CHAPTER 10

拡張 BGP の設定

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

ここでは、次の内容を説明します。

拡張 BGP の概要

BGP は、組織または AS（自律システム）間のループフリー ルーティングを提供する、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 対応デバイス（BGP ピア）との間で TCP セッションを確立するための、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、ピアに継承させる一連のアトリビュートを定義します。継承したアトリビュート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 アトリビュートを定義します。peer-session テンプレートは、別の peer-session テンプレートからアトリビュートを継承することもできます(ローカル定義のアトリビュートによって、継承した peer-session アトリビュートは上書きされます)。
- *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クス、AS_path アトリビュートなど、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 アトリビュート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 15 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、およびその他の機能にルート マップを使用します。ルート マップの詳細については、第 14 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。

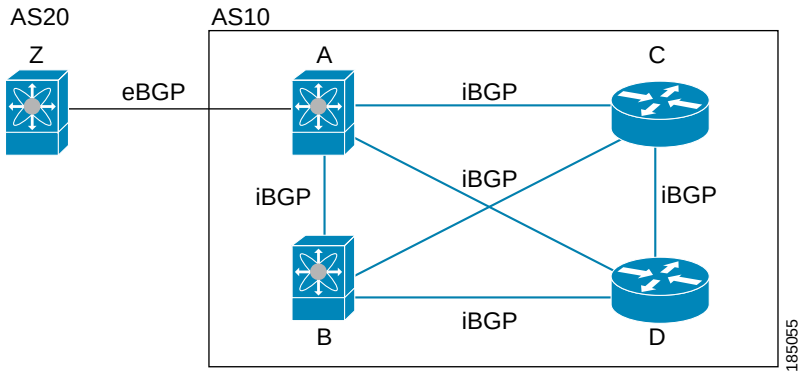
eBGP ピアリング セッションの確立には、ループバック インターフェイスを使用します。ループバック インターフェイスは、インターフェイス フラップが発生する可能性が小さいからです。インターフェイス フラップが発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フェールオーバー、および一般的な TTL（存続可能時間）セキュリティ メカニズム サポートについては、「eBGP の設定」（p.10-22）を参照してください。

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 10-1 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 10-1　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。

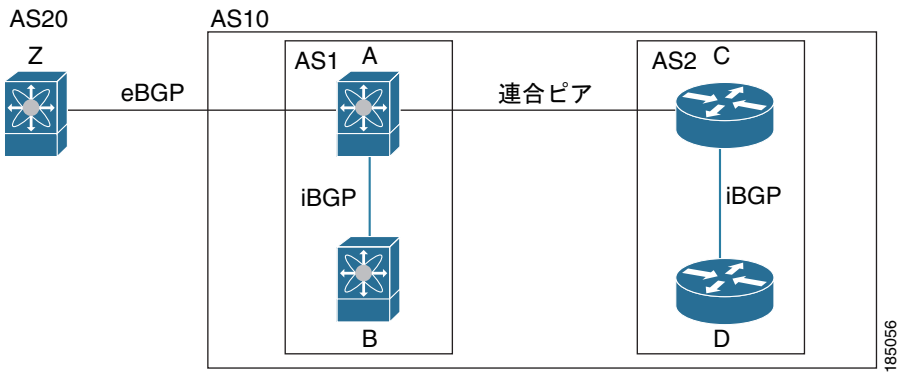
- AS 連合（p.10-5）
- ルータ リフレクタ（p.10-5）

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 10-2 に、図 10-1 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 10-2　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 10-1 のフルメッシュ AS に比べて、リンク数を少なくできます。

ルータ リフレクタ

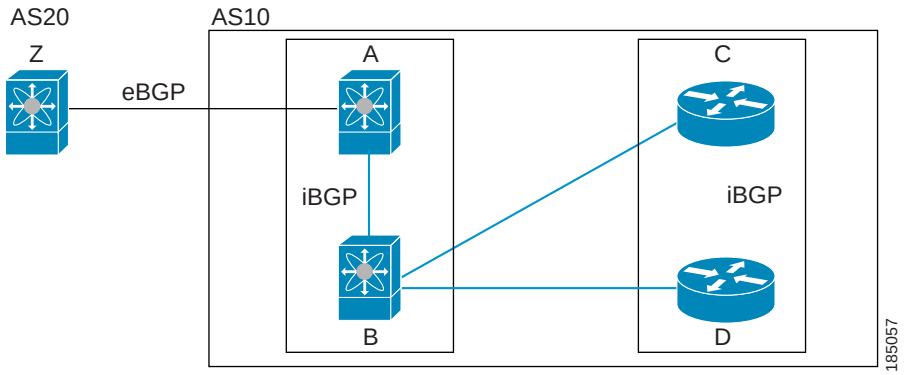
ルータ リフレクタ構成を使用することによって、iBGP メッシュを緩和することもできます。ルータ リフレクタは学習したルートをネイバーに渡し、すべての iBGP ピアをフルメッシュにしなくてもすむようにします。

図 10-1 に、メッシュの iBGP スピーカを 4 つ使用する（ルータ A、B、C、および D）、単純な iBGP 構成を示します。ルータ 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 10-3 では、ルータ B がルータ 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はなくなります。

図 10-3　ルータ リフレクタ



ルータ リフレクタおよびクライアント ピアは、クラスタを形成します。ルータ 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ことを保証するために、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。

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。それぞれ AS1、AS2、および AS3 です。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、再利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。再利用限度が 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、次のアトリビュートが同じ場合に、等コスト パスとみなされます。

- 重み値
- 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、ベスト 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 値およびその他のアトリビュートが同じ場合に、等コスト パスとみなされます。

（注）　iBGP マルチパスに関してルータ リフレクタを設定すると、ルータ リフレクタがピアに選択されたベスト パスを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 はサマリー廃棄の管理ディスタンスを 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。

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 ポリシーでは、宛先、送信元プロトコル、ルート タイプ、ルート タグなどのアトリビュートに基づいて、ルートをフィルタリングできます。詳細については、第 14 章「Route Policy Manager 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、アルゴリズムでの MED アトリビュートおよびルータ ID の扱い方を変更することを含め、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。

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（MBGP）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 ルート用のルート セットを 1 つ伝送できます。

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 コンフィギュレーション モードを使用します。

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。

MGMP を使用するマルチキャストの設定例については、『*Cisco Cisco NX-OS Multicast Configuration Guide*』を参照してください。

グレースフル リスタートおよびハイ アベイラビリティ

Cisco NX-OS は、BGP の無停止フォワーディングおよびグレースフル リスタートをサポートします。

BGP の無停止フォワーディングを使用すると、FIB（転送情報ベース）の既知のルートでデータ パケットを転送し、なおかつフェールオーバー後に BGP ルーティング プロトコル情報を復元できます。NSF では、BGP ピアはルーティング フラップと無縁です。フェールオーバー時に、データ トラフィックはインテリジェント モジュール経由で転送され、スタンバイ スーパーバイザがアクティブになります。

Cisco NX-OS ルータでコールド リブートが発生した場合、ネットワークはルータにトラフィックを転送しないで、ネットワーク トポロジからルータを削除します。この状況では、BGP は非グレースフル リスタートになり、すべてのルートが削除されます。Cisco NX-OS はスタートアップ コンフィギュレーションを適用し、BGP はピアリング セッションを再び確立して、ルートを再学習します。

デュアル スーパーバイザ構成の Cisco NX-OS ルータでは、ステートフル スーパーバイザ スイッチオーバーが実行されます。スイッチオーバーの実行前に、グレースフル リスタートが始まり、BGP がしばらく使用できなくなることが BGP によって告知されます。スイッチオーバーの間、BGP は無停止フォワーディングを使用し、FIB の情報に基づいてトラフィックを転送します。システムがネットワーク トポロジから取り除かれることはありません。リスタートされたルータは、ピアからのルートを「stale」（古い）として明示します。

グレースフル リスタート動作中であることがルータで検出されると、両方のルータがそれぞれのトポロジ テーブルを交換します。すべての BGP ピアからルート アップデートを受信したルータは、古いルートをすべて削除し、アップデートされたルートでベストパス アルゴリズムを実行します。

スイッチオーバー後、Cisco NX-OS によって実行コンフィギュレーションが適用され、BGP は再び動作可能になったことをネイバーに通知します。

ISSU

BGP の ISSU（インサービス ソフトウェア アップグレード）をサポートするには、グレースフル リスタートをイネーブルにする必要があります。

BGP ではピア ホールド タイマーを使用して、非アクティブになったピアのセッションを切断し、応答を中止します。ISSU プロセスの一部として、スイッチオーバー中に BGP コントロール パケットが受信または送信されないことがあり、ピアがキープアライブ メッセージ損失を認識する可能性があります。ただし、ホールド タイムをスイッチオーバー タイムより長くしておくと、ピアがローカル ルータとのセッションを切断することはありません。

スイッチオーバーが発生すると、ピアはローカル ルータ上の新しいアクティブ TCP から TCP 接続リセットを受信します。グレースフル リスタートがイネーブルになっている場合、ピアはルータが再起動したという表示としてリセットを扱い、グレースフル リスタート ヘルパー手順を開始します。

システム スイッチオーバー タイム（約 15 秒）に満たないホールド タイムが設定されている場合、Cisco NX-OS は ISSU を保証できません。

BGP による ISSU サポートは、次のとおりです。

- グレースフル リスタートをディセーブルにすると、この設定では ISSU をサポートできないことを伝える警告が Cisco NX-OS から出されます。
- システム スイッチオーバー タイムに満たないホールド タイムを設定すると、Cisco NX-OS から同様の警告が出されます。ピアが短縮ホールド タイムのネゴシエーションを行うと、Cisco NX-OS がメッセージを記録します。
- スイッチオーバーの前に、Cisco NX-OS が BGP ISSU 関連のコールバック ルーチンを実行した場合は、BGP がすべてのアクティブ ピアについて、グレースフル リスタート ステータスおよびホールド タイムの両方を確認します。グレースフル リスタートがディセーブルになっている場合、またはアクティブ ピアのホールド タイムがシステム スイッチオーバー タイムより短い場合は、Cisco NX-OS が該当する警告を発行し、スイッチオーバーの強制についてはユーザの裁量にまかせます。
- ISSU　がサポートされない場合、スイッチオーバーを強制実行できますが、この強制スイッチオーバー中の転送は維持されません。

仮想化サポート

Cisco NX-OS は、同一システム上で動作する複数の BGP プロトコル インスタンスをサポートします。BGP は、virtual device context（仮想デバイス コンテキスト ; VDC）内に存在する VRF（仮想ルーティングおよびフォワーディング）をサポートします。VDC で設定できる BGP インスタンスは 1 つですが、システム上では複数の VDC を使用できます。

特に VDC および VRF を設定しないかぎり、デフォルトで、Cisco NX-OS はユーザにデフォルト VDC およびデフォルト VRF を使用させます。『*Cisco NX-OS Virtual Device Context Configuration Guide*』および第 13 章「レイヤ 3 仮想化の設定」を参照してください。

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
NX-OS	BGP には Enterprise Services ライセンスが必要です。NX-OS ライセンス方式の詳細、ライセンスを取得して適用する方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

BGP の前提条件

BGP の前提条件は、次のとおりです。

- 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.9-10] 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（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 に関する注意事項および制約事項は、次のとおりです。

- 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。
- VDC を設定する場合は、Advanced Services ライセンスをインストールし、所定の VDC を開始してください（『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照）。

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、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

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、そのあとで 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 アトリビュートを設定できます。

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第 2 テンプレートを設定し、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アトリビュートは、ネイバーが BGP テンプレートから継承したアトリビュートより優先されます。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

（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時を明示的に上書きできます。アトリビュート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。

手順概要

1. **config t**
2. **router bgp** *autonomous-system-number*
3. **template peer-session** *template-name*
4. セッション テンプレートに適切なアトリビュートを追加します。
5. **exit**
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **inherit peer-session** *template-name*
8. 適切なネイバー アトリビュートを追加します。
9. **show bgp peer-session** *template-name*
10. **copy running-config startup-config**

手順詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*
	
	例：
	`switch(config)# router bgp 45000`
	`switch(config-router)#`
		BGP をイネーブルにして、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-session** *template-name*
	
	例：
	`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* **例：** `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。

	コマンド	目的
ステップ 5	**timers** *keepalive hold* **例：** `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**
	
	例：
	`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*
	
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 40000`
	`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	***inherit peer-session*** *template-name*
	
	例：
	`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*
	
	例：
	`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* **例：** `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*** **例：** `switch(config-router-neighbor)# copy running-config startup-config`	(任意) この設定変更を保存します。

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 NX-OS Unicast Routing Command Reference*』Release 4.0 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# config t
switch(config)# router bgp 45000
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 40000
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アトリビュートを定義できます。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アトリビュートは、ネイバーが BGP テンプレートから継承したアトリビュートより優先されます。

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 ファミリ固有のアトリビュートを設定できます。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

（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時を明示的に上書きできます。アトリビュート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。

手順概要

1. **config t**
2. **router bgp** *autonomous-system-number*
3. **template peer-policy** *template-name*
4. ポリシー テンプレートに適切なアトリビュートを追加します。
5. **exit**
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **address-family** {***ipv4*** | ***ipv6}*** ***{multicast*** | **unicast**}
8. **inherit peer-policy** *template-name preference*
9. **show bgp peer-policy** *template-name*
10. **copy running-config startup-config**

手順詳細

	コマンド	目的

ステップ 1	`config t`
	
	例：
	`switch# config t`
	`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*
	
	例：
	`switch(config)# router bgp 45000`
	`switch(config-router)#`
		BGP をイネーブルにして、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	**template peer-policy** *template-name*
	
	例：
	`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** **例：** `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。
ステップ 5	**maximum-prefix** *number* **例：** `switch(config-router-ptmp)# maximum-prefix 20`	（任意）このピアに認めるプレフィクスの最大数を設定します。

ステップ 6	**exit**
	
	例：
	`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*
	
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 40000`
	`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***}
	
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		IPv4 アドレス ファミリに対応するグローバル 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* **例：** `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* **例：** `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*** **例：** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定変更を保存します。

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 NX-OS Unicast Routing Command Reference*』Release 4.0 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# config t
switch(config)# router bgp 40000
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 45000
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 ピア 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 アトリビュートとポリシー アトリビュート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アトリビュートは、ネイバーが BGP テンプレートから継承したアトリビュートより優先されます。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、最大プレフィクス数、ネクストホップ セルフ、タイマーなど、セッション アトリビュートおよびアドレス ファミリ アトリビュートをサポートします。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

（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時を明示的に上書きできます。アトリビュート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。

手順概要

1. **config t**
2. **router bgp** *autonomous-system-number*
3. **template peer** *template-name*
4. ピア テンプレートに適切なアトリビュートを追加します。
5. **exit**
6. **neighbor** *ip-address*
7. **inherit peer** *template-name*
8. 適切なネイバー アトリビュートを追加します。
9. **show bgp peer-template** *template-name*
10. **copy running-config startup-config**

手順詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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* **例：** `switch(config)# router bgp 45000`	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*
	
	例：
	`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* **例：** `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***}
	
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		（任意）IPv4 アドレス ファミリに対応するグローバル 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-policy*** *template-name preference* **例：** `switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1`	（任意）ネイバー 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 7	**exit**
	
	例：
	`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* **例：** `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**
	
	例：
	`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*
	
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 40000`
	`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 11	***inherit peer*** *template-name* **例：** `switch(config-router-neighbor)# inherit peer BasePeer`	peer テンプレートを継承します。

	コマンド	目的
ステップ 12	**timers** *keepalive hold* **例：** `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* **例：** `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*** **例：** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定変更を保存します。

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 NX-OS Unicast Routing Command Reference*』Release 4.0 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# config t
switch(config)# router bgp 45000
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 40000
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

プレフィクス ピアリングの設定

BGP では IPv4 および IPv6 の両方のプレフィクスを使用して、ピア セットを定義できます。これにより、コンフィギュレーションに各ネイバーを追加する必要がなくなるので、テンプレートを使用する以上に設定を簡素化できます。

プレフィクス ピアリングを定義する場合は、プレフィ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かぎり、BGP はプレフィクスおよび 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るので、ネットワークの安定性が向上します。prefix-peer-time-out のデフォルト設定は 30 秒です。

BGP プレフィクス 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* **例：** `switch(config-router-neighbor)# timers prefix-peer-timeout 120`	プレフィクス ピアリングのタイムアウト値を設定します。有効値の範囲は 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* **例：** `switch(config-router-neighbor)# timers prefix-peer-timeout 120`	このプレフィクス ピアリングの最大ピア数を設定します。有効値の範囲は 1 ～ 1000 です。

最大 10 のピアを受け付けるプレフィクス ピアリングの設定例を示します。

```
switch(config)# router bgp 1
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 1
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* **例：** `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 **例：** `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***} **例：** `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。この方法は、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。この場合、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、ネイバー アドレス ファミリ コンフィギュレーション モードで次のパラメータを設定します。

コマンド	目的
next-hop-self **例：** `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 **例：** `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** が設定されていないシングルホップの EBGP ピアに使用します。

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 **例：** `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 **例：** `switch(config-router-neighbor)# soft-reconfiguration inbound`	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 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* **例：** `switch(config-router-neighbor)# ebgp-multihop 5`	eBGP マルチホップの eBGP TTL を設定します。有効値の範囲は 2 ～ 255 です。このコマンドを設定したあとで、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 **例：** `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。イネーブルがデフォルトです。

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* **例：** `switch(config-router)# confederation identifier 4000`	AS 連合を表す連合 ID 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。

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...*] **例：** `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。

ルータ リフレクタの設定

ルータ 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タ リフレクタ クライアントとして、iBGP ピアを設定できます。ルータ 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、ルータ リフレクタが 1 つ存在します。このような状況では、ルータ 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、複数のルータ 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タ 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、ルータ リフレクタが同じクラスタ内のルータ 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。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順概要

1. **config t**
2. **router bgp** *as-number*
3. **cluster-id** *cluster-id*
4. **address-family** {***ipv4*** | ***ipv6***} {***unicast*** | ***multicast***}
5. ***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**} *as-number*
11. **copy running-config startup-config**

手順詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*
	
	例：
	`switch(config)# router bgp 45000`
	`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* **例：** `switch(config-router)# cluster-id 192.0.2.1`	クラスタに対応するルータ 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***}
	
	例：
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		指定のアドレス ファミリに対応するグローバル 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 5	**client-to-client reflection** **例：** `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です。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。

	コマンドまたはアクション	目的

ステップ 6	**exit**
	
	例：
	`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*
	
	例：
	`switch(config-router)# neighbor 192.0.2.10 remote-as 40000`
	`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。

ステップ 8	**address-family** {***ipv4*** | ***ipv6***}{***unicast*** | ***multicast***}
	
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		ユニキャスト IPv4 アドレス ファミリに対応するネイバー 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** **例：** `switch(config-router-neighbor-af)# route-reflector-client`	BGP ルータ 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*** **例：** `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*** **例：** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定変更を保存します。

ルータ 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 45000
switch(config-router)# neighbor 192.0.2.10 remote-as 40000
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*}] **例：** `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 — 範囲は 1 ～ 45 • reuse-limit — 範囲は 1 ～ 20000 • suppress-limit — 範囲は 1 ～ 20000 • max-suppress-time — 範囲は 1 ～ 255

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* **例：** `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。有効値の範囲は 1 ～ 16 です。

最大プレフィクス数の設定

BGP が BGP ピアから受け取ることのできるプレフィクスの最大数を設定できます。任意で、プレフィ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**] **例：** `switch(config-router-neighbor-af)# maximum-paths 12`	ピアからのプレフィ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* — 範囲は 1 ～ 300000 • *threshold* — 範囲は 1 ～ 100%。デフォルト値は 75% です。 • *time* — 範囲は 1 ～ 65635 分 このコマンドによって、プレフィ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 **例：** `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。 デフォルトでディセーブルです。

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*] **例：** `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アトリビュート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、集約からアトリビュート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。

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。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順概要

1. **config t**
2. **router bgp** *as-number*
3. ***address-family*** {***ipv4*** | ***ipv6***} {***unicast*** | ***multicast***}
4. ***redistribute*** {***direct*** | ***eigrp*** *as* | ***isis*** *id* | ***ospf*** *id* | ***ospfv3*** *id* | ***rip*** *id* | ***static route-map*** *map-name*
5. ***default-metric*** *value*
6. ***exit***
7. ***copy running-config startup-config***

手順詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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* **例：** switch(config)# router bgp 45000 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***} **例：** 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*** *as* | ***isis*** *id* | ***ospf*** *id* | ***ospfv3*** *id* | ***rip*** *id* | ***static*** | ***direct***} ***route-map*** *map-name* **例：** 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.14-9）を参照してください。
ステップ 5	***default-metric*** *value* **例：** 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*** **例：** switch(config-router-af)# copy running-config startup-config	（任意）この設定変更を保存します。

EIGRP を BGP に再配布する例を示します。

```
switch# config t
switch(config)# router bgpEnterprise
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
```

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 モードで次のオプション 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***}] **例：** `switch(config-router)# bestpath always-compare-med`	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。
enforce-first-as **例：** `switch(config-router)# enforce-first-as`	ネイバー AS を eBGP の AS_path アトリビュートで指定する最初の AS 番号にします。
log-neighbor-changes **例：** `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* **例：** `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*] **例：** `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* — 再起動後の初期ベスト パス タイムアウト値。有効値の範囲は 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。有効値の範囲は 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。有効値の範囲は 0 ～ 3600 秒です。デフォルト値は 180 です。 • timeout — プレフィクス ピア タイムアウト値。有効値の範囲は 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* **例：** `switch(config-router-af)# distance 20 100 200`	BGP の管理ディスタンスを設定します。有効値の範囲は 1 ～ 255 であり、デフォルトは次のとおりです。 • 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管理ディスタンスです。

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* **例：** `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。
transport connection-mode passive **例：** `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 **例：** `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* **例：** `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 **例：** `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*] **例：** `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***} **例：** `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***} **例：** `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 **例：** `switch(config-router-neighbor-af)# send-community`	この BGP ピアにコミュニティ アトリビュートを送信します。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。

グレースフル リスタートの設定

BGP のグレースフル リスタートを設定し、グレースフル リスタート ヘルパー機能をイネーブルにできます。

準備作業

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.9-10] を参照）。

VDC および VRF を作成します。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順概要

1. **config t**
2. ***router bgp*** *as-number*
3. ***graceful-restart***
4. ***graceful-restart*** [***restart-time*** *time* | ***stalepath-time*** *time*]
5. ***graceful-restart-helper***
6. ***show running-config bgp***
7. ***copy running-config startup-config***

手順詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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* **例：** switch(config)# router bgp 201 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 3	***graceful-restart*** **例：** switch(config-router)# graceful-restart	グレースフル リスタートおよびグレースフル リスタート ヘルパー機能をイネーブルにします。イネーブルがデフォルトです。 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 4	***graceful-restart*** [***restart-time*** *time* | ***stalepath-time*** *time*] **例：** switch(config-router)# graceful-restart restart-time 300	グレースフル リスタート タイマーを設定します。 オプション パラメータは次のとおりです。 • restart-time — BGP ピアに送信されたリスタートの最大時間。有効値の範囲は 1 ～ 3600 秒です。デフォルトは 120 です。 • stalepath-time — BGP が再起動中の BGP ピアからの古いルートを維持する最大時間。有効値の範囲は 1 ～ 3600 秒です。デフォルトは 300 です。 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 5	***graceful-restart-helper*** **例：** switch(config-router)# graceful-restart-helper	グレースフル リスタート ヘルパー機能をイネーブルにします。このコマンドは、グレースフル リスタートをディセーブルにしていながら、グレースフル リスタート ヘルパー機能はイネーブルにする必要がある場合に使用します。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 6	***show running-config bgp*** **例：** switch(config-router)# show running-config bgp	（任意）BGP の設定を表示します。
ステップ 7	***copy running-config startup-config*** **例：** switch(config-router)# copy running-config startup-config	（任意）この設定変更を保存します。

グレースフル リスタートをイネーブルにする例を示します。

```
switch# config t
switch(config)# router bgp 201
switch(config-router)# graceful-restart
switch(config-router)# copy running-config startup-config
```

仮想化の設定

各 VDC で 1 つずつ BGP プロセスを設定できます。各 VDC 内で複数の VRF を作成できます。また、各 VRF で同じ BGP プロセスを使用できます。

準備作業

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.9-10] を参照）。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順概要

1. **config t**
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. ***copy running-config startup-config***

手順詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*
	
	例：
	`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***
	
	例：
	`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*
	
	例：
	`switch(config)# router bgp 201`
	`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。

	コマンド	目的

ステップ 5	**vrf** *vrf-name*
	
	例：
	`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*
	
	例：
	`switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 45000`
	`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	***copy running-config startup-config*** **例：** `switch(config-router-vrf-neighbor)# copy running-config startup-config`	（任意）この設定変更を保存します。

VRF を作成し、VRF でルータ ID を設定する例を示します。

```
switch# config t
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router bgp 201
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 45000
switch(config-router-vrf-neighbor)# copy running-config startup-config
```

拡張 BGP の設定確認

BGP の設定を確認するには、次のコマンドを使用します。

コマンド	目的
show bgp [**vrf** *vrf-name*] **all** [**summary**]	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 [**vrf** *vrf-name*] **convergence**	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **community** {**regexp** | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]}	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-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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] {**damp-params** | **dampened-paths**}	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **history-paths**	BGP ルート ヒストリ パスを表示します。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **filter-list** *list-name*	BGP フィルタ リストの情報を表示します。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **neighbors** [*ip-address* | *ipv6-prefix*]	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] {**nexthop** | **nexthop-database**}	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **policy** *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。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **prefix-list** *list-name*	プレフィクス リストと一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **received-paths**	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **regexp** *expression*	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **route-map** *map-name*	ルート マップと一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] **peer-policy** *name*	BGP ピア ポリシー情報を表示します。
show bgp [**vrf** *vrf-name*] **peer-session** *name*	BGP ピア セッション情報を表示します。
show bgp [**vrf** *vrf-name*] **peer-template** *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 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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **flap-statistics**	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 [**vrf** *vrf-name*] {**ip** | **ipv6**} {**unicast** | **multicast**} [*ip-address* | *ipv6-prefix*] **neighbors** [*ip-address* | *ipv6-prefix*]	BGP ピア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 neighbors** コマンドを使用します。
show bgp [**vrf** *vrf-name*] **sessions**	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。

関連項目

BGP の詳細については、次の項目を参照してください。

- 第 9 章「ベーシック BGP の設定」
- 第 14 章「Route Policy Manager の設定」

デフォルト設定

表 10-1 に、BGP パラメータのデフォルト設定を示します。

表 10-1　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

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.10-37）
- MIB（p.10-37）

関連資料

関連項目	マニュアル名
BGP CLI コマンド	『*Cisco NX-OS Command Line Reference*』
VDC および VRF	『*Cisco NX-OS Virtual Device Contexts Configuration Guide*』

MIB

MIB	MIB リンク
BGP4-MIB CISCO-BGP4-MIB	MIB を検索して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