



高度な 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。

この章は、次の項で構成されています。

- [拡張 BGP の概要](#) (1 ページ)
- [BGP の前提条件](#) (10 ページ)
- [拡張 BGP に関する注意事項と制限事項](#) (10 ページ)
- [BGP のデフォルト設定](#) (12 ページ)
- [高度な BGP の設定](#) (12 ページ)
- [独自の自律システムを含む自律システム パスの設定](#) (36 ページ)
- [BGP グレースフル シャットダウン](#) (53 ページ)
- [拡張 BGP の設定の確認](#) (67 ページ)
- [BGP 統計情報の表示](#) (69 ページ)
- [関連項目](#) (69 ページ)
- [その他の参考資料](#) (70 ページ)

拡張 BGP の概要

BGP は、組織または自律システム間のループフリールーティングを実現する、インターネットメイント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 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、ルータが外部 BGP (eBGP) 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、内部 BGP (iBGP) ピアリング セッションを通じて、ルーティング情報を交換します。

ピア テンプレート

BGP ピア テンプレートを使用すると、類似した BGP ピア間で再利用できる共通のコンフィギュレーションブロックを作成できます。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、ピアのリモート自律システム番号、セッションタイマーなど、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) MD5 パスワードは、BGP ピア間で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。

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変更する場合、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 スピーカー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。

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、トライフィックを転送できます。

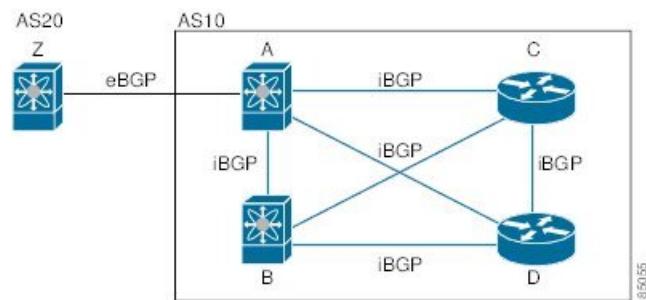
eBGP ピアリングセッションの確立には、ループバックインターフェイスを使用します。ループバックインターフェイスは、インターフェイスフラップが発生する可能性が小さいからです。インターフェイスフラップが発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フォールオーバー、ASパス属性のサイズ制限については、[eBGP の設定](#)のセクションを参照してください。

iBGP

内部 BGP (iBGP) を使用すると、同じ自律システム内の 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（同じ外部自律システム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。

次の図に、より大きな BGP ネットワークの中の iBGP ネットワークを示します。

図 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。



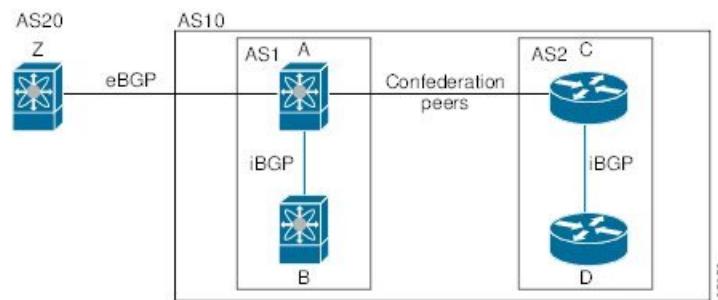
(注) iBGP ネットワークでは別個のインテリアゲートウェイプロトコルを設定する必要があります。

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。自律システムを複数のサブ自律システムに分割し、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、同じ自律システム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。

図には、BGP ネットワークが 2 つのサブ自律システムと 1 つのコンフェデレーションに分けられて表示されています。

図 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 コンフェデレーションを使用することによって、図 1 のフルメッシュ自律システムに比べて、リンク数を少なくできます。

ルートリフレクタ

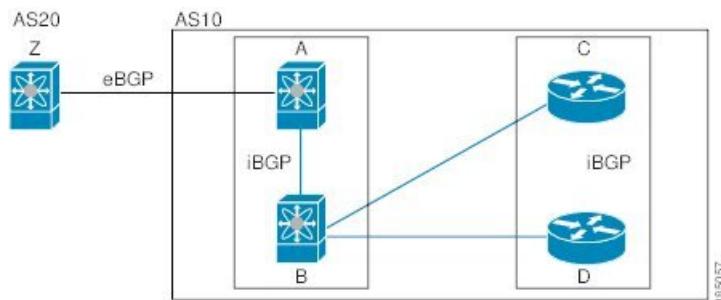
ルートリフレクタ構成を使用することによって、iBGP メッシュを緩和することもできます。ルートリフレクタは学習したルートをネイバーに渡すことで、すべての iBGP ピアをフルメッシュにしなくてもすむようにします。

図 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。

次の図では、ルータ B がルートリフレクタです。ルートリフレクタは、ルータ A からアドバタイズされたルートを受信すると、ルータ C と D へのルートをアドバタイズ (リフレクト) します。ルータ A は、ルータ C と D の両方にアドバタイズする必要がなくなります。

図 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ーが 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。

ルート ダンブニング

ルート ダンブニングは、インターネットワーク上でのフラッピング ルートの伝搬を最小限に抑える 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 自律システム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 ダンブ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、それが他の自律システムに伝播します。

ルート ダンブニングによって、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 ダンブ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（ダンブニング）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ブニング情報を削除します。



(注) ルート ダンブ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、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、選択されたベスト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。

アドバタイズされるルートが少なくなるように、BGP ルート テーブル内には集約プレフィックスが存在します。



(注) Cisco NX-OS は、自動ルート集約をサポートしていません。

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は、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 自律システム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

BGP ネクスト ホップ アドレス トラッキング

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。「[BGP 条件付きアドバタイズメントの設定](#)」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 ベストパスの選択、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) 到達可能性および再帰メトリック 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](#)」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、[ルート ポリシー マネージャの構成のセクション](#)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。

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。たとえば、BGP は IPv4 ユニキャストルーティングのルート 1 セットを伝送します。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。

BGP の前提条件

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。

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 機能を有効にする必要があります（[BGP 機能のイネーブル化](#) のセクションを参照）。
- 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。

拡張 BGP に関する注意事項と制限事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- プレフィックス ピアリングは、パッシブ TCP モードでのみ動作します。ピア アドレスが プレフィックス内にある場合、リモート ピアからの着信接続を受け入れます。
- ダイナミック自律システム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自律システム番号の設定よりも優先します。
- 自律システム連合でプレフィックス ピアにダイナミック自律システム番号を設定した場合、BGP はローカル連合の自律システム番号のみでセッションを確立します。
- ダイナミック自律システム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 マルチホップ存続可能時間 (TTL) 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。
- Cisco NX-OS リリース 9.3(3) 以降では、BGP の BFD は BGP IPv4 と IPv6 のプレフィックス ピアでサポートされます。
- Cisco NX-OS リリース 9.3(3) 以降、BGP プレフィックス ピアはグレースフル リスタートをサポートします。BGP プレフィックス ピアのタイムアウト値（秒単位）を設定するには、ルータ構成モードで **timers prefix-peer-timeout** コマンドを使用します。デフォルト値は 90 秒です。
- IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカルを介した BGP インターフェイス ピアリングには、次の注意事項と制限事項が適用されます。
 - この機能は、複数のインターフェイス間で同じリンクローカルアドレスを設定することをサポートしていません。
 - この機能は、論理インターフェイス（ループバック）ではサポートされていません。イーサネットインターフェイス、ポートチャネルインターフェイス、サブインターフェイス、およびブレークアウトインターフェイスのみがサポートされます。
 - Cisco NX-OS リリース 9.3(6) 以降では、VLAN インターフェイスがサポートされます。
 - この機能は、リンクローカルアドレスを持つ IPv6 対応インターフェイスでのみサポートされます。
 - この機能は、設定されたプレフィックス ピアとインターフェイスのリモート ピアが同じ場合はサポートされません。
 - 次のコマンドはネイバーインターフェイスコンフィギュレーションモードではサポートされていません。
 - **disable-connected-check**
 - **maximum-peers**
 - **update-source**
 - **ebgp-multihop**
 - BFD マルチホップおよび次のコマンドは、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカルを介した BGP インターフェイスピアリングではサポートされません。
 - **bfd-multihop**
 - **bfd multihop interval**
 - **bfd multihop authentication**

BGP のデフォルト設定

- BGPでは、ルートアドバタイズメントのコンバージェンス時間が短縮されます。ルートアドバタイズメント (RA) リンクレベルプロトコルの検出を高速化するには、IPv4 および IPv6 アドレスファミリの IPv6 リンクローカル経由 BGP インターフェイスピアリングを使用する各IPv6対応インターフェイスで次のコマンドを入力します。

```
interface Ethernet port/slot
  ipv6 nd ra-interval 4 min 3
  ipv6 nd ra-lifetime 10
```

BGP のデフォルト設定

次の表に、BGP パラメータのデフォルト設定値を示します。

表 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	無効
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

高度な BGP の設定



(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。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

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

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードになります。
ステップ 2	router bgp <i>autonomous-system-number</i> 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP を有効にして、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 <i>template-name</i> 例： <pre>switch(config-router)# template peer-session BaseSession switch(config-router-stmp)#</pre>	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。

BGP セッション テンプレートの設定

	コマンドまたはアクション	目的
ステップ 4	(任意) password number password 例： <pre>switch(config-router-stmp)# password 0 test</pre>	ネイバーにクリアテキストのパスワード <i>tes</i> 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	(任意) timers keepalive hold 例： <pre>switch(config-router-stmp)# timers 30 90</pre>	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： <pre>switch(config-router-stmp)# exit switch(config-router)#</pre>	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： <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#{</pre>	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： <pre>switch(config-router-neighbor)# inherit peer-session BaseSession switch(config-router-neighbor)#{</pre>	ピアに peer-session テンプレートを適用します。
ステップ 9	(任意) description text 例： <pre>switch(config-router-neighbor)# description Peer Router A switch(config-router-neighbor)#{</pre>	ネイバーの説明を追加します。
ステップ 10	(任意) show bgp peer-session template-name 例： <pre>switch(config-router-neighbor)# show bgp peer-session BaseSession</pre>	peer-policy テンプレートを表示します。
ステップ 11	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで使用できるすべてのコマンドの詳細については、Cisco Nexus 3000 シリーズコマンドリファレンス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。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能の有効化](#)のセクションを参照）。

手順の概要

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

BGP peer-policy テンプレートの設定

11. (任意) copy running-config startup-config

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	router bgp autonomous-system-number 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP を有効にして、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 例： <pre>switch(config-router)# template peer-policy BasePolicy switch(config-router-ptmp)#</pre>	peer-policy テンプレートを作成します。
ステップ 4	(任意) advertise-active-only 例： <pre>switch(config-router-ptmp)# advertise-active-only</pre>	アクティブルートのみをピアにアドバタイズします。
ステップ 5	(任意) maximum-prefix number 例： <pre>switch(config-router-ptmp)# maximum-prefix 20</pre>	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 例： <pre>switch(config-router-ptmp)# exit switch(config-router)#</pre>	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： <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 8	address-family ipv4 unicast 例： switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	指定されたアドレス 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	(任意) show bgp peer-policy template-name 例： switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy	peer-policy テンプレートを表示します。
ステップ 11	(任意) copy running-config startup-config 例： switch(config-router-neighbor)# copy running-config startup-config	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで使用できるすべてのコマンドの詳細については、Cisco Nexus 3000 シリーズ コマンド リファレンス 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 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

BGP peer テンプレートの設定

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。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能のイネーブル化](#) のセクションを参照してください)。

手順の概要

1. **configure terminal**
2. **router bgp *autonomous-system-number***
3. **template peer-session *template-name***
4. (任意) **inherit peer-session *template-name***
5. **address-family ipv4 unicast**
6. (任意) **inherit peer *template-name***
7. **exit**
8. (任意) **timers keepalive hold**
9. **exit**
10. **neighbor *ip-address* remote-as *as-number***
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

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードになります。
ステップ 2	router bgp <i>autonomous-system-number</i> 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP を有効にして、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 <i>template-name</i> 例： 	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。

	コマンドまたはアクション	目的
	switch(config-router)# template peer-session BaseSession switch(config-router-stmp) #	
ステップ 4	(任意) inherit peer-session template-name 例： switch(config-router-neighbor) # inherit peer-session BaseSession	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 unicast 例： 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設定します。
ステップ 6	(任意) inherit peer template-name 例： switch(config-router-neighbor-af) # inherit peer BasePolicy	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ます。
ステップ 7	exit 例： switch(config-router-neighbor-af) # exit switch(config-router) #	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	(任意) timers keepalive hold 例： switch(config-router-neighbor) # timers 45 100	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-stmp) # 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 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 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。
ステップ 12	(任意) timers keepalive hold 例：	このネイバーに BGP タイマー値を追加します。

■ IPv4 および IPv6 アドレス ファミリ向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定

	コマンドまたはアクション	目的
	switch(config-router-neighbor)# timers 60 120	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	(任意) show bgp peer-template template-name 例： switch(config-router-neighbor-af)# show bgp peer-template BasePeer	peer テンプレートを表示します。
ステップ 14	(任意) copy running-config startup-config 例： switch(config-router-neighbor)# copy running-config startup-config	この設定変更を保存します。

例

show bgp neighbor コマンドを実行して、適用されたテンプレートを確認します。テンプレートで使用できるすべてのコマンドの詳細については、Cisco Nexus 3000 シリーズコマンドリファレンス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
```

IPv4 および IPv6 アドレス ファミリ向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定

アンナンバードインターフェイスを使用した自動 BGP ネイバー探索のために、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカルを経由して、BGP インターフェイス ピアリングを設定できます。これにより、インターフェイス名を（インターフェイススコープのアドレスではなく）BGP ピアとして使用する BGP セッションを設定できます。この機能は、ICMPv6 ネイバー探索 (ND) のルートアドバタイズメント (RA) を使用して自動ネイバー探索を行い、RFC 5549 を使用して IPv6 ネクスト ホップで IPv4 ルートを送信します。

始める前に

BGP を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **router bgp *autonomous-system-number***
3. **neighbor *interface-name* remote-as {*as-number* | route-map *map-name*}**
4. **inherit peer *template-name***
5. (任意) **maximum-peers *value***
6. **address-family {*ipv4* | *ipv6*} unicast**
7. (任意) **show bgp {*ipv4* | *ipv6*} unicast neighbors *interface***
8. (任意) **show ip bgp neighbors *interface-name***
9. (任意) **show ipv6 routers [*interface interface*]**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例 : <pre>switch# configure terminal</pre>	コンフィギュレーション モードに入ります。
ステップ2	router bgp <i>autonomous-system-number</i> 例 : <pre>switch(config)# router bgp 65535 switch(config-router) #</pre>	BGP を有効にして、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。AS 番号は 16 ビット整数または 32 ビット整数にできます。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。
ステップ3	neighbor <i>interface-name</i> remote-as {<i>as-number</i> route-map <i>map-name</i>} 例 : <pre>switch(config-router) # neighbor Ethernet1/1 remote-as route-map Testmap switch(config-router-neighbor) #</pre>	<p>BGP ルーティングのためにルータをネイバー設定モードにして、インターフェイスを BGP ピア用に設定します。</p> <p>(注) 指定できるのは、イーサネットインターフェイス、ポートチャネルインターフェイス、サブインターフェイス、およびブレークアウトインターフェイスだけです。</p> <p>Cisco NX-OS リリース 9.3(6) 以降では、ルートマップを指定でき、AS リストを含められるルートマップを指定できます。ダイナミック AS 番号の使用の詳細については、プレフィックス ピアおよびインターフェイス ピアのダイナミック AS 番号 を参照してください。</p>

■ IPv4 および IPv6 アドレス ファミリ向け IPv6 リンク ローカル経由の BGP インターフェイス ピアリングの設定

	コマンドまたはアクション	目的
		設定を複数のインターフェイスに適用する必要がある場合、 <i>interface-name</i> は範囲にすることができます。
ステップ 4	inherit peer template-name 例： <pre>switch(config-router-neighbor)# inherit peer PEER</pre>	peer テンプレートを継承します。
ステップ 5	(任意) maximum-peers value 例： <pre>switch(config-router-neighbor)# maximum-peers 120</pre>	ネイバー設定モードの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。範囲は 1 ~ 1000 です。 (注) 单一のインターフェイス ピアによって起動できるセッションのデフォルト数は 1 です。
ステップ 6	address-family {ipv4 ipv6} unicast 例： <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af) #</pre>	指定のアドレス ファミリに対しグローバル アドレス ファミリ設定モードを開始します。
ステップ 7	(任意) show bgp {ipv4 ipv6} unicast neighbors interface 例： <pre>switch(config-router-neighbor-af) # show bgp ipv4 unicast neighbors e1/25</pre> 例： <pre>switch(config-router-neighbor-af) # show bgp ipv6 unicast neighbors 3FFE:700:20:1::11</pre>	BGP ピアに関する情報を表示します。
ステップ 8	(任意) show ip bgp neighbors interface-name 例： <pre>switch(config-router-neighbor-af) # show ip bgp neighbors Ethernet1/1</pre>	BGP ピアとして使用されるインターフェイスを表示します。
ステップ 9	(任意) show ipv6 routers [interface interface] 例： <pre>switch(config-router-neighbor-af) # show ipv6 routers interface Ethernet1/1</pre>	IPv6 ICMP ルータ アドバタイズメントによって学習されたリモート IPv6 ルータのリンク ローカルアドレスを表示します。
ステップ 10	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor-af) # copy running-config startup-config</pre>	この設定変更を保存します。

例

この例は、ルートマップを使用して、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカル経由で、BGP インターフェイス ピアリングを設定する例を示します。

リーフ 1 の iBGP インターフェイス ピアリング設定：

```
switch# configure terminal
switch(config)# route-map Testmap permit 10
switch(config-route-map)# match as-number 100-200, 300, 400
switch(config-route-map)# exit
switch(config)# router bgp 65000
switch(config-router)# neighbor Ethernet1/1 remote-as route-map Testmap
switch(config-router-neighbor)# inherit peer PEER
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

次に、IPv4 および IPv6 アドレス ファミリの IPv6 リンクローカル経由での、BGP インターフェイス ピアリングのサンプル出力例を示します。

```
switch(config-router-neighbor)# show bgp ipv4 unicast neighbors e1/15.1
BGP neighbor is fe80::2, remote AS 100, ibgp link, Peer index 4
Peer is an instance of interface peering Ethernet1/15.1
BGP version 4, remote router ID 5.5.5.5
Neighbor previous state = OpenConfirm
BGP state = Established, up for 2d16h
Neighbor vrf: default
Peer is directly attached, interface Ethernet1/15.1
Last read 00:00:54, hold time = 180, keepalive interval is 60 seconds
Last written 00:00:08, keepalive timer expiry due 00:00:51
Received 3869 messages, 0 notifications, 0 bytes in queue
Sent 3871 messages, 0 notifications, 0(0) bytes in queue
Enhanced error processing: On
0 discarded attributes
Connections established 2, dropped 1
Last reset by peer 2d16h, due to session closed
Last error length received: 0
Reset error value received 0
Reset error received major: 104 minor: 0
Notification data received:
Last reset by us never, due to No error
Last error length sent: 0
Reset error value sent: 0
Reset error sent major: 0 minor: 0
--More--
```

インターフェイス コンフィギュレーション：

次のいずれかのコマンドを使用して、対応するインターフェイスで IPv6 を有効にする必要があります。

- **ipv6 address *ipv6-address***
- **ipv6 address use-link-local-only**
- **ipv6 link-local *link-local-address***

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ipv6 address use-link-local-only
```



(注) インターフェイスで IPv4 アドレスが設定されていない場合は、**ip forward** コマンドをインターフェイスで設定して IPv4 転送を有効にする必要があります。



(注) IPv6 ND タイマーを調整して、ネイバー探索を高速化し、BGP のルートコンバージェンスを高速化できます。

```
switch(config-if)# ipv6 nd ra-interval 4 min 3
switch(config-if)# ipv6 nd ra-lifetime 10
```



(注) Cisco NX-OS リリース 9.3(6) 以降で、パラレルリンクを使用するカスタマーの導入では、インターフェイスモードで次のコマンドを追加する必要があります。

```
switch(config-if)# ipv6 link-local use-bia
```

このコマンドは、異なるインターフェイス間での IPv6 LLA を一意にします。

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更新を認証するように、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： <pre>switch(config-router-neighbor)# password BGPpassword</pre>	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 設定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： <pre>switch(config-router-neighbor-af)# soft-reconfiguration inbound</pre>	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 { unicast } ip-address soft { in out } 例： <pre>switch# clear bgp ip unicast 192.0.2.1 soft in</pre>	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 例： <pre>switch(config-router-neighbor-af)# next-hop-self</pre>	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： <pre>switch(config-router-neighbor-af)# next-hop-third-party</pre>	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有効であり、無効にすることがでできません。

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 例： <pre>switch(config-router-af)# nexthop trigger-delay critical 5000</pre>	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 例： <pre>switch(config-router-af)# nexthop route-map nextHopLimits</pre>	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 についてベスト 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 例： <pre>switch(config-router-af)# nexthop route-map nextHopLimits</pre>	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。

ネクストホップセルフによるリフレクトルートの制御

NX-OS では、**next-hop-self [all]** 引数を使用して特定のピアに送信する際の iBGP ルートを制御できます。これらの引数を使用すると、ルートのリフレクトが実施されている場合でも、ルートのネクストホップを選択的に変更できます。

コマンド	目的
next-hop-self [all] 例 : <pre>switch(config-router-af) # next-hop-self all</pre>	<p>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。</p> <p>all キーワードはオプションです。all を指定すると、すべてのルートが next-hop-self を使用するピアに送信されます。all を指定しなかった場合、リフレクトしたルートのネクストホップは変更されません。</p>

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 : <pre>switch(config-router-neighbor) # dont-capability-negotiate</pre>	<p>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。</p>

eBGP の設定

このセクションは、次のトピックで構成されています。

eBGP シングルホップ チェックの無効化

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無効にするように、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無効にするには、ネイバー設定モードで次のコマンドを使用します。

■ eBGP マルチホップの設定

コマンド	目的
disable-connected-check 例： <pre>switch(config-router-neighbor)# disable-connected-check</pre>	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無効にします。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 存続可能時間 (TTL) 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-multipath ttl-value 例： <pre>switch(config-router-neighbor)# ebpgp-multipath 5</pre>	eBGP マルチホップの eBGP TTL を設定します。有効な範囲は 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 例： <pre>switch(config-router)# no fast-external-failover</pre>	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、デフォルトでインペーブルになっています。

AS パス属性の制限

AS パス属性で自律システム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 番号の多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 例： 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、2 番めの自律システム (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自律システム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]]] 例： switch(config-router-neighbor) # local-as 1.1	AS_PATH 属性の前に local AS number を付加するよう eBGP を設定します。 local AS number としては 16 ビット整数または 32 ビット整数が可能です。32 ビットの場合、上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式にします。 no-prepend キーワードは、 local AS number とピアリングしているパートナーを除き、 local AS number がダウンストリーム BGP ネイバーの前に付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 属性の前に付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、プリペンドされません。 dual-as キーワードは、eBGP ネイバーを構成し、実際の自律システム番号（ローカルの BGP ルーティングプロセスからのもの）またはローカル AS として構成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します。

eBGP の IPv6 リンクローカル ピアリング (5549) を使用したアンナンバード BGP の設定

アンナンバードインターフェイスを使用した自動 BGP ネイバー探索のために、eBGP の IPv6 リンクローカル ピアリング (5549) により、アンナンバード BGP を設定できます。これにより、インターフェイス名を（インターフェイススコープのアドレスではなく） BGP ピアとして

eBGP の IPv6 リンクローカル ピアリング (5549) を使用したアンナンバード BGP の設定

使用する BGP セッションを設定できます。この機能は、ICMPv6 ネイバー探索 (ND) のルートアドバタイズメント (RA) を使用して自動ネイバー探索を行い、RFC 5549 を使用して IPv6 ネクスト ホップで IPv4 ルートを送信します。

始める前に

BGP を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **router bgp *autonomous-system-number***
3. **neighbor *interface-name* remote-as *as-number***
4. **inherit peer *template-name***
5. **address-family {ipv4 | ipv6} unicast**
6. (任意) **show bgp {ipv4 | ipv6} unicast neighbors *interface***
7. (任意) **show ip bgp neighbors *interface-name***
8. (任意) **show ipv6 routers [*interface interface*]**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp <i>autonomous-system-number</i> 例： <pre>switch(config)# router bgp 65535 switch(config-router) #</pre>	BGP を有効にして、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。AS 番号は 16 ビット整数または 32 ビット整数でできます。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。
ステップ 3	neighbor <i>interface-name</i> remote-as <i>as-number</i> 例： <pre>switch(config-router) # neighbor Ethernet1/1 remote-as 65535 switch(config-router-neighbor) #</pre>	BGP ルーティングのためにルータをネイバー設定モードにして、インターフェイスを BGP ピア用に設定します。 (注) 指定できるのは、イーサネットインターフェイス、ポートチャネルインターフェイス、サブインターフェイス、およびブレークアウトインターフェイスだけです。

	コマンドまたはアクション	目的
ステップ 4	inherit peer template-name 例： switch(config-router-neighbor)# inherit peer PEER	peer テンプレートを継承します。
ステップ 5	address-family {ipv4 ipv6} unicast 例： 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 ファミリ設定モードを開始します。
ステップ 6	(任意) show bgp {ipv4 ipv6} unicast neighbors interface 例： switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors e1/25 例： switch(config-router-neighbor-af)# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11	BGP ピアに関する情報を表示します。
ステップ 7	(任意) show ip bgp neighbors interface-name 例： switch(config-router-neighbor-af)# show ip bgp neighbors Ethernet1/1	BGP ピアとして使用されるインターフェイスを表示します。
ステップ 8	(任意) show ipv6 routers [interface interface] 例： switch(config-router-neighbor-af)# show ipv6 routers interface Ethernet1/1	IPv6 ICMP ルータ アドバタイズメントによって学習されたリモート IPv6 ルータのリンク ローカル アドレスを表示します。
ステップ 9	(任意) copy running-config startup-config 例： switch(config-router-neighbor-af)# copy running-config startup-config	この設定変更を保存します。

例

この例は、eBGP の IPv6 リンクローカル ピアリング (5549) を使用してアンナンバード BGP を設定する方法を示しています。

リーフ 1 の iBGP インターフェイス ピアリング設定：

```
switch# configure terminal
switch(config)# router bgp 65000
switch(config-router)# neighbor Ethernet1/1 remote-as 65000
switch(config-router-neighbor)# inherit peer PEER
switch(config-router-neighbor)# address-family ipv4 unicast
```

eBGP の IPv6 リンクローカルピアリング (5549) を使用したアンナンバード BGP の設定

```
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

この例は、eBGP の IPv6 リンクローカルピアリング (5549) を使用したアンナンバード BGP の出力例を示しています。

```
switch(config-router-neighbor)# show bgp ipv4 unicast neighbors e1/15.1
BGP neighbor is fe80::2, remote AS 100, ibgp link, Peer index 4
Peer is an instance of interface peering Ethernet1/15.1
BGP version 4, remote router ID 5.5.5.5
Neighbor previous state = OpenConfirm
BGP state = Established, up for 2d16h
Neighbor vrf: default
Peer is directly attached, interface Ethernet1/15.1
Last read 00:00:54, hold time = 180, keepalive interval is 60 seconds
Last written 00:00:08, keepalive timer expiry due 00:00:51
Received 3869 messages, 0 notifications, 0 bytes in queue
Sent 3871 messages, 0 notifications, 0(0) bytes in queue
Enhanced error processing: On
0 discarded attributes
Connections established 2, dropped 1
Last reset by peer 2d16h, due to session closed
Last error length received: 0
Reset error value received 0
Reset error received major: 104 minor: 0
Notification data received:
Last reset by us never, due to No error
Last error length sent: 0
Reset error value sent: 0
Reset error sent major: 0 minor: 0
--More--
```

インターフェイス コンフィギュレーション：

次のいずれかのコマンドを使用して、対応するインターフェイスで IPv6 を有効にする必要があります。

- **ipv6 address *ipv6-address***
- **ipv6 address use-link-local-only**
- **ipv6 link-local *link-local-address***

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ipv6 address use-link-local-only
switch(config-if)# ipv6 nd ra-interval 4 min 3
switch(config-if)# ipv6 nd ra-lifetime 10
```



(注) インターフェイスで IPv4 アドレスが設定されていない場合は、**ip forward** コマンドをインターフェイスで設定して IPv4 転送を有効にする必要があります。



(注) IPv6 ND タイマーを調整して、ネイバー探索を高速化し、BGP のルートコンバージョンスを高速化できます。

BGP 属性フィルタリングの設定とエラー処理

Cisco NX-OS リリース 9.3(3) 以降では、BGP 属性フィルタリングとエラー処理を設定して、セキュリティ レベルを向上させることができます。次の機能を利用でき、次の順序で実装されます。

- **パス属性 treat-as-withdraw:** アップデートに指定した属性タイプが含まれている場合に、指定したネイバーから受け取った BGP アップデートを treat-as-withdraw とすることを許可します。アップデートに含まれるプレフィックスは、ルーティングテーブルから削除されます。
- **パス属性 discard:** BGP アップデートの特定のパス属性を特定のネイバーから削除できます。
- **拡張属性エラー処理:** 形式が誤っているアップデートに起因するピア セッションのフラッピングを防止します。

属性タイプ 1、2、3、4、8、14、15、16 は、パス属性 treat-as-withdraw とパス属性 discard に対して設定できません。属性タイプ 9 (Originator)、タイプ 10 (Cluster-id) は、eBGP ネイバーでのみ設定できます。

BGP 更新メッセージからのパス属性の取り消しとしての処理

特定のパス属性を含む BGP 更新を「扱うように」処理するには、ルータ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。

手順

	コマンドまたはアクション	目的
ステップ 1	[no] path-attribute treat-as-withdraw [value range start end] in 例： <pre>switch#(config-router) # neighbor 10.20.30.40 switch(config-router-neighbor) # path-attribute treat-as-withdraw 100 in</pre> 例： <pre>switch#(config-router) # neighbor 10.20.30.40 switch(config-router-neighbor) # path-attribute treat-as-withdraw range 21 255 in</pre>	指定されたパス属性またはパス属性の範囲を含む着信 BGP 更新メッセージをすべて取り消すものとして扱い、ルーティングテーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。treat-as-withdraw である BGP 更新のプレフィックスは、BGP ルーティングテーブルから削除されます。 このコマンドは、BGP テンプレートピアおよび BGP テンプレートピア セッションでもサポートされます。

BGP 更新メッセージからのパス属性の破棄

特定のパス属性を含む BGP アップデートを廃棄するには、ルータ 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。

拡張属性エラー処理のイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	<p>[no] path-attribute discard [value range start end] in</p> <p>例 :</p> <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute discard 100 in</pre> <p>例 :</p> <pre>switch#(config-router)# neighbor 10.20.30.40 switch(config-router-neighbor)# path-attribute discard range 100 255 in</pre>	<p>指定されたネイバーの BGP アップデート メッセージ内の指定されたパス属性をドロップし、ルーティングテーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。特定の属性または不要な属性の範囲全体を設定できます。</p> <p>このコマンドは、BGP テンプレート ピアおよび BGP テンプレート ピア セッションでもサポートされます。</p> <p>(注)</p> <p>discard と treat-as-withdraw の両方に同じパス属性が設定されている場合、treat-as-withdraw の優先順位が高くなります。</p>

拡張属性エラー処理のイネーブル化またはディセーブル化

BGP 拡張属性エラー処理はデフォルトで有効になっていますが、無効にすることもできます。この機能は、RFC 7606 に準拠しており、不正な更新によるピア セッションのフラッピングを防止します。デフォルトの動作は、eBGP ピアと iBGP ピアの両方に適用されます。

拡張エラー処理を無効または再度有効にするには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>[no] enhanced-error</p> <p>例 :</p> <pre>switch(config)# router bgp 1000 switch(config-router)# enhanced-error</pre>	BGP 拡張属性エラー処理をいネーブルまたはディセーブルにします。

取り消されたパス属性または破棄されたパス属性の表示

廃棄または不明なパス属性に関する情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show bgp {ipv4 ipv6} unicast path-attribute discard]	属性が破棄されたすべてのプレフィックスを表示します。

コマンド	目的
show bgp {ipv4 ipv6} unicast path-attribute unknown]	不明な属性を持つすべてのプレフィックスを表示します。
show bgp {ipv4 ipv6} unicast ip-address	プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

次の例は、属性が廃棄されたプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute discard
Network          Next Hop
1.1.1.1/32       20.1.1.1
1.1.1.2/32       20.1.1.1
1.1.1.3/32       20.1.1.1
```

次の例は、不明な属性を持つプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute unknown
Network          Next Hop
2.2.2.2/32       20.1.1.1
2.2.2.3/32       20.1.1.1
```

次の例は、プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

```
switch# show bgp ipv4 unicast 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6241
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
    1000
      20.1.1.1 from 20.1.1.1 (20.1.1.1)
        Origin IGP, localpref 100, valid, external, best
        unknown transitive attribute: flag 0xE0 type 0x62 length 0x64
          value 0000 0000 0100 0000 0200 0000 0300 0000
                  0400 0000 0500 0000 0600 0000 0700 0000
                  0800 0000 0900 0000 0A00 0000 0B00 0000
                  0C00 0000 0D00 0000 0E00 0000 0F00 0000
                  1000 0000 1100 0000 1200 0000 1300 0000
                  1400 0000 1500 0000 1600 0000 1700 0000
                  1800 0000
        rx pathid: 0, tx pathid: 0x0
        Updated on Jul 20 2019 07:50:43 PST
```

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連合内の自律システムグループは、自律システム番号として連合 ID を持つ、1つの自律システムとして認識されます。

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。

独自の自律システムを含む自律システム パスの設定

コマンド	目的
confederation identifier as-number 例 : <pre>switch(config-router)# confederation identifier 64512</pre>	AS 連合を表す連合 ID を設定します。 各連合には別のサブ自律システム番号があり、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 連合に所属する自律システムを設定するには、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 : <pre>switch(config-router)# bgp confederation peers 5 33 44</pre>	連合に所属する自律システム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を含む自律システム (AS) パスを受け入れる機能を BGP でイネーブルにします。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能のイネーブル化](#) のセクションを参照してください)。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config) #</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp as-number 例： <pre>switch(config) # router bgp as-number</pre>	BGP モードを開始し、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。as-number の値の範囲は 1 ~ 65535 です。
ステップ 3	neighbor ip-address remote-as as-number 例： <pre>switch(config-router) # neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor) #</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family ipv4 unicast 例： <pre>switch(config-router-neighbor) # address-family ipv4 unicast switch(config-router-neighbor-af) #</pre>	指定のアドレス ファミリに対応するルータ 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	[no default] allowas-in [allowas-in-cnt] 例： <pre>switch(config-router-neighbor-af) # allowas-in 5</pre>	BGP の allowas-in 機能をイネーブルにし、自律システム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、自律システム番号の発生回数は 3 に設定されます。
ステップ 6	end 例： <pre>switch(config-router-neighbor-af) # end</pre>	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	(任意) show running-config bgp 例： <pre>switch# show running-config bgp</pre>	BGP の設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor) # copy running-config startup-config</pre>	この設定変更を保存します。

ルートリフレクタの設定

例

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。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能の有効化](#) のセクションを参照)。

手順の概要

1. **configure terminal**
2. **router bgp *as-number***
3. **cluster-id *cluster-id***
4. **address-family ipv4 unicast**
5. (任意) **client-to-client reflection**
6. **exit**
7. **neighbor *ip-address* remote-as *as-number***
8. **address-family ipv4 unicast**
9. **route-reflector-client**
10. **show bgp ip unicast neighbors**
11. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp as-number 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP を有効にして、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	cluster-id cluster-id 例： <pre>switch(config-router)# cluster-id 192.0.2.1</pre>	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 unicast 例： <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	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	(任意) client-to-client reflection 例： <pre>switch(config-router-af)# client-to-client reflection</pre>	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なっています。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 例： <pre>switch(config-router-neighbor-af)# exit switch(config-router-neighbor)#</pre>	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： <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#</pre>	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。

ルート ダンプニングの設定

	コマンドまたはアクション	目的
ステップ 8	address-family ipv4 unicast 例： <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af) #</pre>	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 例： <pre>switch(config-router-neighbor-af) # route-reflector-client</pre>	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 unicast neighbors 例： <pre>switch(config-router-neighbor-af) # show bgp ip unicast neighbors</pre>	BGP ピアを表示します。
ステップ 11	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor) # copy running-config startup-config</pre>	この設定変更を保存します。

例

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 [{ <i>half-life reuse-limit suppress-limit max-suppress-time route-map map-name</i> }] 例 : <pre>switch(config-router-af) # dampening route-map bgpDamp</pre>	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。 <ul style="list-style-type: none"> • 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。



(注) ECMP はワープモードではサポートされません。

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] <i>maxpaths</i> 例 : <pre>switch(config-router-af) # maximum-paths 12</pre>	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 ~ 32 です。デフォルトは 1 です。 (注) ECMP構成を防ぐために、ワープモードで maximum-path を 1 に設定することをお勧めします。

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。

BGP 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。

■ ダイナミック機能の設定

コマンド	目的
maximum-prefix maximum [threshold] [restart time warming-only] 例 : <pre>switch(config-router-neighbor-af)# maximum-prefix 12</pre>	<p>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。</p> <ul style="list-style-type: none"> • <i>maximum</i> : 指定できる範囲は 1 ~ 300000 です。 • <i>threshold</i> : 指定できる範囲は 1 ~ 100 % です。デフォルトは 75% です。 • <i>time</i> : 指定できる範囲は 1 ~ 65535 分です。 <p>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。</p>

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 : <pre>switch(config-router-neighbor)# dynamic-capability</pre>	<p>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。</p> <p>このコマンドはデフォルトでは無効になっています。</p>

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
<pre>aggregate-address ip-prefix/length [as-set] [summary-only] [advertise-map map-name] [attribute-map map-name] [suppress-map map-name]</pre> <p>例 :</p> <pre>switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set</pre>	<p>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、自律システム セットです。</p> <ul style="list-style-type: none"> • as-set キーワードは、関係するパスから自律システム セットパス情報およびコミュニティ情報を生成します。 • summary-only キーワードは、アップデートから具体的なルートをすべてフィルタリングします。 • 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では、固有性の強いルートを条件付きでフィルタ処理します。

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 文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 文内にある permit 文のみを処理します。

ルートが条件を満たさない場合、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。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

1. configure terminal

BGP 条件付きアドバタイズメントの設定

2. **router bgp *as-number***
 3. **neighbor *ip-address* remote-as *as-number***
 4. **address-family ipv4 unicast**
 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

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードになります。
ステップ 2	router bgp as-number 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、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	neighbor ip-address remote-as as-number 例： <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family ipv4 unicast 例： <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	アドレス ファミリ設定モードを開始します。
ステップ 5	advertise-map adv-map { exist-map exist-rmap non-exist-map nonexist-rmap } 例： <pre>switch(config-router-neighbor-af)# advertise-map advertise exist-map exist</pre>	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。 <ul style="list-style-type: none"> 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 文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

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • <i>nonexist-rmap</i> : 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。<i>nonexist-rmap</i> 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	(任意) show ip bgp neighbor 例： <pre>switch(config-router-neighbor-af)# show ip bgp neighbor</pre>	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	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

例

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

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。

始める前に

BGP 機能を有効にしていることを確認します ([BGP 機能のイネーブル化](#) のセクションを参照してください)。

手順の概要

1. **configure terminal**
2. **router bgp *as-number***
3. **address-family ipv4 unicast**
4. **redistribute { direct | { eigrp | 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

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードになります。
ステップ 2	router bgp <i>as-number</i> 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、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	address-family ipv4 unicast 例： <pre>switch(config-router)# address-family ipv4 unicast switch(config-router-af)#</pre>	アドレスファミリ設定モードを開始します。
ステップ 4	redistribute { direct { eigrp ospf ospfv3 rip } <i>instance-tag</i> static } route-map <i>map-name</i> 例： <pre>switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmapping</pre>	他のプロトコルからのルートを BGP に再配布します。ルートマップの設定の詳細については、 ルートマップの設定 のセクションを参照してください。

	コマンドまたはアクション	目的
ステップ 5	(任意) default-metric value 例： switch(config-router-af)# default-metric 33	BGP へのデフォルトルートを生成します。
ステップ 6	(任意) copy running-config startup-config 例： switch(config-router-neighbor)# copy running-config startup-config	この設定変更を保存します。

例

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 のユニ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。

始める前に

BGP 機能を有効にしていることを確認します（[BGP 機能のイネーブル化](#)のセクションを参照してください）。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	router bgp as-number 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	BGP モードを開始し、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	neighbor ip-address remote-as as-number 例： <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#</pre>	BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	address-family ipv4 unicast 例： <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	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	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

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 igp-metric ignore med { missing-as-worst non-deterministic } 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。 <ul style="list-style-type: none"> • always-compare-med : 異なる自律システム (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。 • igp-metric ignore : ベストパス選択時に内部ゲートウェイプロトコル (IGP) メトリックを無視します。このオプションは、Cisco NX-OS リリース 9.2(2) 以降で使用可能です。 • med missing-as-worst : 消失した MED を最高の MED と見なします。 • med non-deterministic : 同じ自律システムからのパス間で、必ずしも最適な MED パスを選択しません。 • as-path multipath-relax : AS パスの長さが同じで、他のマルチパスの条件を満たしている場合、別の自律システムから受け取ったパスをマルチパスとして扱えるようにします。
enforce-first-as	ネイバー自律システムを eBGP の AS_path 属性で指定する最初の AS 番号にします。
log-neighbor-changes	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 <i>id</i>	この BGP スピーカのルータ ID を手動で設定します。
timers [bestpath-delay <i>delay</i> bgp keepalive <i>holdtime</i> prefix-peer-timeout <i>timeout</i>]	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。 <p>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。</p>

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： <pre>switch(config-router-af)# distance 20 100 200</pre>	BGP のアドミニスト레이ティブ ディスタンスを設定します。範囲は 1 ~ 255 です。デフォルトの設定は次のとおりです。

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： <pre>switch(config-router-neighbor)# description main site</pre>	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 例： <pre>switch(config-router-neighbor)# low-memory exempt</pre>	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 例： <pre>switch(config-router-neighbor)# transport connection-mode passive</pre>	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： <pre>switch(config-router-neighbor)# remove-private-as</pre>	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： <pre>switch(config-router-neighbor)# update-source ethernet 2/1</pre>	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： <pre>switch(config-router-neighbor-af)# suppress-inactive</pre>	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： <pre>switch(config-router-neighbor-af)# default-originate</pre>	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： <pre>switch(config-router-neighbor-af)# filter-list BGPFILTER in</pre>	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： <pre>switch(config-router-neighbor-af)# prefix-list PrefixFilter in</pre>	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 例： <pre>switch(config-router-neighbor-af)# send-community</pre>	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 例： <pre>switch(config-router-neighbor-af)# send-extcommunity</pre>	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

始める前に

BGP 機能を有効にしていることを確認します（BGP 機能の有効化のセクションを参照）。

手順の概要

1. **configure terminal**
2. **vrf context vrf-name**
3. **exit**
4. **router bgp as-number**

仮想化の設定

5. **vrf *vrf-name***
6. **neighbor *ip-address* remote-as *as-number***
7. (任意) **bestpath as-path multipath-relax**
8. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ2	vrf context <i>vrf-name</i> 例： <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	新しいVRFを作成し、VRF設定モードを開始します。
ステップ3	exit 例： <pre>switch(config-vrf)# exit switch(config)#</pre>	VRF設定モードを終了します。
ステップ4	router bgp <i>as-number</i> 例： <pre>switch(config)# router bgp 65536 switch(config-router)#</pre>	自律システム番号を設定して、新しいBGPプロセスを作成します。
ステップ5	vrf <i>vrf-name</i> 例： <pre>switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#</pre>	ルータVRF設定モードを開始し、このBGPインスタンスとVRFを関連付けます。
ステップ6	neighbor <i>ip-address</i> remote-as <i>as-number</i> 例： <pre>switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536 switch(config-router--vrf-neighbor)#</pre>	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	(任意) bestpath as-path multipath-relax 例： <pre>switch(config-router-vrf)# bestpath as-path multipath-relax</pre>	自律パスの長さが同じで、他のマルチパスの条件を満たしている場合、別の自律システムから受け取ったパスをマルチパスとして扱えるようにします。

	コマンドまたはアクション	目的
ステップ 8	(任意) copy running-config startup-config 例： <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	この設定変更を保存します。

例

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
```

BGP グレースフル シャットダウン

BGP グレース フル シャットダウンに関する情報

リリース 9.3(1) 以降、BGP はグレースフル シャットダウン機能をサポートしています。この BGP 機能は、BGP **shutdown** コマンドと連携します。名前にかかわらず、BGP グレースフル シャットダウンは実際にはシャットダウンを引き起こしません。代わりに、ルータまたはリンクが間もなくダウンすることを、接続されているルータに通知します。

- ルータまたはリンクがオフラインになったときのネットワークコンバージェンス時間を大幅に短縮します。
- ルータまたはリンクがオフラインになったときに、転送中のドロップされたパケットを削減または排除します。

グレースフル シャットダウン機能は、GRACEFUL_SHUTDOWN ウエルノウン コミュニティ (0xFFFFF0000 または 65535:0) を使用します。これは、IANA および IETF によって RFC 8326 によって識別されます。この既知のコミュニティは任意のルートにアタッチでき、ルートの他の属性と同様に処理されます。

この機能は、ルータまたはリンクがダウンすることを通知するため、メンテナンス時間帯または計画停止の準備に役立ちます。トライフィックへの影響を制限するには、BGP をシャットダウンする前にこの機能を使用します。

グレースフルシャットダウンの認識とアクティブ化

BGPルータは、すべてのルートの優先事項を、GRACEFUL SHUTDOWN 対応というコンセプトを通し、GRACEFUL_SHUTDOWN コミュニティによって制御できます。グレースフルシャットダウン対応は、デフォルトでイネーブルになっています。これにより、受信側ピアは、GRACEFUL_SHUTDOWN コミュニティを伝える着信ルートを優先しなくなります。一般的な使用例ではありませんが、**graceful-shutdown aware** コマンドを使用して、グレースフルシャットダウン対応を無効にしてから再度有効にすることもできます。

グレースフルシャットダウン対応は、BGP グローバルコンテキストでのみ適用されます。コンテキストの詳細については、[グレースフルシャットダウンのコンテキスト（54 ページ）](#) を参照してください。対応のためのオプションは、**activate** という別のオプションと一緒に動作します。このオプションをルートマップに割り当てるとき、グレースフルシャットダウンのルートをより詳細に制御できます。

グレースフルシャットダウン対応オプションとアクティブ化オプションの協同作用

グレースフルシャットダウンがアクティブな場合、**activate** キーワードを指定した場合にのみ、GRACEFUL_SHUTDOWN コミュニティがルート更新に追加されます。この時点で、コミュニティを含む新しいルート更新が生成され、送信されます。**graceful-shutdown aware** コマンドが設定されると、コミュニティを受信するすべてのルータは、アップデート内のルートの優先を解除します（そのルート優先度を下げます）。**graceful-shutdown aware** コマンドを使用しなかった場合、BGPはGRACEFUL_SHUTDOWN コミュニティの設定されたルートの優先度を下げません。

この機能がアクティブになり、ルータがグレースフルシャットダウンの対応状態になった場合でも、BGPは引き続き、GRACEFUL_SHUTDOWN コミュニティが有効だとしてルートを考慮します。ただし、これらのルートには、最適パスの計算で最低の優先度が与えられます。代替パスが使用可能な場合は、新しい最適パスが選択され、まもなくダウンするルータまたはリンクに対応するためのコンバージェンスが行われます。

グレースフルシャットダウンのコンテキスト

BGPのグレースフルシャットダウン機能には、機能の影響と使用可能な機能を決定する2つのコンテキストがあります。

コンテキスト	影響	コマンド
グローバル	スイッチ全体と、スイッチによって処理されるすべてのルート。たとえば、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートを再アドバタイズします。	graceful-shutdown activate [route-map ルートマップ] graceful-shutdown aware

コンテキスト	影響	コマンド
Peer	BGP ピアまたはネイバー間のリンク。たとえば、ピア間のリンクを 1 つだけ GRACEFUL_SHUTDOWN コミュニティでアドバタイズします。	graceful-shutdown activate [route-map ルートマップ]

ルートマップによるグレースフルシャットダウン

グレースフルシャットダウンは、ルートポリシーマネージャ（RPM）機能と連携して、スイッチの BGP ルータが GRACEFUL_SHUTDOWN コミュニティを使用してルートを送受信する方法を制御します。ルートマップは、インバウンドおよびアウトバウンド方向でコミュニケーションとのルート更新を処理できます。通常、ルートマップは必要ありません。ただし、必要に応じて、グレースフルシャットダウンルートの制御をカスタマイズするために使用できます。

通常のインバウンドルートマップ

通常のインバウンドルートマップは、BGP ルータに着信するルートに影響します。ルータはデフォルトでグレースフルシャットダウンを認識するため、通常のインバウンドルートマップはグレースフルシャットダウン機能では一般的に使用されません。

Cisco NX-OS リリース 9.3 (1) 以降を実行している Cisco Nexus スイッチでは、グレースフルシャットダウン機能のインバウンドルートマップは必要ありません。Cisco NX-OS リリース 9.3 (1) 以降には、BGP ルータがグレースフルシャットダウン対応である場合に GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートを自動的に非優先にする、暗黙のインバウンドルートマップがあります。

通常のインバウンドルートマップは、既知の GRACEFUL_SHUTDOWN コミュニティと一致するように設定できます。これらの着信ルートマップは一般的ではありませんが、使用される場合があります。

- スイッチが 9.3 (1) よりも前の Cisco NX-OS リリースを実行している場合、NX-OS 9.3 (1) には暗黙的なインバウンドルートマップがありません。これらのスイッチでグレースフルシャットダウン機能を使用するには、グレースフルシャットダウンインバウンドルートマップを作成する必要があります。ルートマップは、既知の GRACEFUL_SHUTDOWN コミュニティを持つインバウンドルートと一致し、それらを許可し、それらを非優先にする必要があります。着信ルートマップが必要な場合は、9.3 (1) より前のバージョンの NX-OS を実行し、グレースフルシャットダウンルートを受信している BGP ピアで作成します。
- グレースフルシャットダウン認識をディセーブルにし、一部の BGP ネイバーからの GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートでルータを動作させる場合は、それぞれのピアでインバウンドルートマップを設定できます。

通常のアウトバウンドルート マップ

通常のアウトバウンドルート マップは、BGP ルータが送信するルートの転送を制御します。通常のアウトバウンドルート マップは、グレースフルシャットダウン機能に影響を与える可能性があります。たとえば、GRACEFUL_SHUTDOWN コミュニティで一致するようにアウトバウンドルート マップを設定し、属性を設定できます。これは、グレースフルシャットダウン アウトバウンドルート マップよりも優先されます。

グレースフルシャットダウン アウトバウンドルート マップ

アウトバウンドグレースフルシャットダウンルート マップは、グレースフルシャットダウン機能のアウトバウンドルート マップの特定のタイプです。これらはオプションですが、ルート マップに関連付けられているコミュニティリストがすでにある場合に役立ちます。通常のグレースフルシャットダウン アウトバウンドルート マップには、特定の属性を設定または変更するための `set` 句のみが含まれています。

アウトバウンドルート マップは、次の方法で使用できます。

- 既存のアウトバウンドルート マップをすでに持っている顧客の場合は、より大きいシーケンス番号を持つ新しいエントリを追加し、GRACEFUL_SHUTDOWN ウェルノウン コミュニティで照合し、必要な属性を追加できます。
- graceful-shutdown activate route-map name** オプションを使用してグレースフルシャットダウン アウトバウンドルート マップを使用することもできます。これが一般的な使用例です。

このルート マップには `match` 句が必要ないため、ルート マップはネイバーに送信されるすべてのルートで一致します。

ルート マップの優先順位

同じルータ上に複数のルート マップが存在する場合は、次の優先順位が適用されて、コミュニティとのルートの処理方法が決定されます。次の例を考慮してください。60 のローカル設定を設定する標準の発信ルート マップ名 Red があるとします。また、Blue という名前のピアグレースフルシャットダウンルート マップがあり、local-pref が 30 に設定されているとします。ルート更新が処理されると、Red は Blue を上書きするため、ローカルプリファレンスは 60 に設定されます。

- 通常の発信ルート マップは、ピアグレースフルシャットダウン マップよりも優先されます。
- ピアグレースフルシャットダウン マップは、グローバルグレースフルシャットダウン マップよりも優先されます。

注意事項と制約事項

BGP グローバルシャットダウンの制限事項と注意事項は、次のとおりです。

- グレースフルシャットダウン機能は、影響を受けるルータの代替ルートがネットワークに存在する場合にのみ、トラフィック損失を回避するのに役立ちます。ルータに代替ルートがない場合は、GRACEFUL_SHUTDOWN コミュニティを伝送するルートが使用可能な唯一のルートであるため、最適パスの計算に使用されます。この状況では、機能の目的が失われます。
- GRACEFUL_SHUTDOWN コミュニティを送信するには、BGP 送信コミュニティの設定が必要です。
- ルートマップの場合:
 - グローバルルートマップとネイバールートマップが設定されている場合、ネイバー単位のルートマップが優先されます。
 - 発信ルートマップは、グレースフルシャットダウン用に設定されたグローバルルートマップよりも優先されます。
 - 発信ルートマップは、グレースフルシャットダウン用に設定されたピアルートマップよりも優先されます。
 - レガシー（既存の）インバウンドルートマップにグレースフルシャットダウン機能を追加するには、次の手順を実行します。
 1. `graceful shutdown match` 句をルートマップの先頭に追加します。これには、句に低いシーケンス番号（たとえば、シーケンス番号 0）を設定します。
 2. `graceful shutdown` 句の後に `continue` ステートメントを追加します。`continue` ステートメントを省略すると、`graceful shutdown` 句と一致するルートマップ処理が停止します。シーケンス番号が大きい他の句（たとえば、1以上）は処理されません。

グレースフルシャットダウンタスクの概要

グレースフルシャットダウン機能を使用するには、通常、すべての Cisco Nexus スイッチでグレースフルシャットダウン対応をイネーブルにし、機能をイネーブルのままにします。BGP ルータをオフラインにする必要がある場合は、`graceful-shutdown activate` を設定します。

次の詳細に、グレースフルシャットダウン機能を使用するためのベストプラクティスを示します。

- ルータまたはリンクをダウンさせるには、次の手順を実行します。
1. グレースフルシャットダウン機能を設定します。
 2. ネイバーでベストパスを確認します。
 3. 最適パスが再計算されたら、BGP を無効にする `shutdown` コマンドを発行します。
 4. ルータまたはリンクをシャットダウンする必要がある作業を実行します。

ルータまたはリンクをオンラインに戻すには、次の手順を実行します。

リンクのグレースフルシャットダウンの設定

1. シャットダウンが必要な作業が完了したら、BGP を再度イネーブルにします (**no shutdown**)。
 2. グレースフルシャットダウン機能を無効にします (config モードの **no graceful-shutdown activate**)。

リンクのグレースフルシャットダウンの設定

この作業では、2つのBGPルータ間の特定のリンクでグレースフルシャットダウンを設定できます。

始める前に

BGPをまだ有効にしていない場合は、ここで有効にします (**feature bgp**)。

手順の概要

1. config terminal
 2. router bgp *autonomous-system-number*
 3. neighbor { *ipv4-address|ipv6-address* } remote-as *as-number*
 4. graceful-shutdown activate [route-map *map-name*]

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	config terminal 例： switch-1# configure terminal switch-1(config)#	グローバル 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-1(config)# router bgp 110 switch-1(config-router)#	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 3	neighbor { ipv4-address ipv6-address } remote-as as-number 例： switch-1(config-router)# neighbor 10.0.0.3 remote-as 200 switch-1(config-router-neighbor)#{	ネイバーが属する自律システム (AS) を設定します。
ステップ 4	graceful-shutdown activate [route-map map-name] 例：	ネイバーへのリンクでグレースフルシャットダウンを設定します。また、既知の

コマンドまたはアクション	目的
<pre>switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer switch-1(config-router-neighbor)#</pre>	<p>GRACEFUL_SHUTDOWN コミュニティを使用してルートをアドバタイズし、アウトバウンドルート更新にルートマップを適用します。</p> <p>ルートは、デフォルトでグレースフルシャットダウン コミュニティでアドバタイズされます。この例では、ルートは gshutPeer という名前のルートマップを使用して、グレースフルシャットダウン コミュニティを持つネイバーにアドバタイズされます。</p> <p>gshut コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティング ポリシーを適用します。</p>

GRACEFUL_SHUTDOWN コミュニティに基づく BGP ルートのフィルタリングとローカルプリファレンスの設定

まだ 9.3(1) を実行していないスイッチには、GRACEFUL_SHUTDOWN コミュニティ名と一致するインバウンドルートマップがありません。したがって、正しいルートを識別して先送りする方法はありません。

9.3(1) よりも前のリリースの NX-OS を実行しているスイッチでは、グレースフルシャットダウン (65535:0) のコミュニティ値と一致するインバウンドルートマップを設定し、ルートを非優先にする必要があります。

スイッチが 9.3(1) 以降を実行している場合、着信ルートマップを設定する必要はありません。

手順の概要

1. **configure terminal**
2. **ip community list standard *community-list-name* seq *sequence-number* { permit | deny } *value***
3. **route map *map-tag* {deny | permit} *sequence-number***
4. **match community *community-list-name***
5. **set local-preference *local-pref-value***
6. **exit**
7. **router bgp *community-list-name***
8. **neighbor { *ipv4-address|ipv6-address* }**
9. **address-family { *address-family sub family* }**
10. **send community**
11. **route map *map-tag* in**

GRACEFUL_SHUTDOWN コミュニティに基づく BGP ルートのフィルタリングとローカルプリファレンスの設定

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch-1# configure terminal switch-1<config>#</pre>	グローバル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	ip community list standard community-list-name seq sequence-number { permit deny } value 例： <pre>switch-1(config)# ip community-list standard GSHUT seq 10 permit 65535:0 switch-1(config)#</pre>	コミュニティリストを設定し、よく知られたグレースフルシャットダウン コミュニティ値を持つルートを許可または拒否します。
ステップ 3	route map map-tag {deny permit} sequence-number 例： <pre>switch-1(config)# route-map RM_GSHUT permit 10 switch-1(config-route-map)#</pre>	ルートマップをシーケンス 10 として設定し、GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。
ステップ 4	match community community-list-name 例： <pre>switch-1(config-route-map)# match community GSHUT switch-1(config-route-map)#</pre>	IP コミュニティリスト GSHUT に一致するルートがルートポリシーマネージャ (RPM) により処理されるように設定します。
ステップ 5	set local-preference local-pref-value 例： <pre>switch-1(config-route-map)# set local-preference 10 switch-1(config-route-map)#</pre>	IP コミュニティリスト GSHUT に一致するルートに、指定されたローカルプリファレンスが与えられるように設定します。
ステップ 6	exit 例： <pre>switch-1(config-route-map)# exit switch-1(config)#</pre>	ルートマップ設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	router bgp community-list-name 例： <pre>switch-1(config)# router bgp 100 switch-1(config-router)#</pre>	ルータ設定モードを開始し、BGP インスタンスを作成します。
ステップ 8	neighbor { ipv4-address ipv6-address } 例： <pre>switch-1(config-router)# neighbor 10.0.0.3 switch-1(config-router-neighbor)#</pre>	指定したネイバーのルート BGP ネイバー モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	address-family { address-family sub family } 例： <pre>nxosv2 (config-router-neighbor) # address-family ipv4 unicast nxosv2 (config-router-neighbor-af) #</pre>	ネイバーをアドレス ファミリ (AF) 設定モードにします。
ステップ 10	send community 例： <pre>nxosv2 (config-router-neighbor-af) # send-community nxosv2 (config-router-neighbor-af) #</pre>	ネイバーとの BGP コミュニティ交換を可能にします。
ステップ 11	route map map-tag in 例： <pre>nxosv2 (config-router-neighbor-af) # route-map RM_GSHUT in nxosv2 (config-router-neighbor-af) #</pre>	ネイバーからの着信ルートにルート マップを適用します。この例では、RM_GSHUT という名前のルート マップは、ネイバーからの GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。

すべての BGP ネイバーのグレースフル シャットダウンの設定

グレースフル シャットダウン イニシエータのすべてのネイバーに GRACEFUL_SHUTDOWN ウェルノウン コミュニティを手動で適用できます。

すべての BGP ネイバーに対して、グローバル レベルでグレースフル シャットダウンを設定できます。

始める前に

BGP をまだ有効にしていない場合は、ここで有効にします (**feature bgp**)。

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system-number**
3. **graceful-shutdown activate [route-map map-name]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch-1# configure terminal switch-1(config) #</pre>	グローバル コンフィギュレーション モードを開始します。

GRACEFUL_SHUTDOWN コミュニティを使用したすべてのルートの pri ファレンスの制御

	コマンドまたはアクション	目的
ステップ 2	router bgp autonomous-system-number 例： <pre>switch-1(config)# router bgp 110 switch-1(config-router)# </pre>	ルータコンフィギュレーションモードを開始して、BGP ルーティングプロセスを作成または設定します。
ステップ 3	graceful-shutdown activate [route-map map-name] 例： <pre>switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer switch-1(config-router-neighbor)# </pre>	すべてのネイバーへのリンクのグレースフルシャットダウンルートマップを設定します。また、既知の GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートをアドバタイズし、ルートマップをアウトバウンドルートアップデートに適用します。 ルートはデフォルトで GRACEFUL_SHUTDOWN コミュニティでアドバタイズされます。この例では、ルートが gshutPeer という名前のルートマップを持つコミュニティを持つすべてのネイバーにアドバタイズされます。ルートマップには set 句のみを含める必要があります。 GRACEFUL_SHUTDOWN コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティングポリシーを適用します。

GRACEFUL_SHUTDOWN コミュニティを使用したすべてのルートの pri ファレンスの制御

Cisco NX-OS では、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートの優先順位を下げるすることができます。 **graceful shutdown aware** が有効になっている場合、最適パス計算時に、BGP はコミュニティを伝送するルートを最も低い優先順位と見なします。デフォルトでは、pri ファレンスの引き下げが有効になっていますが、このオプションを選択的に無効にすることもできます。

このオプションをイネーブルまたはディセーブルにするたびに、BGP のベストパス計算がトリガーされます。このオプションを使用すると、グレースフルシャットダウンのウェルノウンコミュニティにおける BGP のベストパス計算の動作を柔軟に制御できます。

始める前に

BGP を有効にしていない場合は、ここで有効にします (**feature bgp**)。

手順の概要

1. **configure terminal**
2. **router bgp autonomous-system**
3. (任意) **no graceful-shutdown aware**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch-1(config)# config terminal switch-1(config)#{</pre>	グローバル 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 例： <pre>switch-1(config)# router bgp 100 switch-1(config-router)#{</pre>	ルータ コンフィギュレーション モードを開始し、BGP ルーティング プロセスを設定します。
ステップ 3	(任意) no graceful-shutdown aware 例： <pre>switch-1(config-router)#{ no graceful-shutdown aware switch-1(config-router)#{</pre>	このBGPルータでは、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートに低い優先順位を指定しないという意味です。グ雷斯フルシャットダウン認識機能がディセーブルになっている場合、デフォルトアクションはルートを非優先にします。そのため、コマンドには no 形式というオプションが存在しており、これを使用すると、グ雷斯フルシャットダウンルートは非優先になりません。

GRACEFUL_SHUTDOWN コミュニティのピアへの送信の防止

発信ルート更新にルート属性として追加されたGRACEFUL_SHUTDOWN コミュニティが不要になった場合は、コミュニティを削除して、指定されたネイバーに送信しなくなります。1つの使用例は、ルータが自律システム境界にあり、グ雷斯フルシャットダウン機能が自律システム境界の外部に伝播しないようにする場合です。

GRACEFUL_SHUTDOWN がピアに送信されないようにするには、send community オプションを無効にするか、コミュニティを発信ルートマップから削除します。

次の方法の中から 1 つを選択してください。

- 実行コンフィギュレーションで send-community を無効にします。

例：

```
nxosv2(config-router-neighbor-af)#{ no send-community standard
nxosv2(config-router-neighbor-af)#{
```

このオプションを使用すると、スイッチはGRACEFUL_SHUTDOWN コミュニティを受信しますが、発信ルートマップを介してダウンストリーム ネイバーに送信されません。すべての標準コミュニティも送信されません。

■ グレースフルシャットダウン情報の表示

- 次の手順に従って、発信ルートマップを介して GRACEFUL_SHUTDOWN コミュニティを削除します。

- GRACEFUL_SHUTDOWN コミュニティと一致する IP コミュニティリストを作成します。
- GRACEFUL_SHUTDOWN コミュニティと照合する発信ルートマップを作成します。
- set community-list delete** 句を使用して GRACEFUL_SHUTDOWN コミュニティを削除します。

このオプションを使用すると、コミュニティリストは GRACEFUL_SHUTDOWN コミュニティと一致し、許可されます。その後、発信ルートマップはコミュニティと照合され、発信ルートマップから削除されます。他のすべてのコミュニティは、問題なく発信ルートマップを通過します。

グレースフルシャットダウン情報の表示

グレースフルシャットダウン機能に関する情報は、次の **show** コマンドで確認できます。

コマンド	アクション
show ip bgp community-list graceful-shutdown	GRACEFUL_SHUTDOWN コミュニティを持つ BGP ルーティングテーブル内のすべてのエントリを表示します。
show running-config bgp	実行中の BGP のデフォルト設定を示します。
show running-config bgp all	グレースフルシャットダウン機能に関する情報など、実行中の BGP 設定のすべての情報を表示します。
show bgp address-family neighbors neighbor-address	機能がピアに設定されている場合、次のように表示されます。 <ul style="list-style-type: none"> 指定されたネイバーの graceful-shutdown-activate 機能の状態 指定されたネイバーに設定されたグレースフルシャットダウンルートマップの名前

コマンド	アクション
show bgp process	コンテキストに応じて異なる情報を表示します。 graceful-shutdown-activate オプションがピア コンテキストで設定されている場合、 graceful-shutdown-active を介して機能の有効または無効状態を示します。 graceful-shutdown-activate オプションがグローバル コンテキストで設定され、 graceful-shutdown ルートマップがある場合は、次のように機能の有効状態が表示されます。 <ul style="list-style-type: none">• graceful-shutdown-active• graceful-shutdown-aware• graceful-shutdown route-map
show ip bgp address	指定されたアドレスについて、次を含む BGP ルーティング テーブル情報を表示します。 <ul style="list-style-type: none">• 最適パスとして指定されたアドレスの状態• 指定されたアドレスが GRACEFUL_SHUTDOWN コミュニティの一部であるかどうか

グレースフル シャットダウンの設定例

次に、グレースフルシャットダウン機能を使用するための設定例を示します。

BGP リンクのグレースフル シャットダウンの設定

次に、ローカルプリファレンスとコミュニティを設定しながらグレースフルシャットダウンを設定する例を示します。

- 指定されたネイバーへのリンクのグレースフル シャットダウン アクティブ化の設定
- ルートへの GRACEFUL_SHUTDOWN コミュニティの追加
- コミュニティとのアウトバウンドルートに対して set 句のみを使用して gshutPeer という名前のルートマップを設定します。

```
router bgp 100
neighbor 20.0.0.3 remote-as 200
graceful-shutdown activate route-map gshutPeer
address-family ipv4 unicast
send-community
```

■ グレースフルシャットダウンの設定例

```
route-map gshutPeer permit 10
  set local-preference 0
  set community 200:30
```

All-Neighbor BGP リンクのグレースフルシャットダウンの設定

次に例を示します。

- ローカルルータとそのすべてのネイバーを接続するすべてのリンクに対してグレースフルシャットダウンアクティブ化を設定します。
- GRACEFUL_SHUTDOWN コミュニティをルートに追加しています。
- すべての発信ルートに対して set 句のみを使用して gshutAll という名前のルートマップを設定します。

```
router bgp 200
  graceful-shutdown activate route-map gshutAll

route-map gshutAll permit 10
  set as-path prepend 10 100 110
  set community 100:80

route-map Red permit 10
  set local-pref 20

router bgp 100
  graceful-shutdown activate route-map gshutAll
  router-id 2.2.2.2
    address-family ipv4 unicast
    network 2.2.2.2/32
    neighbor 1.1.1.1 remote-as 100
    update-source loopback0
    address-family ipv4 unicast
      send-community
    neighbor 20.0.0.3 remote-as 200
    address-family ipv4 unicast
      send-community
      route-map Red out
```

この例では、ネイバー 1.1.1.1 に対して gshutAll ルートマップが有効になりますが、ネイバー 20.0.0.3 で設定された発信ルートマップ Red が優先されるため、ネイバー 20.0.0.3 に対しては有効になりません。

ピアテンプレートでのグレースフルシャットダウンの設定

この例では、ピアセッションテンプレートでグレースフルシャットダウン機能を設定します。これはネイバーによって継承されます。

```
router bgp 200
  template peer-session p1
    graceful-shutdown activate route-map gshut_out
  neighbor 1.1.1.1 remote-as 100
    inherit peer-session p1
    address-family ipv4 unicast
      send-community
```

GRACEFUL_SHUTDOWN コミュニティの使用およびインバウンドルートマップに基づく BGP ルートのフィルタリングとローカルプリファレンスの設定

次に、コミュニティリストを使用して、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートをフィルタリングする例を示します。この設定は、Cisco NX-OS 9.3(1) を最小バージョンとして実行していないレガシースイッチに役立ちます。

次に例を示します。

- GRACEFUL_SHUTDOWN コミュニティを持つルートを許可する IP コミュニティリスト。
- RM_GSHUT という名前のルートマップは、GSHUT という名前の標準コミュニティリストに基づいてルートを許可します。
- また、ルートマップは、処理するルートの優先順位を 0 に設定します。これにより、ルータがオフラインになったときに、それらのルートに最適パス計算の優先順位が低くなります。ネイバー (20.0.0.2) からの着信 IPv4 ルートにルートマップが適用されます。

```
ip community-list standard GSHUT permit 65535:0
route-map RM_GSHUT permit 10
  match community GSHUT
  set local-preference 0
router bgp 200
  neighbor 20.0.0.2 remote-as 100
    address-family ipv4 unicast
      send-community
      route-map RM_GSHUT in
```

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 {unicast} [ip-address] 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 {unicast} [ip-address] community-list list-name [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。

■ 拡張 BGP の設定の確認

コマンド	目的
show bgp ip {unicast} [ip-address] 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 {unicast} [ip-address] extcommunity-list list-name [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 {unicast} [ip-address] {dampening dampened-paths [regexp expression]} [vrf vrf-name]	BGP ルート ダンピングの情報を表示します。ルート フラップ ダンピ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 {unicast} [ip-address] 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 {unicast} [ip-address] 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 {unicast} [ip-address] neighbors [ip-address] [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 {unicast} [ip-address] {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 {unicast} [ip-address] 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。
show bgp ip {unicast} [ip-address] 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 {unicast} [ip-address] 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 {unicast} [ip-address] 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 {unicast} [ip-address] 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。

コマンド	目的
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 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 シリーズ コマンド リファレンス を参照してください。
show ip 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 シリーズ コマンド リファレンス 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 {unicast} [ip-address] 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クリアするには、 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クリアするには、 clear bgp sessions 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クリアするには、 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。

関連項目

BGP の詳細については、次の項目を参照してください。

■ その他の参考資料

- 基本的 BGP の設定
- Route Policy Manager の設定

その他の参考資料

BGP の実装に関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
- MIB

関連資料

関連項目	マニュアル タイトル
BGP CLI コマンド	『Cisco Nexus 3000 Series Command Reference』

MIB

MIB	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	MIB を検索してダウンロードするには、次の MIB ロケータ に移動します。

翻訳について

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