switch(config-router-neighbor)# maximum-peers 120	このプレフィックス ピアリングの最大ピア数を設定します。指定できる範囲は 1 ～ 1000 です。

最大 10 のピアを受け付けるプレフィックス ピアリングの設定例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 65536
switch(config-router-neighbor)# maximum-peers 10
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

所定のプレフィックス ピアリングの設定の詳細とともに、現在受け付けられているインスタンスのリスト、アクティブ ピア数、最大同時ピア数、および受け付けたピアの合計数を表示するには、**show ip bgp neighbor** コマンドを使用します。

BGP 認証の設定

MD5 ダイジェストを使用して、ピアからのルート アップデートを認証するように BGP を設定できます。

MD5 認証を使用するように BGP を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
password [**0** | **3** | **7**] *string* **Example:** switch(config-router-neighbor)# password BGPpassword	MGP ネイバー セッションの MD5 パスワードを設定します。

BGP セッションのリセット

BGP のルート ポリシーを変更した場合は、関連付けられた BGP ピア セッションをリセットする必要があります。BGP ピアがルート リフレッシュをサポートしない場合は、着信ポリシー変更に関するソフト再構成を設定できます。Cisco NX-OS は自動的に、セッションのソフト リセットを試みます。

ソフト再構成着信を設定するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
soft-reconfiguration inbound **Example:** `switch(config-router-neighbor-af)# soft-reconfiguration inbound`	着信 BGP ルート アップデートを格納するために、ソフト再構成をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

BGP ネイバー セッションをリセットするには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear bgp {**ip** | **ipv6**} {**unicast** | **multicast**} *ip-address* **soft** {**in** | **out**} **Example:** `switch# clear bgp ip unicast 192.0.2.1 soft in`	TCP セッションを切断しないで、BGP セッションをリセットします。

ネクスト ホップ アドレスの変更

次の方法で、ルート アドバタイズメントで使用するネクスト ホップ アドレスを変更できます。

- ネクストホップ計算をディセーブルにして、ローカル BGP スピーカ アドレスをネクストホップ アドレスとして使用します。
- ネクスト ホップ アドレスをサードパーティ アドレスとして設定します。この機能は、元のネクスト ホップ アドレスがルートの送り先のピアと同じサブネット上にある場合に使用します。この機能を使用すると、フォワーディング時に余分なホップを節約できます。

ネクストホップ アドレスを変更するには、コマンド アドレス ファミリ コンフィギュレーション モードで次のパラメータを使用します。

コマンド	目的
next-hop-self **Example:** `switch(config-router-neighbor-af)# next-hop-self`	ルート アップデートのネクスト ホップ アドレスとして、ローカル BGP スピーカ アドレスを使用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
next-hop-third-party **Example:** `switch(config-router-neighbor-af)# next-hop-third-party`	ネクスト ホップ アドレスをサードパーティ アドレスとして設定します。このコマンドは、**next-hop-self** を設定されていないシングルホップ EBGP ピアに使用します。

BGP ネクスト ホップ アドレス トラッキングの設定

BGP ネクスト ホップ アドレス トラッキングはデフォルトでイネーブルであり、ディセーブルにすることができません。

BGP ネクスト ホップ トラッキングのパフォーマンスを向上するために、RIB チェック間の遅延インターバルを変更できます。BGP ネクスト ホップの到達可能性に影響を及ぼすルートのクリティカル タイマーを設定したり、BGP テーブルのその他のルートすべての非クリティカル タイマーを設定したりできます。

BGP ネクストホップ アドレス トラッキングを変更するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
nexthop trigger-delay {**critical** | **non-critical**} *milliseconds* **Example:** `switch(config-router-af)# nexthop trigger-delay critical 5000`	クリティカルなネクスト ホップの到達可能性ルートおよび非クリティカルなルートについて、ネクスト ホップ アドレス トラッキングの遅延タイマーを指定します。指定できる範囲は 1 ～ 4294967295 ミリ秒です。クリティカル タイマーのデフォルトは 3000 です。非クリティカル タイマーのデフォルトは 10000 です。
nexthop route-map *name* **Example:** `switch(config-router-af)# nexthop route-map nextHopLimits`	BGP ネクスト ホップ アドレスが一致するルート マップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ネクスト ホップ フィルタリングの設定

BGP ネクスト ホップ フィルタリングを使用すると、RIB でネクスト ホップ アドレスがチェックされるときにそのネクスト ホップ アドレスの基盤となるルートがルート マップを経由します。ルート マップでそのルートが拒否されると、ネクスト ホップ アドレスは到達不能として扱われます。

BGP は、ルート ポリシーによって拒否されたすべてのネクスト ホップを無効であるとマークし、無効なネクスト ホップ アドレスを使用するルートについて最適パスを計算しません。

BGP ネクスト ホップ フィルタリングを設定するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
nexthop route-map *name* **Example:** `switch(config-router-af)# nexthop route-map nextHopLimits`	BGP ネクスト ホップ ルートが一致するルート マップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

機能ネゴシエーションのディセーブル化

機能ネゴシエーションをディセーブルにすると、機能ネゴシエーションをサポートしない古い BGP ピアとの相互運用が可能です。

機能ネゴシエーションをディセーブルにするには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dont-capability-negotiate **Example:** `switch(config-router-neighbor)# dont-capability-negotiate`	機能ネゴシエーションをディセーブルにします。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

eBGP の設定

ここでは、次の内容について説明します。

eBGP シングルホップ チェックのディセーブル化

シングルホップ eBGP ピアがローカル ルータに直接接続されているかどうかのチェック機能をディセーブルにするように、eBGP を設定できます。このオプションは、直接接続されたスイッチ間のシングルホップ ループバック eBGP セッションの設定に使用します。

シングルホップ eBGP ピアが直接接続されているかどうかのチェックをディセーブルにするには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
disable-connected-check **Example:** `switch(config-router-neighbor)# disable-connected-check`	シングルホップ eBGP ピアが直接接続されているかどうかのチェックをディセーブルにします。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

eBGP マルチホップの設定

eBGP マルチホップをサポートする eBGP TTL（存続可能時間）値を設定できます。eBGP ピアは状況によって、別の eBGP ピアに直接接続されず、リモート eBGP ピアに到達するために複数のホップを必要とします。ネイバー セッションに eBGP TTL 値を設定すると、このようなマルチホップ セッションが可能になります。

eBGP マルチホップを設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ebgp-multihop *ttl-value* **Example:** `switch(config-router-neighbor)# ebgp-multihop 5`	eBGP マルチホップの eBGP TTL を設定します。指定できる範囲は 2 ～ 255 です。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

高速外部フェールオーバーのディセーブル化

通常、BGP ルータと直接接続 eBGP ピア間の接続が失われると、ピアとの eBGP セッションをリセットすることによって、BGP が高速外部フェールオーバーを開始します。この高速外部フェールオーバーをディセーブルにすると、リンク フラップが原因の不安定さを制限できます。

高速外部フェールオーバーをディセーブルにするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no fast-external-failover **Example:** `switch(config-router)# no fast-external-failover`	eBGP ピアの高速外部フェールオーバーをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

AS パス属性の制限

AS パス属性で AS 番号が高いルートを廃棄するように eBGP を設定できます。

AS パス属性で AS 番号が高いルートを廃棄するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maxas-limit *number* **Example:** `switch(config-router)# maxas-limit 50`	AS パス セグメントの番号が指定された上限を超えている eBGP ルートを廃棄します。指定できる範囲は 1 ～ 2000 です。

ローカル AS サポートの設定

ローカル AS 機能では、ルータが実際の AS に加えて、別の自律システム（AS）のメンバであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い AS 番号を使用し続けます。

ローカル AS は正しい eBGP ピアにしか使用できません。別のコンフェデレーションのサブ自律システムのメンバである 2 ピアに対しては、この機能は使用できません。

eBGP ローカル AS のサポートを設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
local-as *number* **[no-prepend [replace-as [dual-as]]]** **Example:** `switch(config-router-neighbor)# local-as 1.1`	AS_PATH 属性にローカル AS の *number* を付加するよう eBGP を設定します。 **local-as** *number* は 16 ビット整数または 32 ビット整数です。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 **no-prepend** キーワードは、**local-as** *number* が **local-as** 番号とピアリングしているパートナーを除き、ダウンストリーム BGP ネイバーに追加されないようにします。 **replace-as** キーワードは、ピアリング セッションの **local-as** *number* だけが AS_PATH 属性に追加されるようにします。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。 **dual-as** キーワードは、実際の自律システム番号（ローカル BGP ルーティング プロセスから）を使用して、またはローカル AS として設定された自律システム番号を使用して、ピアリング セッションを確立するように eBGP ネイバーを設定します。

AS 連合の設定

AS 連合を設定するには、連合識別情報を指定する必要があります。AS 連合内の AS グループは、AS 番号として連合 ID を持つ、1 つの AS として外部で認識されます。

BGP 連合 ID を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
confederation identifier *as-number* **Example:** `switch(config-router)# confederation identifier 64512`	AS 連合を表す連合 ID を設定します。 各連合には別のサブ AS 番号があり、通常は専用番号です（64512 ～ 65534）。 このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

AS 連合に所属する AS を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
bgp confederation peers *as-number* [*as-number2...*] **Example:** switch(config-router)# bgp confederation peers 5 33 44	連合に所属する AS のリストを指定します。 このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

独自の自律システムを含む自律システム パスの設定

独自の自律システム（AS）を含む AS パスを受け入れるように BGP の allowas-in 機能をイネーブルにします。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **router bgp** *as-number*
3. switch(config-router) # **neighbor** *ip-address* **remote-as** *as-number*
4. switch(config-router-neighbor) # **address-family** {**ipv4** | **ipv6**} {**multicast** | **unicast**}
5. switch(config-router-neighbor-af) # **[no | default] allowas-in** [*allowas-in-cnt*]
6. switch(config-router-neighbor-af) # **end**
7. （任意）switch# **show running-config bgp**
8. switch# **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **router bgp** *as-number*	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。*as-number* の値の範囲は 1 ～ 65535 です。
ステップ 3	switch(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	switch(config-router-neighbor)# **address-family** {**ipv4** | **ipv6**} {**multicast** | **unicast**}	指定のアドレス ファミリに対しルータ アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	`switch(config-router-neighbor-af)# [no | default] allowas-in [allowas-in-cnt]`	BGP の allowas-in 機能をイネーブルにし、AS 番号の発生回数を設定します。 *allowas-in-cnt* には、1 ～ 10 の整数を入力します。デフォルトでは、AS 番号の発生回数は 3 に設定されます。
ステップ 6	`switch(config-router-neighbor-af)# end`	ルータ アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 7	`switch# show running-config bgp`	（任意）BGP の設定を表示します。
ステップ 8	`switch# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、BGP の allowas-in 機能を設定し、ユニキャスト IPv4 アドレス ファミリ用に設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 77
switch(config-router)# neighbor 6.20.1.1 remote-as 66
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# allowas-in 5
switch(config-router-neighbor-af)# end
```

ルート リフレクタの設定

ルート リフレクタとして動作するローカル BGP スピーカに対するルート リフレクタ クライアントとして、iBGP ピアを設定できます。ルート リフレクタとそのクライアントがともにクラスタを形成します。クライアントからなるクラスタには通常、ルート リフレクタが 1 つ存在します。このような状況では、ルート リフレクタのルータ ID でクラスタを識別します。ネットワークの冗長性を高め、シングル ポイント障害を回避するために、複数のルート リフレクタからなるクラスタを設定できます。クラスタ内のすべてのルート リフレクタは、同じ 4 バイト クラスタ ID で設定する必要があります。これは、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるようにするためです。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **cluster-id** *cluster-id*
4. **address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**}
5. （任意）**client-to-client reflection**
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*

8. **address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**}
9. **route-reflector-client**
10. **show bgp** {**ip** | **ipv6**} {**unicast** | **multicast**} **neighbors**
11.（任意）**copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**cluster-id** *cluster-id* **Example:** switch(config-router)# cluster-id 192.0.2.1	クラスタに対応するルート リフレクタの 1 つとして、ローカル ルータを設定します。クラスタを識別するクラスタ ID を指定します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 4	**address-family** {**ipv4**	**ipv6**} {**unicast**	**multicast**} **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	指定のアドレス ファミリに対しルータ アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**client-to-client reflection** **Example:** switch(config-router-af)# client-to-client reflection	（任意）クライアント間のルート リフレクションを設定します。この機能は、デフォルトでイネーブルにされています。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 6	**exit** **Example:** switch(config-router-neighbor)# exit switch(config-router)#	ルータ アドレス コンフィギュレーション モードを終了します。
ステップ 7	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.0.2.10 remote-as 65536 switch(config-router-neighbor)#	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。

	コマンドまたはアクション	目的
ステップ 8	**address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	指定のアドレス ファミリに対応しネイバー アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 9	**route-reflector-client** **Example:** switch(config-router-neighbor-af)# route-reflector-client	BGP ルート リフレクタとしてスイッチを設定し、そのクライアントとしてネイバーを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 10	**show bgp** {**ip** | **ipv6**} {**unicast** | **multicast**} **neighbors** **Example:** switch(config-router-neighbor-af)# show bgp ip unicast neighbors	（任意）BGP ピアを表示します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ルート リフレクタとしてルータを設定し、クライアントとしてネイバーを 1 つ追加する例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.10 remote-as 65536
switch(config-router-neighbor)# address-family ip unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# copy running-config startup-config
```

ルート ダンプニングの設定

iBGP ネットワーク上でのルート フラップの伝播を最小限に抑えるために、ルート ダンプニングを設定できます。

ルート ダンプニングを設定するには、アドレス ファミリまたは VRF アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dampening [{*half-life reuse-limit suppress-limit max-suppress-time* | **route-map** *map-name*}] **Example:** switch(config-router-af)# dampening route-map bgpDamp	機能ネゴシエーションをディセーブルにします。パラメータ値は次のとおりです。 • half-life：指定できる範囲は 1 ～ 45 です。 • reuse-limit：指定できる範囲は 1 ～ 20000 です。 • suppress-limit：指定できる範囲は 1 ～ 20000 です。 • max-suppress-time：指定できる範囲は 1 ～ 255 です。

ロード シェアリングおよび ECMP の設定

等コスト マルチパス ロード バランシング用に BGP がルート テーブルに追加するパスの最大数を設定できます。

パスの最大数を設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-paths [**ibgp**] *maxpaths* **Example:** `switch(config-router-af)# maximum-paths 12`	ロード シェアリング用の等コスト パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルトは 1 です。

最大プレフィックス数の設定

BGP が BGP ピアから受け取ることのできるプレフィックスの最大数を設定できます。任意で、プレフィックス数がこの値を超えた場合に、BGP に警告メッセージを生成させる、またはピアとの BGP セッションを切断させることを設定できます。

BPG ピアに認めるプレフィックスの最大数を設定するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-prefix *maximum* [*threshold*] [**restart** *time* | **warming-only**] **Example:** `switch(config-router-neighbor-af)# maximum-prefix 12`	ピアからのプレフィックスの最大数を設定します。パラメータの範囲は次のとおりです。 • *maximum*：指定できる範囲は 1 ～ 300000 です。 • *threshold* : 指定できる範囲は 1 ～ 100% です。デフォルトは 75% です。 • *time*：指定できる範囲は 1 ～ 65535 分です。 このコマンドによって、プレフィックス限度を超えた場合に、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

ダイナミック機能の設定

BGP ピアのダイナミック機能を設定できます。

ダイナミック機能を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dynamic-capability **Example:** `switch(config-router-neighbor)# dynamic-capability`	ダイナミック機能をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。 このコマンドは、デフォルトではディセーブルです。

集約アドレスの設定

BGP ルート テーブルの集約アドレス エントリを設定できます。

集約アドレスを設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
aggregate-address *ip-prefix/length* [**as-set**] [**summary-only**] [**advertise-map** *map-name*] [**attribute-map** *map-name*] [*suppress*-**map** *map-name*] **Example:** `switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set`	集約アドレスを作成します。このルートに関してアドバタイズされるパスは、集約されているすべてのパスに含まれるすべての要素からなる、AS セットです。 • **as-set** キーワードで、AS セット パス情報および関係するパスに基づくコミュニティ情報が生成されます。 • **summary-only** キーワードによって、アップデートから固有性の強いルートがすべてフィルタリングされます。 • **advertise-map** キーワードおよび引数では、選択されたルートから属性情報を選択するためのルート マップを指定します。 • **attribute-map** キーワードおよび引数では、集約から属性情報を選択するためのルート マップを指定します。 • **suppress-map** キーワードおよび引数によって、固有性の強いルートを条件付きでフィルタリングします。

BGP 条件付きアドバタイズメントの設定

BGP がプロパゲートするルートを制限するように BGP 条件付きアドバタイズメントを設定できます。次の 2 つのルート マップを定義します。

- アドバタイズ マップ：BGP が条件付きアドバタイズメントを考慮する前にルートが一致する必要のある条件を指定します。このルート マップには、適切な match ステートメントを含めることができます。

- 存在マップまたは非存在マップ：BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在する必要のあるプレフィックスを定義します。非存在マップは、BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在してはならないプレフィックスを定義します。BGP は、これらのルート マップでプレフィックス リストの match ステートメント内にある permit ステートメントのみを処理します。

ルートが条件を渡さない場合、そのルートが BGP テーブルにあれば BGP によってルートが取り消されます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** *ipaddress* **remote-as** *as-number*
4. **address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**}
5. **advertise-map** *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*}
6. （任意）**show ip bgp neighbor**
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	**address-family** {**ipv4**	**ipv6**} {**unicast**	**multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**advertise-map** *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*} **Example:** `switch(config-router-neighbor-af)# advertise-map advertise exist-map exist`	2 つの設定済みルート マップに従い、ルートを条件付きでアドバタイズするように BGP を設定します。 • *adv-map*：BGP がルートを次のルート マップに渡す前に、そのルートが渡す必要のある ***match*** ステートメントを使用してルート マップを指定します。*adv-map* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • *exist-rmap :* プレフィックス リストの match ステートメントを使用してルート マップを指定します。BGP テーブル内のプレフィックスは、BGP がルートをアドバタイズする前に、プレフィックス リスト内のプレフィックスと一致する必要があります。*exist-rmap* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • *nonexist-rmap :* プレフィックス リストの match ステートメントを使用してルート マップを指定します。BGP テーブル内のプレフィックスは、BGP がルートをアドバタイズする前に、プレフィックス リスト内のプレフィックスと一致してはいけません。*nonexist-rmap* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。
ステップ 6	**show ip bgp neighbor** **Example:** `switch(config-router-neighbor-af)# show ip bgp neighbor`	（任意）BGP に関する情報、および設定した条件付きアドバタイズメントのルート マップに関する情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、BGP 条件付きアドバタイズメントを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
```

ルートの再配布の設定

別のルーティング プロトコルからのルーティング情報を受け入れて、BGP ネットワークを通じてその情報を再配布するように、BGP を設定できます。任意で、再配布ルートのためのデフォルト ルートを割り当てることができます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**}
4. **redistribute** {**direct** | {**eigrp** | **isis** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name*
5. （任意）**default-metric** *value*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**} **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 4	**redistribute** {**direct** | {**eigrp** | **isis** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name* **Example:** switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap	他のプロトコルからのルートを BGP に再配布します。ルート マップの詳細については、「ルート マップの設定」（P.16-12）を参照してください。

	コマンド	目的
ステップ 5	**default-metric** *value* **Example:** switch(config-router-af)# default-metric 33	（任意）BGP へのデフォルト ルートを作成します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、EIGRP を BGP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap
switch(config-router-af)# copy running-config startup-config
```

マルチプロトコル BGP の設定

複数のアドレス ファミリ（IPv4 および IPv6 のユニキャストおよびマルチキャスト ルートを含む）をサポートするように MP-BGP を設定できます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** *ip-address* **remote-as** *as-numbe*r
4. **address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**}
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。

	コマンド	目的
ステップ 3	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	**address-family** {**ipv4** | **ipv6**} {**unicast** | **multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ネイバーのマルチキャスト RPF に対して IPv4 および IPv6 ルートのアドバタイズおよび受信をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8::1
switch(config-if)# router bgp 65536
switch(config-router)# neighbor 192.168.1.2 remote-as 35537
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# address-family ipv6 multicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP の調整

一連のオプション パラメータを使用することによって、BGP 特性を調整できます。

BGP を調整するには、ルータ コンフィギュレーション モードで次の ofptional コマンドを使用します。

コマンド	目的

bestpath [**always-compare-med** | **compare-routerid** | **med** {**missing-as-worst** | **non-deterministic**}| **as-path multipath-relax**]
 	
Example:
`switch(config-router)# bestpath always-compare-med`
`switch(config-router)# bestpath as-path multipath-relax`
	ベストパス アルゴリズムを変更します。オプション パラメータは次のとおりです。
	• **always-compare-med**：異なる AS からのパスの MED を比較します。
	• **compare-routerid**：同一の eBGP パスのルータ ID を比較します。
	• **med missing-as-worst**：脱落 MED を最上位 MED として扱います。
	• **med non-deterministic**：同じ AS からのパス間で、必ずしも最適な MED パスを選択しません。
	• **as-path multipath-relax**：Cisco NX-OS Release 5.0(3)U1(2) から、AS パスの長さが同じで、他のマルチパス条件を満たしている場合は、マルチパスのさまざまな AS から受信したパスをスイッチで処理できるようになりました。

enforce-first-as **Example:** `switch(config-router)# enforce-first-as`	ネイバー AS を eBGP の AS_path 属性で指定する最初の AS 番号にします。
log-neighbor-changes **Example:** `switch(config-router)# log-neighbor-changes`	ネイバーでステートが変化したときに、システム メッセージを生成します。
router-id *id* **Example:** `switch(config-router)# router-id 209.165.20.1`	この BGP スピーカのルータ ID を手動で設定します。
timers [**bestpath-delay** *delay* | **bgp** *keepalive holdtime* | **prefix-peer-timeout** *timeout*] **Example:** `switch(config-router)# timers bgp 90 270`	BGP タイマー値を設定します。オプション パラメータは次のとおりです。 • *delay*：再起動後の初期最適パス タイムアウト値。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 300 です。 • keepalive：BGP セッション キープアライブ タイム。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 60 です。 • holdtime：BGP セッション ホールド タイム。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 180 です。 • timeout：プレフィックス ピア タイムアウト値。指定できる範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。 このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

BGP を調整するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
distance *ebgp-distance ibgp distance local-distance* **Example:** `switch(config-router-af)# distance 20 100 200`	BGP のアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトの設定は次のとおりです。 • eBGP ディスタンス：20 • iBGP ディスタンス：200 • ローカル ディスタンス：220。ローカル ディスタンスは、集約廃棄ルートが RIB に組み込まれている場合に、集約廃棄ルートに使用するアドミニストレーティブ ディスタンスです。

BGP を調整するには、ネイバー コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
description *string* **Example:** `switch(config-router-neighbor)# description main site`	この BGP ピアを説明するストリングを設定します。ストリングには最大 80 の英数字を使用できます。
low-memory exempt **Example:** `switch(config-router-neighbor)# low-memory exempt`	メモリ不足状態によるシャットダウンからこの BGP ネイバーを除外します。
transport connection-mode passive **Example:** `switch(config-router-neighbor)# transport connection-mode passive`	受動接続の確立だけが可能です。この BGP スピーカは BGP ピアへの TCP 接続を開始しません。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。
remove-private-as **Example:** `switch(config-router-neighbor)# remove-private-as`	eBGP ピアへの発信ルート アップデートからプライベート AS 番号を削除します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
update-source *interface-type number* **Example:** `switch(config-router-neighbor)# update-source ethernet 2/1`	ピアとの BGP セッション用に設定されたインターフェイスの送信元 IP アドレスを使用するように、BGP スピーカを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

BGP を調整するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
suppress-inactive **Example:** switch(config-router-neighbor-af)# suppress-inactive	ベスト（アクティブ）ルートだけを BGP ピアにアドバタイズします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
default-originate [**route-map** *map-name*] **Example:** switch(config-router-neighbor-af)# default-originate	BGP ピアへのデフォルト ルートを作成します。
filter-list *list-name* {**in** | **out**} **Example:** switch(config-router-neighbor-af)# filter-list BGPFilter in	着信または発信ルート アップデートに関して、この BGP ピアに AS_path フィルタ リストを適用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
prefix-list *list-name* {**in** | **out**} **Example:** switch(config-router-neighbor-af)# prefix-list PrefixFilter in	着信または発信ルート アップデートに関して、この BGP ピアにプレフィックス リストを適用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
send-community **Example:** switch(config-router-neighbor-af)# send-community	この BGP ピアにコミュニティ属性を送信します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
send-extcommunity **Example:** switch(config-router-neighbor-af)# send-extcommunity	この BGP ピアに拡張コミュニティ属性を送信します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

仮想化の設定

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.7-11）を参照）。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **exit**
4. **router bgp** *as-number*
5. **vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **bestpath as-path multipath-relax**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF コンフィギュレーション モードを開始します。
ステップ 3	**exit** **Example:** switch(config-vrf)# exit switch(config)#	VRF コンフィギュレーション モードを終了します。
ステップ 4	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	AS 番号を設定して、新しい BGP プロセスを作成します。
ステップ 5	**vrf** *vrf-name* **Example:** switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	ルータ VRF コンフィギュレーション モードを開始し、この BGP インスタンスと VRF を関連付けます。
ステップ 6	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536 switch(config-router--vrf-neighbor)#	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。
ステップ 7	**bestpath as-path multipath-relax** **Example:** switch(config-router-vrf)# bestpath as-path multipath-relax	（任意）Cisco NX-OS Release 5.0(3)U1(2) から、AS パスの長さが同じで、他のマルチパス条件を満たしている場合は、マルチパスのさまざまな AS から受信したパスをスイッチで処理できるようになりました。
ステップ 8	**copy running-config startup-config** **Example:** switch(config-router-vrf-neighbor)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成し、VRF でルータ ID を設定する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router bgp 65536
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536
switch(config-router-vrf-neighbor)# copy running-config startup-config
```

拡張 BGP の設定の確認

BGP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show bgp all [**summary**] [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp convergence [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **community** {**regexp** *expression* | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]} [**vrf** *vrf-name*]	BGP コミュニティと一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **community-list** *list-nam*e [**vrf** *vrf-name*]	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **extcommunity** {**regexp** *expression* | **generic** [**non-transitive** | **transitive**] *aa4:nn* [**exact-match**]} [**vrf** *vrf-name*]	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **extcommunity-list** *list-nam*e [**exact-match**] [**vrf** *vrf-name*]	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] {**dampening dampened-paths** [**regexp** *expression*]} [**vrf** *vrf-name*]	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、**clear bgp dampening** コマンドを使用します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **history-paths** [**regexp** *expression*] [**vrf** *vrf-name*]	BGP ルート ヒストリ パスを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **filter-list** *list-name* [**vrf** *vrf-name*]	BGP フィルタ リストの情報を表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **neighbors** [*ip-address* | *ipv6-prefix*] [**vrf** *vrf-name*]	BGP ピアの情報を表示します。これらのネイバーを消去するには、**clear bgp neighbors** コマンドを使用します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] {**nexthop** | **nexthop-database**} [**vrf** *vrf-name*]	BGP ルート ネクスト ホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **policy** *name* [**vrf** *vrf-name*]	BGP ポリシー情報を表示します。ポリシー情報を消去するには、**clear bgp policy** コマンドを使用します。

コマンド	目的
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **prefix-list** *list-name* [**vrf** *vrf-name*]	プレフィックス リストと一致する BGP ルートを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **received-paths** [**vrf** *vrf-name*]	ソフト再構成用に保管されている BGP パスを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **regexp** *expression* [**vrf** *vrf-name*]	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **route-map** *map-name* [**vrf** *vrf-name*]	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy *name* [**vrf** *vrf-name*]	BGP ピア ポリシー情報を表示します。
show bgp peer-session *name* [**vrf** *vrf-name*]	BGP ピア セッション情報を表示します。
show bgp peer-template *name* [**vrf** *vrf-name*]	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、**clear bgp peer-template** コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。
show {**ip** | **ipv6**} **bgp** *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 3000 Series Command Reference,*』を参照してください。
show {**ip** | **ipv6**} **mbgp** *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 3000 Series Command Reference,*』を参照してください。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報の表示

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **flap-statistics** [**vrf** *vrf-name*]	BGP ルート フラップの統計情報を表示します。これらの統計情報を消去するには、**clear bgp flap-statistics** コマンドを使用します。
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。

コマンド	目的
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

関連資料

BGP の詳細については、次の項目を参照してください。

- 第 8 章「拡張 BGP の設定」
- 第 16 章「Route Policy Manager の設定」

その他の関連資料

BGP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.8-43）
- 「管理情報ベース（MIB）」（P.8-43）

関連資料

関連項目	マニュアル名
BGP CLI コマンド	*『Cisco Nexus 3000 Series Command Reference,』*

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	管理情報ベース（MIB）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

BGP 機能の履歴

表 8-2 は、この機能のリリースの履歴です。

表 8-2　BGP 機能の履歴

機能名	リリース	機能情報
BGP	5.0(3)U1(1)	この機能が導入されました。
BFD	5.0(3)U2(2)	BFD のサポートが追加されました。詳細については、第 9 章「BGP の双方向フォワーディング検出の設定」を参照してください。

表 8-2　BGP 機能の履歴 （続き）

機能名	リリース	機能情報
BGP	5.0(3)U2(2a)	ローカル AS のサポートが追加されました。詳細については、「ローカル AS サポートの設定」（P.8-24）を参照してください。
IPv6	5.0(3)U3(1)	IPv6 のサポートが追加されました。
ルート リフレクタ	5.0(3)U3(1)	**route-reflector-client** コマンドが追加されました。
ネクスト ホップ アドレス	5.0(3)U3(1)	**next-hop-self** コマンドが追加されました。