



BGP の設定

- [BGP の制約事項 \(1 ページ\)](#)
- [BGP に関する情報 \(1 ページ\)](#)
- [BGP の設定方法 \(16 ページ\)](#)
- [BGP の設定例 \(60 ページ\)](#)
- [BGP のモニタリングおよびメンテナンス \(63 ページ\)](#)
- [ボーダー ゲートウェイ プロトコルの機能情報 \(64 ページ\)](#)

BGP の制約事項

グレースフルリスタートが無効になっている場合でも、BGP ホールド時間は常にデバイスのグレースフルリスタートのホールド時間よりも長く設定する必要があります。ホールド時間がサポートされていないピアデバイスでは、オープンメッセージを介してデバイスとのセッションを確立できますが、グレースフルリスタートが有効になっていると、セッションはフラッピングします。

BGP に関する情報

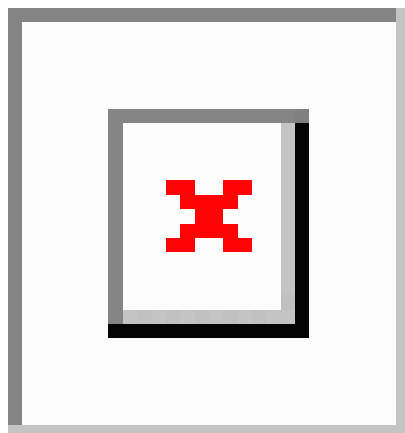
ボーダー ゲートウェイ プロトコル (BGP) は、Exterior Gateway Protocol です。自律システム間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティングシステムを設定するために使用されます。自律システムは、同じ管理下で動作して RIP や OSPF などの Interior Gateway Protocol (IGP) を境界内で実行し、Exterior Gateway Protocol (EGP) を使用して相互接続されるルータで構成されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。

BGP ネットワーク トポロジ

同じ自律システム (AS) に属し、BGP アップデートを交換するルータは内部 BGP (IBGP) を実行し、異なる自律システムに属し、BGP アップデートを交換するルータは外部 BGP (EBGP) を実行します。大部分のコンフィギュレーションコマンドは、EBGP と IBGP で同じですが、

ルーティングアップデートが自律システム間で交換されるか（EBGP）、または AS 内で交換されるか（IBGP）という点で異なります。下の図に、EBGP と IBGP の両方を実行しているネットワークを示します。

図 1: EBGP、IBGP、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼働する IGP に BGP ルーティング情報を再配布して、AS 内のネットワークに到達することを確認します。

BGP ルーティングプロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。BGP はトランスポートプロトコルとして伝送制御プロトコル（TCP）を使用します（特にポート 179）。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。上の図では、ルータ A と B が BGP ピアで、ルータ B と C、ルータ C と D も同様です。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない自律システムマップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼働し、2 つのネイバーが相互に到達するかぎり、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（連合およびルートリフレクタ）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティングテーブルを最初に交換し、差分更新だけを送信します。BGP ピアはキープアライブメッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGPの場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（自律システムパス）、および他のパス属性リストで構成されます。BGPシステムの主な機能は、ASパスのリストに関する情報など、ネットワークの到達可能性情報を他のBGPシステムと交換することです。この情報は、ASが接続されているかどうかを判別したり、ルーティンググループをプルーニングしたり、ASレベルポリシー判断を行うために使用できます。

Cisco IOSが稼働しているルータやデバイスがIBGPルートを選択または使用するのには、ネクストホップルータで使用可能なルートがあり、IGPから同期信号を受信している（IGP同期が無効の場合は除く）場合です。複数のルートが使用可能な場合、BGPは属性値に基づいてパスを選択します。BGP属性については、「BGP判断属性の設定」の項を参照してください。

BGPバージョン4ではクラスレスドメイン間ルーティング（CIDR）がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティングテーブルのサイズを削減できます。CIDRは、BGP内部のネットワーククラス概念をエミュレートし、IPプレフィックスのアドバタイズをサポートします。

NSF 認識

BGP NSF 認識機能は、Network Advantage ライセンスで IPv4 に対してサポートされます。。BGP ルーティングでこの機能を有効にするには、グレースフル リスタートを有効にする必要があります。隣接ルータが NSF 対応で、この機能が有効になっている場合、レイヤ 3 デバイスは、ルータに障害が発生してプライマリルートプロセッサ（RP）がバックアップ RP によって引き継がれる間、または無停止ソフトウェアアップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

BGP ルーティングに関する情報

BGP ルーティングを有効にするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ~ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーションコマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は

IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。同期化は、デフォルトで有効に設定されています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼働している場合は、同期化を無効にし、IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束するようにします。

ルーティング ポリシーの変更

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンドルーティングテーブルアップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。このあとで BGP フィルタ、重み、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハードリセットとソフトリセットの 2 種類があります。Cisco IOS Release 12.1 以降では、事前に設定を行わなくても、ソフトリセットを使用できます。事前設定なしにソフトリセットを使用するには、両方の BGP ピアでソフトルートリフレッシュ機能がサポートされていないならばなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。ソフトリセットを使用すると、BGP ルータ間でルートリフレッシュ要求およびルーティング情報を動的に交換したり、それぞれのアウトバウンドルーティングテーブルをあとで再アドバタイズできます。

- ソフトリセットによってネイバーからインバウンドアップデートが生成された場合、このリセットはダイナミック インバウンドソフトリセットとといいます。
- ソフトリセットによってネイバーに一連のアップデートが送信された場合、このリセットはアウトバウンドソフトリセットとといいます。

ソフトインバウンドリセットが発生すると、新規インバウンドポリシーが有効になります。ソフトアウトバウンドリセットが発生すると、BGP セッションがリセットされずに、新規ローカルアウトバウンドポリシーが有効になります。アウトバウンドポリシーのリセット中に新しい一連のアップデートが送信されると、新規インバウンドポリシーも有効になる場合があります。

下の表に、ハードリセットとソフトリセットの利点および欠点を示します。

表 1: ハードリセットとソフトリセットの利点および欠点

リセットタイプ	利点	欠点
ハードリセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供された BGP、FIB テーブルのプレフィックス。非推奨
発信ソフトリセット	ルーティングテーブルアップデートが設定、保管されません。	インバウンドルーティングテーブルがリセットされない。

リセットタイプ	利点	欠点
ダイナミック インバウンドソフトリセット	BGPセッションおよびキャッシュがクリアされません。 ルーティングテーブルアップデートを保管する必要がなく、メモリオーバーヘッドが発生しません。	両方のBGPルータでルーティングテーブルをサポートする必要があり、IOS Release 12.1 以降)。

BGP 判断属性

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを1つ選択する必要があります。選択されたパスは BGP ルーティングテーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されている属性値、および BGP で設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィックスに対する 2 つの EBGP パスを学習するとき、最適パスを選択して IP ルーティングテーブルに挿入します。BGP マルチパスサポートが有効で、同じネイバー自律システムから複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスが IP ルーティングテーブルに格納されます。そのあと、パケットスイッチング中に、複数のパス間でパケット単位または宛先単位のロードバランシングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するために属性を評価する順序が決まります。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。BGP ネクストホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as router** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理を無効にするには、ルートマップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 最大の重みのパスを推奨します（シスコ独自のパラメータ）。ウェイト属性はルータにローカルであるため、ルーティングアップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。最大の重みのルートを推奨します。重みを設定するには、アクセスリスト、ルートマップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。
3. ローカルプリファレンス値が最大のルートを推奨します。ローカルプリファレンスはルーティングアップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル初期設定属性のデフォルト値は 100 です。ローカルプリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルートマップを使用します。
4. ローカルルータ上で稼働する BGP から送信されたルートを推奨します。

5. AS パスが最短のルートを推奨します。
6. 送信元タイプが最小のルートを推奨します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック属性が最小のルートを推奨します。MED を設定するには、ルートマップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部 (IBGP) パスより、外部 (EBGP) パスを推奨します。
9. 最も近い IGP ネイバー (最小の IGP メトリック) を通って到達できるルートを推奨します。ルータは、AS 内の最短の内部パス (BGP のネクストホップへの最短パス) を使用し、宛先に到達するためです。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。
 - 最適ルートと目的のルートがともに外部ルートである
 - 最適ルートと目的のルートの両方が、同じネイバー自律システムからのルートである
 - **maximum-paths** が有効である
11. マルチパスが有効でない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック (仮想) アドレスですが、実装に依存することがあります。

ルートマップ

BGP 内でルートマップを使用すると、ルーティング情報を制御、変更したり、ルーティングドメイン間でルートを再配布する条件を定義できます。各ルートマップには、ルートマップを識別する名前 (マップタグ) およびオプションのシーケンス番号が付いています。

BGP フィルタリング

BGP アドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パスフィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセスリストを併用することもできます。**distribute-list** フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティングアップデートのアドバタイズおよび処理の制御」の項を参照してください。

ネイバー単位でルートマップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。ルートマップは、インバウンドアップデートまたはアウトバ

ウンドアップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには **match as-path access-list** ルートマップコマンド、コミュニティに基づくマッチングには **match community-list** ルートマップコマンド、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドが必要です。

BGP フィルタリングのプレフィックス リスト

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセスリストの代わりにプレフィックスリストを使用できます。プレフィックスリストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、コマンドラインインターフェイス (CLI) 設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィックス リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィックス リストに記載されたプレフィックスとルートのプレフィックスが照合されます。一致すると、一致したルートが使用されます。プレフィックスが許可されるか、または拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィックス リストはすべてのプレフィックスを許可します。
- 特定のプレフィックスがプレフィックスリストのどのエン트리とも一致しなかった場合、実質的に拒否されたものと見なされます。
- 指定されたプレフィックスと一致するエントリがプレフィックスリスト内に複数存在する場合は、シーケンス番号が最小であるプレフィックス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成を無効にした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が1の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

BGP コミュニティ フィルタリング

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。この属性によって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。各宛先は複数のコミュニティに属します。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネットコミュニティに属します。コミュニティは、過渡的でグローバルなオプションの属性である、COMMUNITIES 属性 (1 ~ 4294967200 の数値) によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet** : このルートをインターネットコミュニティにアドバタイズします。すべてのルータが所属します。

- **no-export** : EBGp ピアにこのルートをアドバタイズしません。
- **no-advertise** : どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as** : ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配布するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES 属性に、すべての初期ルートの全コミュニティが含まれます。

コミュニティリストを使用すると、ルートマップの **match** 句で使用されるコミュニティグループを作成できます。さらに、アクセスリストの場合と同様、一連のコミュニティリストを作成することもできます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

BGP ネイバーおよびピアグループ

通常、BGP ネイバーの多くは同じアップデートポリシー（同じアウトバウンドルートマップ、配信リスト、フィルタリスト、アップデート送信元など）を使用して設定されます。アップデートポリシーが同じネイバーをピアグループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピアグループを設定するには、ピアグループを作成し、そこにオプションを割り当て、ピアグループメンバーとしてネイバーを追加します。ピアグループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピアグループメンバーは **remote-as**（設定されている場合）、**version**、**update-source**、**out-route-map**、**out-filter-list**、**out-dist-list**、**minimum-advertisement-interval**、**next-hop-self** など、ピアグループの設定オプションをすべて継承します。すべてのピアグループメンバーは、ピアグループに対する変更を継承します。また、アウトバウンドアップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

集約ルート

クラスレスドメイン間ルーティング (CIDR) を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティングテーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配布するか、または BGP ルーティングテーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング ドメイン コンフェデレーション

IBGP メッシュを削減する方法の 1 つは、自律システムを複数のサブ自律システムに分割して、単一の自律システムとして認識される単一の連合にグループ化することです。各自律システムは内部で完全にメッシュ化されていて、同じコンフェデレーション内の他の自律システムとの間には数本の接続があります。異なる自律システム内にあるピアでは EBGp セッションが使用

されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。具体的には、ネクストホップ、MED、およびローカルプリファレンス情報は維持されます。すべての自律システムで単一の IGP を使用できます。

BGP ルート リフレクタ

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから学習されたルートを他の内部ネイバーに送信しません。

ルートリフレクタを使用すると、学習されたルートをネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。IBGP ピアをルートリフレクタに設定すると、その IBGP ピアは IBGP によって学習されたルートを一連の IBGP ネイバーに送信するようになります。ルートリフレクタの内部ピアには、クライアントピアと非クライアントピア（AS 内の他のすべてのルータ）の 2 つのグループがあります。ルートリフレクタは、これらの 2 つのグループ間でルートを反映させます。ルート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。非クライアントピアは相互に完全メッシュ構造にする必要がありますが、クライアントピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

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、ネイバーに応じて、次のいずれかのアクションを実行します。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアントピアにアドバタイズします。
- 非クライアントピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアントピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルートリフレクタが 1 つあり、クラスタはルートリフレクタのルータ ID で識別されます。冗長性を高めて、シングルポイントでの障害を回避するには、クラスタに複数のルートリフレクタを設定する必要があります。このように設定した場合は、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、クラスタ内のすべてのルートリフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。クラスタを処理するすべてのルートリフレクタは完全メッシュ構造にし、一連の同一なクライアントピアおよび非クライアントピアを設定する必要があります。

ルート ダンプニング

ルートフラップダンプニングは、インターネットワーク内でフラッピングルートの伝播を最小化するための BGP 機能です。ルートの状態が使用可能、使用不可能、使用可能、使用不可能という具合に、繰り返し変化する場合、ルートはフラッピングと見なされます。ルートダンプニングが有効の場合は、フラッピングしているルートにペナルティ値が割り当てられます。

ルートの累積ペナルティが、設定された制限値に到達すると、ルートが稼働している場合であっても、BGP はルートのアドバタイズメントを抑制します。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

条件付き BGP ルートの注入

BGP を通じてアドバタイズされるルートは、通常、使用されるルートの数が最小化され、グローバルルーティングテーブルのサイズが小さくなるように集約されます。しかし、共通のルート集約では、より具体的なルーティング情報（より正確であるが、パケットを宛先に転送するために必要なわけではない）がわかりにくくなってしまいます。ルーティングの精度は、共通のルート集約により低下します。これは、トポロジ的に大きな領域に広がる複数のアドレスやホストを表すプレフィックスを1つのルートに正確に反映させることはできないからです。シスコソフトウェアには、プレフィックスを BGP 由来とする方法がいくつか用意されています。BGP 条件付きルート注入機能の導入以前は、既存の方法として、再配布や **network** または **aggregate-address** コマンドが使用されていました。ただし、これらの方法は、より具体的なルーティング情報（開始されるルートと一致するもの）がルーティングテーブルまたは BGP テーブルのいずれかに存在することを前提にしています。

BGP の条件付きルートの注入により、一致するものがなくても、プレフィックスを BGP ルーティングテーブルにすることができます。この機能を使って、管理ポリシーやトラフィックエンジニアリング情報に基づいて、より具体的なルートを生成することができます。これにより、設定された条件が満たされた場合にだけ BGP ルーティングテーブルに注入される、より具体的なルートへのパケットの転送をさらに厳密に制御できるようになります。この機能を有効にすると、条件に応じて、あまり具体的ではないプレフィックスにより具体的なプレフィックスを注入または置き換えることにより、共通のルート集約の精度を高めることができます。元のプレフィックスと同じ、またはより具体的なプレフィックスだけが注入されます。BGP 条件付きルート注入を有効にするには、**bgp inject-map exist-map** コマンドを使用します。また、BGP 条件付きルート注入では、2つのルートマップ（注入マップと存在マップ）を使用して、1つ（または複数）のより具体的なプレフィックスが BGP ルーティングテーブルに注入されます。存在マップは、BGP スピーカーが追跡するプレフィックスを指定します。注入マップは、ローカル BGP テーブルで作成され、このテーブルにインストールされるプレフィックスを定義します。



- (注) 注入マップおよび存在マップで一致となるプレフィックスはルートマップ句ごとに1つだけです。さらにプレフィックスを注入するには、ルートマップ句を追加で設定する必要があります。複数のプレフィックスが使用されている場合は、一致する最初のプレフィックスが使用されます。

BGP Peer テンプレート

構成管理など、ピアグループの制約の一部に対応するため、BGP アップデートグループ コンフィギュレーションをサポートする BGP ピア テンプレートが導入されました。

ピア テンプレートは、ポリシーを共有するネイバーに適用可能なコンフィギュレーション パターンです。ピア テンプレートは再利用が可能で、継承がサポートされているため、ネットワーク オペレータはピア テンプレートを使用して、ポリシーを共有している BGP ネイバーに対して異なるネイバー コンフィギュレーションをグループ化し適用できます。また、ネットワーク オペレータは、別のピア テンプレートからコンフィギュレーションを継承できるというピア テンプレートの機能を使用して、非常に複雑なコンフィギュレーションパターンを定義できるようになります。

ピア テンプレートには 2 種類あります。

- ピア セッション テンプレート。アドレス ファミリ モードおよび NLRI コンフィギュレーション モードすべてに共通する一般的なセッション コマンドのコンフィギュレーションをグループ化し、適用するために使用されます。
- ピア ポリシー テンプレート。特定のアドレスファミリおよび NLRI コンフィギュレーション モードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。

ピア テンプレートにより、柔軟性が高まり、ネイバー コンフィギュレーションの機能が強化されます。また、ピア テンプレートはピアグループ コンフィギュレーションに代わるものを提供し、ピアグループの制約の一部を解決します。ピアテンプレートを使用した BGP ピア デバイスも、自動アップデートグループ コンフィギュレーションの恩恵を受けています。BGP ピアテンプレートが設定され、BGP ダイナミックアップデートピアグループがサポートされたことにより、ネットワーク オペレータは BGP でピアグループを設定する必要がなくなります。また、ネットワークはコンフィギュレーションの柔軟性が高まり、コンバージェンスが高速化されたことによる恩恵を受けます。



- (注) BGP ネイバーを、ピアグループとピアテンプレートの両方と連動するようには設定できません。BGP ネイバーは、1つのピアグループだけに属するように設定するか、またはピアテンプレートからポリシーを継承するように設定します。

ピアポリシーテンプレートには、次の制約事項が適用されます。

- ピアポリシーテンプレートは、直接的、または間接的に、最高 8 個のピアポリシーテンプレートを継承できます。
- BGP ネイバーを、ピアグループとピアテンプレートの両方と連動するようには設定できません。BGP ネイバーは、1つのピアグループだけに属するように設定するか、またはピアテンプレートだけからポリシーを継承するように設定できます。

ピア テンプレートでの継承

継承機能は、ピア テンプレート操作の重要なコンポーネントです。ピア テンプレートでの継承は、たとえば、ファイルとディレクトリツリーなど、一般的なコンピューティングで見られるノードとツリーの構造に似ています。ピア テンプレートは、別のピア テンプレートから直接、または間接的にコンフィギュレーションを継承することができます。直接継承されたピア テンプレートは、構造体のツリーを表します。間接継承されたピア テンプレートはツリーのノードを表します。個々のノードもまた継承をサポートしているため、ブランチを作成して、そこから直接継承されたピアテンプレートすなわちツリーの起点へ連なる全ての間接継承されたピアテンプレートの設定を適用することができます。

この構造により、ネイバーのグループに通常、再適用されるコンフィギュレーション文を繰り返す必要がなくなります。これは、共通のコンフィギュレーション文を一度適用しておく、その後は共通のコンフィギュレーションを持つネイバー グループに適用されるピア グループにより間接継承されるからです。ノードとツリー内部の別々の箇所で重複するコンフィギュレーション文は、ツリーの起点で直接継承したテンプレートによりフィルタ処理されます。直接継承されたテンプレートは、重複する間接継承された文を直接継承された文で上書きします。

継承によりネイバーコンフィギュレーションのスケラビリティと柔軟性がさらに広がり、複数のピアテンプレートコンフィギュレーションを連ねることで、共通のコンフィギュレーション文を継承する単純なコンフィギュレーションを作成したり、共通に継承されるコンフィギュレーションとともに非常に限定的なコンフィギュレーション文を適用する複雑なコンフィギュレーションを作成したりできるようになります。ピアセッションテンプレートおよびピアポリシーテンプレートでの継承の設定についての詳細は、これ以降のセクションで説明します。

BGP ネイバーが継承したピア テンプレートを使用する場合、特定のテンプレートに関連付けられているポリシーを判断するのが難しいことがあります。 **show ip bgptemplate peer-policy** コマンドに、特定のテンプレートに関連付けられているローカルポリシーおよび継承されたポリシーの詳しいコンフィギュレーションを表示するためのキーワード **detail** が追加されました。

ピア セッションテンプレート

ピアセッションテンプレートは、一般的なセッション コマンドのコンフィギュレーションをグループ化し、セッションコンフィギュレーション要素を共有するネイバーのグループに適用するために使用されます。異なるアドレスファミリで設定されているネイバーに共通する一般的なセッション コマンドは、同じピアセッションテンプレートに設定できます。ピアセッションテンプレートの作成と設定は、ピアセッションコンフィギュレーションモードで行います。ピアセッションテンプレートで設定できるのは、一般的なセッション コマンドだけです。次の一般的なセッション コマンドは、ピアセッションテンプレートでサポートされています。

- **description**
- **disable-connected-check**
- **ebgp-multihop**
- **exit peer-session**

- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

一般的なセッションコマンドをピアセッションで一度設定しておく、ピアセッションテンプレートの直接適用、またはピアセッションテンプレートの間接継承によって、多数のネイバーに適用できます。ピアセッションテンプレートのコンフィギュレーションにより、自律システム内のすべてのネイバーに共通に適用される一般的なセッションコマンドのコンフィギュレーションが簡素化されます。

ピアセッションテンプレートは、直接継承と間接継承をサポートします。一度にピアの設定に使用できるピアセッションテンプレートは1つだけです。また、このピアセッションテンプレートは、間接継承されたピアセッションテンプレートを1つだけ含むことができます。



- (注) 1つのピアセッションテンプレートを使って、複数の継承文を設定しようとすると、エラーメッセージが表示されます。

この動作により、BGP ネイバーは1つのセッションテンプレートだけを直接継承し、最高7個のピアセッションテンプレートを間接継承できます。したがって、1つのネイバーに最高8個のピアセッションコンフィギュレーション（直接継承されたピアセッションテンプレートのコンフィギュレーションと最高7個の間接継承されたピアセッションテンプレートのコンフィギュレーション）を適用できます。継承されたピアセッションコンフィギュレーションは、ブランチの最後のノードが最初に評価されて適用され、ツリーの起点で直接適用されたピアセッションテンプレートが最後に適用されます。直接適用されたピアセッションテンプレートは、継承されたピアセッションテンプレートコンフィギュレーションよりも優先されます。継承されたピアセッションテンプレートで重複するコンフィギュレーション文はすべて、直接適用されたピアセッションテンプレートにより上書きされます。したがって、基本セッションコマンドが異なる値で再び適用される場合は、後の値が優先され、間接継承されたテンプレートに設定されていた前の値は上書きされます。次に、この機能を使用した例を示します。

次の例では、一般セッションコマンド **remote-as 1** がピアセッションテンプレート **SESSION-TEMPLATE-ONE** に適用されます。

```
template peer-session SESSION-TEMPLATE-ONE
```

```
remote-as 1
exit peer-session
```

ピアセッションテンプレートは、一般的なセッションコマンドだけをサポートします。特定のアドレスファミリー、またはNLRIコンフィギュレーションモードだけのために設定されるBGPポリシーコンフィギュレーションコマンドは、ピアポリシーテンプレートで設定されません。

ピアポリシーテンプレート

ピアポリシーテンプレートは、特定のアドレスファミリーおよびNLRIコンフィギュレーションモードで適用されるコマンドのコンフィギュレーションをグループ化し、適用するために使用されます。ピアポリシーテンプレートの作成と設定は、ピアポリシーコンフィギュレーションモードで行います。特定のアドレスファミリー専用設定されるBGPポリシーコマンドは、ピアポリシーテンプレートで設定されます。ピアポリシーテンプレートでは、次のBGPポリシーコマンドがサポートされています。

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**
- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**

- **weight**

ピア ポリシー テンプレートは、特定のアドレス ファミリに属するネイバーに設定される BGP ポリシー コマンドの設定に使用されます。ピア セッション テンプレートと同様、ピア ポリシー テンプレートを一度設定しておく、直接適用、または継承を通じて、多数のネイバーにピア ポリシー テンプレートを適用することができます。ピア ポリシー テンプレートの設定により、自律システム内のすべてのネイバーに適用される BGP ポリシー コマンドの設定が簡略化されます。

ピア セッション テンプレートと同様、ピア ポリシー テンプレートは継承をサポートしていません。しかし、多少の違いはあります。直接適用されたピア ポリシー テンプレートは、最大 7 つのピア ポリシー テンプレートから設定を直接的または間接継承できます。したがって、合計 8 つのピア ポリシー テンプレートをネイバーまたはネイバー グループに適用できます。ルート マップと同じように、継承されたピア ポリシー テンプレートにはシーケンス番号が設定されます。また、ルート マップと同じように、継承されたピア ポリシー テンプレートは、最も低いシーケンス番号を持つ **inherit peer-policy** 文が最初に評価され、最も高いシーケンス番号のものが最後に評価されます。ただし、ピア ポリシー テンプレートはルート マップのように折りたたむことはできません。シーケンスはすべて評価されます。異なる値を使って、BGP ポリシー コマンドが再適用された場合は、シーケンス番号の小さいものから順に、前の値がすべて上書きされます。

直接適用されたピア ポリシー テンプレートと、シーケンス番号が最も大きい **inherit peer-policy** 文のプライオリティは常に最も高く、最後に適用されます。これ以降のピア テンプレートに再適用されるコマンドは、必ず、前の値を上書きします。この動作は、個々のポリシー コンフィギュレーション コマンドを繰り返さずとも、共通のポリシー コンフィギュレーションは大規模なネイバー グループに適用し、特定のポリシー コンフィギュレーションは特定のネイバー やネイバー グループだけに適用できるように設計されています。

ピア ポリシー テンプレートは、ポリシー コンフィギュレーション コマンドだけをサポートします。特定のアドレス ファミリ用に設定される BGP ポリシー コンフィギュレーション コマンドは、ピア ポリシー テンプレートで設定されます。

ピア ポリシー テンプレートの設定により、BGP 設定が簡略化され、柔軟性が向上します。特定のポリシーを 1 回設定すれば、何回も参照できます。ピア ポリシーは最大 8 レベルの継承をサポートするため、非常に具体的で複雑な BGP ポリシーも作成できます。

BGP ルート マップ ネクスト ホップ セルフ

BGP ルート マップ ネクスト ホップ セルフ機能は、**bgp next-hop unchanged** と **bgp next-hop unchanged allpaths** の設定を選択的にオーバーライドする方法を提供します。これらの設定はアドレスファミリに対してグローバルに適用されます。ルートによっては、これは適切でない場合があります。たとえば、スタティック ルートは、自身をネクスト ホップとして再配布する必要のある一方で、接続ルート、および内部ボーダー ゲートウェイ プロトコル (IBGP) または外部ボーダー ゲートウェイ プロトコル (EBGP) を介して学習されたルートは、引き続きネクスト ホップを変更せずに再配布する場合があります。

BGP ルートマップネクストホップセルフ機能は、`bgp next-hop unchanged` 設定と `bgp next-hop unchanged allpaths` 設定をオーバーライドする新しい `ip next-hop self` 設定を構成できるように、既存のルートマップインフラストラクチャを変更します。

`ip next-hop self` 設定は、VPNv4 および VPNv6 アドレスファミリにのみ適用されます。BGP 以外のプロトコルによって配布されるルートは影響を受けません。

新しい `bgp route-map priority` 設定を使用すると、`bgp next-hop unchanged` と `bgp next-hop unchanged allpaths` の設定よりもルートマップが優先されることを BGP に通知できます。`bgp route-map priority` 設定は、BGP にのみ影響します。`bgp next-hop unchanged` または `bgp next-hop unchanged allpaths` 設定を構成していない場合、`bgp route-map priority` 設定は効果がありません。

BGP の設定方法

BGP のデフォルト設定

下の表に、BGP のデフォルト設定を示します。

表 2: BGP のデフォルト設定

機能	デフォルト設定
集約アドレス	無効：未定義
AS パス アクセス リスト	未定義
自動サマリー	ディセーブル。
最適パス	<ul style="list-style-type: none"> ルータはルートを選択する場合に <i>as-path</i> を考慮し、外部 BGP 類似ルートは比較しません。 ルータ ID の比較：無効
BGP コミュニティ リスト	<ul style="list-style-type: none"> 番号：未定義。コミュニティ番号を示す特定の値を許可すると、いないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルトされます。 フォーマット：シスコ デフォルト フォーマット (32 ビット番号)
BGP 連合 ID/ピア	<ul style="list-style-type: none"> ID：未設定 ピア：識別なし
BGP 高速外部フォールオーバー	有効
BGP ローカル初期設定	100。指定できる範囲は 0~4294967295 です (大きな値を推奨)。

機能	デフォルト設定
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし
BGP ルート ダンプニング	デフォルトでは、無効です。有効の場合は、次のようになります。 <ul style="list-style-type: none"> • 半減期は 15 分 • 再使用は 750 (10 秒増分) • 抑制は 2000 (10 秒増分) • 最大抑制時間は半減期の 4 倍 (60 分)
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合、バック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元 (プロトコルまたはネットワーク再配布)	ディセーブル。
デフォルト メトリック	自動メトリック変換 (組み込み)
ディスタンス	<ul style="list-style-type: none"> • 外部ルート アドミニストレーティブ ディスタンス : 20 (有効) • 内部ルート アドミニストレーティブ ディスタンス : 200 (有効) • ローカル ルート アドミニストレーティブ ディスタンス : 200 (有効) • 255)
ディストリビュート リスト	<ul style="list-style-type: none"> • 入力 (アップデート中に受信されたネットワークをフィルタリング) • 出力 (アップデート中のネットワークのアドバタイズを抑制)
内部ルート再配布	無効
IP プレフィックス リスト	未定義
Multi Exit Discriminator (MED)	<ul style="list-style-type: none"> • 常に比較 : 無効。異なる自律システム内のネイバーからのパスを比較しません。 • 最適パスの比較 : 無効 • 最悪パスである MED の除外 : 無効 • 決定的な MED 比較 : 無効

機能	デフォルト設定
ネイバー	<ul style="list-style-type: none"> • アドバタイズメントインターバル：外部ピアの場合は30秒、内部ピアの場合は5秒 • ロギング変更：有効 • 条件付きアドバタイズ：無効 • デフォルト送信元：ネイバーに送信されるデフォルトルートはなし • 説明：なし • ディストリビュートリスト：未定義 • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィックスの最大数：制限なし • ネクスト ホップ（BGP ネイバーのネクスト ホップとなるルータ） • パスワード：無効 • ピア グループ：定義なし、割り当てメンバーなし • プレフィックス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア • プライベート AS 番号の削除：無効 • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし。 • シャットダウンまたはソフト再設定：無効 • タイマー：60 秒、ホールドタイム：180 秒 • アップデート送信元：最適ローカル アドレス • バージョン：BGP バージョン 4 • 重み：BGP ピアによって学習されたルート：0、ローカル ルートされたルート：32768
NSF ¹ 認識	<p>無効にされた NSF 認識は、グレースフルリスタートを有効にすることによって、Network Advantage ライセンスを実行するスイッチ上で IPv4 に対して有効です。² 有効な場合、レイヤ 3 スイッチでは、ハードウェアやソフトウェアのアップグレード中に、隣接する NSF 対応ルータからのパケットを転送し続けることが可能です。</p>
ルート リフレクタ	未設定

機能	デフォルト設定
同期化 (BGP および IGP)	無効
テーブル マップ アップデート	無効
タイマー	キープアライブ : 60 秒、ホールドタイム : 180 秒

¹ Nonstop Forwarding

²

BGP ルーティングのイネーブル化

始める前に



(注) EIGRP を有効にするには、スタンドアロンスイッチまたはアクティブスイッチで Network Advantage ライセンスを実行している必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip routing 例 : Device (config)# ip routing	IP ルーティングを有効にします。
ステップ 4	router bgp autonomous-system 例 : Device (config)# router bgp 45000	BGP ルーティング プロセスを有効にして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1~65535 です。64512~65535 は、プライベート AS 番号専用です。

	コマンドまたはアクション	目的
ステップ 5	network <i>network-number</i> [mask <i>network-mask</i>] [route-map <i>route-map-name</i>] 例 : Device(config-router)# network 10.108.0.0	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。
ステップ 6	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i> 例 : Device(config-router)# neighbor 10.108.1.2 remote-as 65200	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 7	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remove-private-as 例 : Device(config-router)# neighbor 172.16.2.33 remove-private-as	(任意) 発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 8	synchronization 例 : Device(config-router)# synchronization	(任意) BGP と IGP の同期化を有効にします。
ステップ 9	auto-summary 例 : Device(config-router)# auto-summary	(任意) 自動ネットワーク サマライズを有効にします。IGP から BGP にサブネットが再配布された場合、ネットワーク ルートだけが BGP テーブルに挿入されます。
ステップ 10	bgp graceful-restart 例 : Device(config-router)# bgp graceful-start	(任意) NSF 認識をスイッチで有効にします。NSF 認識はデフォルトでは無効です。
ステップ 11	end 例 : Device(config-router)# end	特権 EXEC モードに戻ります。
ステップ 12	show ip bgp network <i>network-number</i> 例 :	設定を確認します。

	コマンドまたはアクション	目的
	Device# <code>show ip bgp network 10.108.0.0</code>	
ステップ 13	show ip bgp neighbor 例 : Device# <code>show ip bgp neighbor</code>	NSF 認識 (グレースフル リスタート) がネイバーで有効にされていることを確認します。スイッチおよびネイバーで NSF 認識が有効になっている場合、次のメッセージが表示されます。Graceful Restart Capability: advertised and received スイッチで NSF 認識が有効になっていて、ネイバーで有効になっていない場合、次のメッセージが表示されます。Graceful Restart Capability: advertised
ステップ 14	copy running-config startup-config 例 : Device# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシー変更の管理

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	show ip bgp neighbors 例 : Device# <code>show ip bgp neighbors</code>	ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 <i>Received route refresh capability from peer</i>
ステップ 2	clear ip bgp {* <i>address</i> <i>peer-group-name</i> } 例 : Device# <code>clear ip bgp *</code>	指定された接続上でルーティングテーブルをリセットします。 <ul style="list-style-type: none"> すべての接続をリセットする場合は、アスタリスク (*) を入力します。 特定の接続をリセットする場合は、IP アドレスを入力します。 ピア グループをリセットする場合は、ピア グループ名を入力します。

	コマンドまたはアクション	目的
ステップ 3	clear ip bgp {* <i>address</i> <i>peer-group-name</i> } soft out 例： Device# clear ip bgp * soft out	(任意) 指定された接続上でインバウンドルーティングテーブルをリセットするには、アウトバウンドソフトリセットを実行します。このコマンドは、ルートリフレッシュがサポートされている場合に使用してください。 <ul style="list-style-type: none"> • すべての接続をリセットする場合は、アスタリスク (*) を入力します。 • 特定の接続をリセットする場合は、IP アドレスを入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	show ip bgp 例： Device# show ip bgp	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 5	show ip bgp neighbors 例： Device# show ip bgp neighbors	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	router bgp <i>autonomous-system</i> 例 : Device (config) # router bgp 4500	BGP ルーティング プロセスを有効にして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 4	bgp best-path as-path ignore 例 : Device (config-router) # bgp bestpath as-path ignore	(任意) ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 5	neighbor {<i>ip-address</i> <i>peer-group-name</i>} next-hop-self 例 : Device (config-router) # neighbor 10.108.1.1 next-hop-self	(任意) ネクストホップアドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理を無効にします。
ステップ 6	neighbor {<i>ip-address</i> <i>peer-group-name</i>} weight <i>weight</i> 例 : Device (config-router) # neighbor 172.16.12.1 weight 50	(任意) ネイバー接続に重みを割り当てます。指定できる値は 0 ~ 65535 です。最大の重みのルートを推奨します。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 7	default-metric <i>number</i> 例 : Device (config-router) # default-metric 300	(任意) 推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルータも、この値に設定されます。指定できる範囲は 1 ~ 4294967295 です。最小値を推奨します。
ステップ 8	bgp bestpath med missing-as-worst 例 : Device (config-router) # bgp bestpath med missing-as-worst	(任意) MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 9	bgp always-compare med 例 : Device (config-router) # bgp always-compare-med	(任意) 異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間でだけ比較されます。
ステップ 10	bgp bestpath med confed 例 : Device (config-router) # bgp bestpath med confed	(任意) 連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。

	コマンドまたはアクション	目的
ステップ 11	bgp deterministic med 例 : Device(config-router)# bgp deterministic med	(任意) 同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 12	bgp default local-preference value 例 : Device(config-router)# bgp default local-preference 200	(任意) デフォルトのローカルプリファレンス値を変更します。指定できる範囲は 0 ~ 4294967295 で、デフォルト値は 100 です。最大のローカルプリファレンス値を推奨します。
ステップ 13	maximum-paths number 例 : Device(config-router)# maximum-paths 8	(任意) IP ルーティングテーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティングテーブルに追加されます。指定できる範囲は 1 ~ 16 です。複数の値を指定すると、パス間のロードバランシングが可能になります。スイッチソフトウェアでは最大 32 の等コストルートが許可されていますが、スイッチハードウェアはルートあたり 17 パス以上は使用しません。
ステップ 14	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 15	show ip bgp 例 : Device# show ip bgp	ルーティングテーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 16	show ip bgp neighbors 例 : Device# show ip bgp neighbors	ルーティングテーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 17	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ルート マップによる BGP フィルタリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	route-map map-tag [permit deny] [sequence-number] 例： Device(config)# route-map set-peer-address permit 10	ルートマップを作成し、ルートマップ コンフィギュレーション モードを開始します。
ステップ 4	set ip next-hop ip-address [...ip-address] [peer-address] 例： Device(config)# set ip next-hop 10.1.1.3	（任意）ネクストホップ処理を無効にするようにルートマップを設定します。 <ul style="list-style-type: none"> インバウンドルートマップの場合は、一致するルートのネクストホップをネイバーピアアドレスに設定し、サードパーティのネクストホップを上書きします。 BGP ピアのアウトバウンドルートマップの場合は、ネクストホップをローカルルータのピアアドレスに設定して、ネクストホップ計算を無効にします。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show route-map [map-name] 例： Device# show route-map	設定を確認するため、設定されたすべてのルートマップ、または指定されたルートマップだけを表示します。

	コマンドまたはアクション	目的
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ネイバーによる BGP フィルタリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp autonomous-system 例 : Device(config)# router bgp 109	BGP ルーティングプロセスを有効にして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor {ip-address peer-group name} distribute-list {access-list-number name} {in out} 例 : Device(config-router)# neighbor 172.16.4.1 distribute-list 39 in	(任意) アクセスリストの指定に従って、ネイバーに対して送受信される BGP ルーティングアップデートをフィルタリングします。 (注) neighbor prefix-list ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 5	neighbor {ip-address peer-group name} route-map map-tag {in out} 例 : Device(config-router)# neighbor 172.16.70.24 route-map internal-map in	(任意) ルート マップを適用し、着信または発信ルートをフィルタリングします。

	コマンドまたはアクション	目的
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show ip bgp neighbors 例： Device# show ip bgp neighbors	設定を確認します。
ステップ 8	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

アクセスリストおよびネイバーによる BGP フィルタリングの設定

BGP 自律システムパスに基づいて着信および発信の両方のアップデートにアクセスリストフィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現を使用するアクセスリストです。この方法を使用するには、自律システムパスのアクセスリストを定義し、特定のネイバーとの間のアップデートに適用します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip as-path access-list access-list-number {permit deny} as-regular-expressions 例： Device(config)# ip as-path access-list 1 deny _65535_	BGP-related アクセスリストを定義します。

	コマンドまたはアクション	目的
ステップ 4	router bgp <i>autonomous-system</i> 例： Device(config)# router bgp 110	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 5	neighbor { <i>ip-address</i> <i>peer-group name</i> } filter-list { <i>access-list-number</i> <i>name</i> } { in out weight weight } 例： Device(config-router)# neighbor 172.16.1.1 filter-list 1 out	アクセスリストに基づいて、BGP フィルタを確立します。
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show ip bgp neighbors [<i>paths regular-expression</i>] 例： Device# show ip bgp neighbors	設定を確認します。
ステップ 8	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

BGP フィルタリング用のプレフィックス リストの設定

コンフィギュレーションエントリを削除する場合は、シーケンス番号を指定する必要はありません。**Show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィックス リストを使用する場合は、あらかじめプレフィックス リストを設定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip prefix-list list-name [seq seq-value] deny permit network/len [ge ge-value] [le le-value] 例 : Device(config)# ip prefix-list BLUE permit 172.16.1.0/24	一致条件に合わせてアクセスを deny または permit するプレフィックスリストを作成します。シーケンス番号を指定することもできます。少なくとも 1 つの permit または deny 句を入力する必要があります。 <ul style="list-style-type: none"> • <i>network/len</i> は、ネットワーク番号およびネットワーク マスクの長さ (ビット単位) です。 • (任意) ge および le の値は、一致させるプレフィックス長を指定します。指定する <i>ge-value</i> および <i>le-value</i> は次の条件を満たしている必要があります。 $len < ge-value < le-value < 32$
ステップ 4	ip prefix-list list-name seq seq-value deny permit network/len [ge ge-value] [le le-value] 例 : Device(config)# ip prefix-list BLUE seq 10 permit 172.24.1.0/24	(任意) プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip prefix list [detail summary] name [network/len] [seq seq-num] [longer] [first-match] 例 : Device# show ip prefix list summary test	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

BGP コミュニティ フィルタリングの設定

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip community-list community-list-number {permit | deny} community-number**
4. **router bgp autonomous-system**
5. **neighbor {ip-address | peer-group name} send-community**
6. **set comm-list list-num delete**
7. **exit**
8. **ip bgp-community new-format**
9. **end**
10. **show ip bgp community**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip community-list community-list-number {permit deny} community-number 例： Device(config)# ip community-list 1 permit 50000:10	コミュニティ リストを作成し、番号を割り当てます。 • <i>community-list-number</i> は 1 ~ 99 の整数です。この値は、コミュニティの 1 つ以上の許可または拒否グループを識別します。 • <i>community-number</i> は、 set community ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 4	router bgp autonomous-system 例：	BGP ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device(config)# router bgp 108	
ステップ 5	neighbor {ip-address peer-group name} send-community 例 : Device(config-router)# neighbor 172.16.70.23 send-community	この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 6	set comm-list list-num delete 例 : Device(config-router)# set comm-list 500 delete	(任意) ルート マップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 7	exit 例 : Device(config-router)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	ip bgp-community new-format 例 : Device(config)# ip bgp-community new format	(任意) AA:NN の形式で、BGP コミュニティを表示、解析します。 BGP コミュニティは、2つの部分からなる2バイト長形式で表示されます。シスコのデフォルトのコミュニティ形式は、NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 9	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 10	show ip bgp community 例 : Device# show ip bgp community	設定を確認します。
ステップ 11	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピアグループの設定

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示す ルータ コンフィギュレーション コマンドのいずれかを指定します。ピアグループにオプションを割り当てるには、ピアグループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用して、コンフィギュレーション情報を削除せずに、BGP ピア、またはピアグループを削除することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp autonomous-system	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor peer-group-name peer-group	BGP ピアグループを作成します。
ステップ 5	neighbor ip-address peer-group peer-group-name	BGP ネイバーをピアグループのメンバにします。
ステップ 6	neighbor {ip-address peer-group-name} remote-as number	BGP ネイバーを指定します。 remote-as number を使用してピアグループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピアグループを作成します。指定できる範囲は 1 ~ 65535 です。
ステップ 7	neighbor {ip-address peer-group-name} description text	(任意) ネイバーに説明を関連付けます。
ステップ 8	neighbor {ip-address peer-group-name} default-originate [route-map map-name]	(任意) BGP スピーカー（ローカル ルータ）にネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、このルートがデフォルトルートとして使用されるようにします。
ステップ 9	neighbor {ip-address peer-group-name} send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。

	コマンドまたはアクション	目的
ステップ 10	neighbor { <i>ip-address</i> <i>peer-group-name</i> } update-source <i>interface</i>	(任意) 内部 BGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 11	neighbor { <i>ip-address</i> <i>peer-group-name</i> } ebgp-multihop	(任意) ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルトルート (0.0.0.0) の場合、マルチホップ セッションは確立されません。
ステップ 12	neighbor { <i>ip-address</i> <i>peer-group-name</i> } local-as <i>number</i>	(任意) ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ~ 65535 です。
ステップ 13	neighbor { <i>ip-address</i> <i>peer-group-name</i> } advertisement-interval <i>seconds</i>	(任意) BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 14	neighbor { <i>ip-address</i> <i>peer-group-name</i> } maximum-prefix <i>maximum</i> [<i>threshold</i>]	(任意) ネイバーから受信できるプレフィックス数を制御します。指定できる範囲は 1 ~ 4294967295 です。 <i>threshold</i> (任意) は、警告メッセージが生成される基準となる最大値 (パーセンテージ) です。デフォルトは 75% です。
ステップ 15	neighbor { <i>ip-address</i> <i>peer-group-name</i> } next-hop-self	(任意) ネイバー宛ての BGP アップデートに関して、ネクストホップでの処理を無効にします。
ステップ 16	neighbor { <i>ip-address</i> <i>peer-group-name</i> } password <i>string</i>	(任意) TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 17	neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>map-name</i> { in out }	(任意) 着信または発信ルートにルート マップを適用します。
ステップ 18	neighbor { <i>ip-address</i> <i>peer-group-name</i> } send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 19	neighbor { <i>ip-address</i> <i>peer-group-name</i> } timers <i>keepalive holdtime</i>	(任意) ネイバーまたはピアグループ用のタイマーを設定します。 <ul style="list-style-type: none"> • <i>keepalive</i> インターバルは、キープアライブメッセージがピアに送信される間隔です。指定できる範囲は 1 ~ 4294967295 秒です。デフォルト値は 60 秒です。 • <i>holdtime</i> は、キープアライブメッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲

	コマンドまたはアクション	目的
		は 1 ~ 4294967295 秒です。デフォルト値は 180 秒です。
ステップ 20	neighbor { <i>ip-address</i> <i>peer-group-name</i> } weight <i>weight</i>	(任意) ネイバーからのすべてのルートに関する重みを指定します。
ステップ 21	neighbor { <i>ip-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-number</i> <i>name</i> } { in out }	(任意) アクセスリストの指定に従って、ネイバーに対して送受信される BGP ルーティングアップデートをフィルタリングします。
ステップ 22	neighbor { <i>ip-address</i> <i>peer-group-name</i> } filter-list <i>access-list-number</i> { in out weight <i>weight</i> }	(任意) BGP フィルタを確立します。
ステップ 23	neighbor { <i>ip-address</i> <i>peer-group-name</i> } version <i>value</i>	(任意) ネイバーと通信するとき使用する BGP バージョンを指定します。
ステップ 24	neighbor { <i>ip-address</i> <i>peer-group-name</i> } soft-reconfiguration inbound	(任意) 受信したアップデートのストアを開始するようにソフトウェアを設定します。
ステップ 25	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 26	show ip bgp neighbors	設定を確認します。
ステップ 27	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ルーティング テーブルでの集約アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	router bgp <i>autonomous-system</i> 例 : Device(config)# router bgp 106	BGP ルータ コンフィギュレーションモードを開始します。
ステップ 4	aggregate-address <i>address mask</i> 例 : Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートはASからのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。
ステップ 5	aggregate-address <i>address mask as-set</i> 例 : Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set	(任意) AS 設定パス情報を生成します。このコマンドは、この前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。
ステップ 6	aggregate-address <i>address-mask summary-only</i> 例 : Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only	(任意) サマリー アドレスだけをアドバタイズします。
ステップ 7	aggregate-address <i>address mask suppress-map map-name</i> 例 : Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 suppress-map map1	(任意) 選択された、より具体的なルートを抑制します。
ステップ 8	aggregate-address <i>address mask advertise-map map-name</i> 例 : Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 advertise-map map2	(任意) ルート マップによって指定された設定に基づいて集約を生成します。
ステップ 9	aggregate-address <i>address mask attribute-map map-name</i> 例 :	(任意) ルート マップで指定された属性を持つ集約を生成します。

	コマンドまたはアクション	目的
	Device(config-router)# aggregate-address 10.0.0.0 255.0.0.0 attribute-map map3	
ステップ 10	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 11	show ip bgp neighbors [advertised-routes] 例： Device# show ip bgp neighbors	設定を確認します。
ステップ 12	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティングドメイン連合の設定

自律システムのグループの自律システム番号として機能する連合 ID を指定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system</i> 例： Device(config)# router bgp 100	BGP ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	bgp confederation identifier <i>autonomous-system</i> 例 : Device (config)# bgp confederation identifier 50007	BGP 連合 ID を設定します。
ステップ 5	bgp confederation peers <i>autonomous-system</i> [<i>autonomous-system ...</i>] 例 : Device (config)# bgp confederation peers 51000 51001 51002	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 6	end 例 : Device (config)# end	特権 EXEC モードに戻ります。
ステップ 7	show ip bgp neighbor 例 : Device# show ip bgp neighbor	設定を確認します。
ステップ 8	show ip bgp network 例 : Device# show ip bgp network	設定を確認します。
ステップ 9	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

BGP ルート リフレクタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system</i> 例： Device(config)# router bgp 101	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor {<i>ip-address</i> <i>peer-group-name</i>} route-reflector-client 例： Device(config-router)# neighbor 172.16.70.24 route-reflector-client	ローカル ルータを BGP ルートリフレクタとして、指定されたネイバーをクライアントとして、それぞれ設定します。
ステップ 5	bgp cluster-id <i>cluster-id</i> 例： Device(config-router)# bgp cluster-id 10.0.1.2	(任意) クラスタに複数のルートリフレクタが存在する場合、クラスタ ID を設定します。
ステップ 6	no bgp client-to-client reflection 例： Device(config-router)# no bgp client-to-client reflection	(任意) クライアント間のルート反映を無効にします。デフォルトでは、ルートリフレクタクライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルートリフレクタはルートをクライアントに反映させる必要がありません。
ステップ 7	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show ip bgp 例： Device# show ip bgp	設定を確認します。送信元 ID およびクラスタリスト属性を表示します。
ステップ 9	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ルート ダンプニングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp autonomous-system 例： Device(config)# router bgp 100	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	bgp dampening 例： Device(config-router)# bgp dampening	BGP ルート ダンプニングを有効にします。
ステップ 5	bgp dampening half-life reuse suppress max-suppress [route-map map] 例： Device(config-router)# bgp dampening 30 1500 10000 120	(任意) ルート ダンプニング係数のデフォルト値を変更します。
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show ip bgp flap-statistics [{ regexp regexp } { filter-list list } { address mask [longer-prefix] }] 例： Device# show ip bgp flap-statistics	(任意) フラッピングしているすべてのパスのフラップを監視します。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 8	show ip bgp dampened-paths 例：	(任意) 抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。

	コマンドまたはアクション	目的
	Device# show pi bgp dampened-paths	
ステップ 9	clear ip bgp flap-statistics [{ regexp <i>regexp</i> } { filter-list <i>list</i> } { address mask [longer-prefix] } 例 : Device# clear ip bgp flap-statistics	(任意) BGP フラップ統計情報を消去して、ルートがダンプニングされる可能性を小さくします。
ステップ 10	clear ip bgp dampening 例 : Device# clear ip bgp dampening	(任意) ルートダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 11	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルートの条件付き注入

標準のルート集約を通じて選択された具体性にかけるプレフィックスではなく、より具体的なプレフィックスを BGP ルーティング テーブルに注入するには、この作業を実行します。より具体的なプレフィックスを使用すると、集約されたルートを使う場合よりも、よりきめ細かなトラフィック エンジニアリングや管理制御を行うことができます。

始める前に

この作業は、BGP ピアに対して、IGP がすでに設定されていることを前提にしています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**]
5. **exit**
6. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
7. **match ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] } **prefix-list** *prefix-list-name* [*prefix-list-name...*]
8. **match ip route-source** { *access-list-number* | *access-list-name* } [*access-list-number...* | *access-list-name...*]
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]

11. **set ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
12. **set community** {*community-number* [**additive**] [*well-known-community*] | **none**}
13. **exit**
14. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
15. 作成される各プレフィックス リストについて、ステップ 14 を繰り返します。
16. **exit**
17. **show ip bgp injected-paths**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 40000	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	bgp inject-map <i>inject-map-name</i> exist-map <i>exist-map-name</i> [copy-attributes] 例： Device(config-router)# bgp inject-map ORIGINATE exist-map LEARNED_PATH	条件付きルート注入のために、注入マップと存在マップを指定します。 <ul style="list-style-type: none">• 注入したルートが集約ルートの属性を継承することを指定するには、copy-attributes キーワードを使用します。
ステップ 5	exit 例： Device(config-router)# exit	ルータ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>] 例： Device(config)# route-map LEARNED_PATH permit 10	ルートマップを設定し、ルートマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	<p>match ip address {<i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] <i>access-list-name</i> [<i>access-list-number...</i> <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]}</p> <p>例 :</p> <pre>Device(config-route-map)# match ip address prefix-list SOURCE</pre>	<p>より具体的なルートの注入先となる集約ルートを指定します。</p> <ul style="list-style-type: none"> この例では、ルートのソースの再配布に、プレフィックスリスト SOURCE が使用されています。
ステップ 8	<p>match ip route-source {<i>access-list-number</i> <i>access-list-name</i>} [<i>access-list-number...</i> <i>access-list-name...</i>]</p> <p>例 :</p> <pre>Device(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE</pre>	<p>ルートのソースを再配布するための一致条件を指定します。</p> <ul style="list-style-type: none"> この例では、ルートのソースの再配布に、プレフィックスリスト ROUTE_SOURCE が使用されています。 <p>(注) ルートソースは、neighbor remote-as コマンドで設定されたネイバーアドレスです。より具体的なルートの注入先となし注入する集約ルートを指定します。</p>
ステップ 9	<p>exit</p> <p>例 :</p> <pre>Device(config-route-map)# exit</pre>	<p>ルートマップコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードを開始します。</p>
ステップ 10	<p>route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>]</p> <p>例 :</p> <pre>Device(config)# route-map ORIGINATE permit 10</pre>	<p>ルートマップを設定し、ルートマップコンフィギュレーションモードを開始します。</p>
ステップ 11	<p>set ip address {<i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] <i>access-list-name</i> [<i>access-list-number...</i> <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]}</p> <p>例 :</p> <pre>Device(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES</pre>	<p>注入されるルートを指定します。</p> <p>この例では、ルートのソースの再配布に、プレフィックスリスト <i>originated_routes</i> が使用されています。</p>
ステップ 12	<p>set community {<i>community-number</i> [additive] [<i>well-known-community</i>] none}</p> <p>例 :</p> <pre>Device(config-route-map)# set community 14616:555 additive</pre>	<p>注入されたルートの BGP コミュニティ属性を設定します。</p>

	コマンドまたはアクション	目的
ステップ 13	exit 例： Device (config-route-map) # exit	ルートマップコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードを開始します。
ステップ 14	ip prefix-list list-name [seq seq-value] {deny network/length permit network/length} [ge ge-value] [le le-value] 例： Device (config) # ip prefix-list SOURCE permit 10.1.1.0/24	プレフィックスリストを設定します。 この例では、プレフィックスリスト SOURCE は、ネットワーク 10.1.1.0/24 からのルートを許可するように設定されています。
ステップ 15	作成される各プレフィックスリストについて、ステップ 14 を繰り返します。	--
ステップ 16	exit 例： Device (config) # exit	グローバルコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 17	show ip bgp injected-paths 例： Device# show ip bgp injected-paths	(任意) 注入されたパスに関する情報を表示します。

ピアセッションテンプレートの設定

次の作業では、ピアセッションテンプレートを作成し、設定します。

基本的なピアセッションテンプレートの設定

一般的な BGP ルーティングセッションコマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピアセッションテンプレートを作成するには、この作業を実行します。



(注) ステップ 5 と 6 のコマンドは任意で、サポートされている一般的なセッションコマンドのいずれとでも置き換えが可能です。



(注) ピアセッションテンプレートには、次の制約事項が適用されます。

- ピアセッションテンプレートが直接継承できるセッションテンプレートは1つだけです。また、継承されたセッションテンプレートはそれぞれ、間接継承されたセッションテンプレートを1つ含むことができます。したがって、ネイバー、またはネイバーグループの設定には、直接適用されたピアセッションテンプレートを1個だけと、間接継承されたピアセッションテンプレートを7個使用できます。
- BGP ネイバーを、ピアグループとピアテンプレートの両方と連動するには設定できません。BGP ネイバーは、1つのピアグループだけに属するように設定するか、またはピアテンプレートだけからポリシーを継承するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **remote-as** *autonomous-system-number*
6. **timers** *keepalive-interval hold-time*
7. **end**
8. **show ip bgp template peer-session** [*session-template-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 101	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
ステップ 4	template peer-session <i>session-template-name</i> 例 : Device(config-router)# template peer-session INTERNAL-BGP	セッションテンプレート コンフィギュレーションモードを開始して、ピアセッションテンプレートを作成します。
ステップ 5	remote-as <i>autonomous-system-number</i> 例 : Device(config-router-stmp)# remote-as 202	(任意) 指定された自律システムでリモート ネイバーとのピアリングを設定します。 (注) ここでは、サポートされている一般セッションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 6	timers <i>keepalive-interval hold-time</i> 例 : Device(config-router-stmp)# timers 30 300	(任意) BGP キープアライブとホールドタイマーを設定します。 ホールドタイムは、少なくともキープアライブ タイムの 2 倍の長さが必要です。 (注) ここでは、サポートされている一般セッションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。
ステップ 7	end 例 : Device(config-router)# end	セッションテンプレート コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 8	show ip bgp template peer-session [<i>session-template-name</i>] 例 : Device# show ip bgp template peer-session	ローカルに設定されたピアセッションテンプレートを表示します。 <i>session-template-name</i> 引数を使用して、ピアポリシーテンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

inherit peer-session コマンドを使用したピアセッションテンプレートの継承の設定

この作業は、**inherit peer-session** コマンドを使用して、ピアセッションテンプレートの継承を設定します。これは、ピアセッションテンプレートを作成、設定し、別のピアセッションテンプレートからコンフィギュレーションを継承できるようにします。



(注) ステップ5と6のコマンドは任意で、サポートされている一般的なセッションコマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **description** *text-string*
6. **update-source** *interface-type interface-number*
7. **inherit peer-session** *session-template-name*
8. **end**
9. **show ip bgp template peer-session** [*session-template-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 101	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	template peer-session <i>session-template-name</i> 例： Device(config-router)# template peer-session CORE1	セッションテンプレート コンフィギュレーションモードを開始して、ピアセッションテンプレートを作成します。
ステップ 5	description <i>text-string</i> 例： Device(config-router-stmp)# description CORE-123	(任意) 説明を設定します。 text-string には最大 80 文字を使用できます。

	コマンドまたはアクション	目的
		<p>(注) ここでは、サポートされている一般セッションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。</p>
<p>ステップ 6</p>	<p>update-source <i>interface-type interface-number</i></p> <p>例 :</p> <pre>Device(config-router-stmp)# update-source loopback 1</pre>	<p>(任意) ルーティングテーブルアップデートを受信するための特定のソース、またはインターフェイスを選択するようにルータを設定します。</p> <p>この例では、ループバックインターフェイスを使用します。このコンフィギュレーションの利点は、ループバックインターフェイスはフラッピングしているインターフェイスの影響を受けにくいところにあります。</p> <p>(注) ここでは、サポートされている一般セッションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「制限事項」の項を参照してください。</p>
<p>ステップ 7</p>	<p>inherit peer-session <i>session-template-name</i></p> <p>例 :</p> <pre>Device(config-router-stmp)# inherit peer-session INTERNAL-BGP</pre>	<p>別のピアセッションテンプレートのコンフィギュレーションを継承するように、このピアセッションテンプレートを設定します。</p> <p>この例では、INTERNAL-BGPからコンフィギュレーションを継承するようにピアセッションテンプレートを設定しています。このテンプレートはネイバーに適用可能で、コンフィギュレーション INTERNAL-BGP は間接的に適用されます。その他のピアセッションテンプレートは直接適用できません。ただし、直接継承されたテンプレートは最高7個の間接継承されたピアセッションテンプレートを持つことができます。</p>
<p>ステップ 8</p>	<p>end</p> <p>例 :</p> <pre>Device(config-router)# end</pre>	<p>セッションテンプレートコンフィギュレーションモードを終了して、特権 EXEC モードを開始します。</p>
<p>ステップ 9</p>	<p>show ip bgp template peer-session [<i>session-template-name</i>]</p> <p>例 :</p> <pre>Device# show ip bgp template peer-session</pre>	<p>ローカルに設定されたピアセッションテンプレートを表示します。</p> <p>オプションの <i>session-template-name</i> 引数を使用して、ピアポリシーテンプレートが1つだけ表示される</p>

	コマンドまたはアクション	目的
		ように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

neighbor inherit peer-session コマンドを使用したピアセッションテンプレートの継承の設定

この作業では、**neighbor inherit peer-session** コマンドを使用して、ピアセッションテンプレートをネイバーに送信し、指定されたピアセッションテンプレートからコンフィギュレーションを継承させるようにデバイスを設定します。次の手順に従って、ピアセッションテンプレートコンフィギュレーションをネイバーに送信し、継承させます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **inherit peer-session** *session-template-name*
6. **end**
7. **show ip bgp template peer-session** [*session-template-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 101	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	neighbor <i>ip-address</i> remote-as <i>autonomous-system-number</i> 例：	指定されたネイバーを使ってピアリングセッションを設定します。 手順 5 の neighbor inherit 文を動作させるには、 remote-as 文を明示的に使用する必要があります。

	コマンドまたはアクション	目的
	Device(config-router)# neighbor 172.16.0.1 remote-as 202	ピアリングが設定されていない場合、手順 5 で指定されたネイバーはセッションテンプレートを受け付けません。
ステップ 5	neighbor ip-address inherit peer-session session-template-name 例 : Device(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1	<p>ネイバーがコンフィギュレーションを継承できるように、このネイバーにピアセッションテンプレートを送信します。</p> <p>この例では、ピアセッションテンプレート CORE1 を 172.16.0.1 ネイバーに送信し、継承させるようにデバイスを設定しています。このテンプレートはネイバーに適用できます。また、別のピアセッションテンプレートが CORE1 で間接継承された場合、間接継承されたコンフィギュレーションも適用されます。その他のピアセッションテンプレートは直接適用できません。ただし、直接継承されたテンプレートも、さらに最高 7 個の間接継承されたピアセッションテンプレートを継承することができます。</p>
ステップ 6	end 例 : Device(config-router)# end	ルータコンフィギュレーションモードを終了して、特権 EXEC モードを開始します。
ステップ 7	show ip bgp template peer-session [session-template-name] 例 : Device# show ip bgp template peer-session	<p>ローカルに設定されたピアセッションテンプレートを表示します。</p> <p>オプションの <i>session-template-name</i> 引数を使用して、ピアポリシーテンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。</p>

ピアポリシー テンプレートの設定

次の作業では、ピアポリシーテンプレートを作成し、設定します。

基本的なピアポリシー テンプレートの設定

BGP ポリシー コンフィギュレーション コマンドを使って、この次に説明する 2 つの作業のうち 1 つを使用して、多数のネイバーに適用できる基本的なピアポリシー テンプレートを作成するには、この作業を実行します。



(注) ステップ5～7のコマンドは任意で、サポートされているBGPポリシーコンフィギュレーションコマンドのいずれとでも置き換えが可能です。



(注) ピアポリシーテンプレートには、次の制約事項が適用されます。

- ピアポリシーテンプレートは、直接的、または間接的に、最高8個のピアポリシーテンプレートを継承できます。
- BGPネイバーを、ピアグループとピアテンプレートの両方と連動するようには設定できません。BGPネイバーは、1つのピアグループだけに属するように設定するか、またはピアテンプレートだけからポリシーを継承するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval* | **warning-only**]
6. **weight** *weight-value*
7. **prefix-list** *prefix-list-name* {**in** | **out**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 45000	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
ステップ 4	template peer-policy <i>policy-template-name</i> 例 : Device (config-router) # template peer-policy GLOBAL	ポリシーテンプレートコンフィギュレーションモードを開始し、ピアポリシーテンプレートを作成します。
ステップ 5	maximum-prefix <i>prefix-limit</i> [<i>threshold</i>] [restart <i>restart-interval</i> warning-only] 例 : Device (config-router-ptmp) # maximum-prefix 10000	(任意) このピアがネイバーから受け入れるプレフィックスの最大数を設定します。 (注) ここでは、サポートされている BGP ポリシーコンフィギュレーションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピアポリシーテンプレート」の項を参照してください。
ステップ 6	weight <i>weight-value</i> 例 : Device (config-router-ptmp) # weight 300	(任意) このネイバーから送信されるルートへのデフォルトの重みを設定します。 (注) ここでは、サポートされている BGP ポリシーコンフィギュレーションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピアポリシーテンプレート」の項を参照してください。
ステップ 7	prefix-list <i>prefix-list-name</i> { in out } 例 : Device (config-router-ptmp) # prefix-list NO-MARKETING in	(任意) ルータにより受信、またはルータから送信されるプレフィックスをフィルタします。 この例のプレフィックスリストは、インバウンド内部アドレスをフィルタします。 (注) ここでは、サポートされている BGP ポリシーコンフィギュレーションコマンドならどれでも使用できます。サポートされているコマンドの一覧については、「ピアポリシーテンプレート」の項を参照してください。
ステップ 8	end 例 : Device (config-router-ptmp) # end	ポリシーテンプレートコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業は、**inherit peer-policy** コマンドを使用して、ピア ポリシー テンプレートの継承を設定します。これは、ピア ポリシー テンプレートを作成、設定し、別のピア ポリシー テンプレートからコンフィギュレーションを継承できるようにします。



(注) ステップ5と6のコマンドは任意で、サポートされているBGPポリシーコンフィギュレーションコマンドのいずれとでも置き換えが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **route-map** *map-name* {**in**|**out**}
6. **inherit peer-policy** *policy-template-name* *sequence-number*
7. **end**
8. **show ip bgp template peer-policy** [*policy-template-name*[**detail**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device(config)# router bgp 45000	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	template peer-policy <i>policy-template-name</i> 例： Device(config-router)# template peer-policy NETWORK1	ポリシー テンプレート コンフィギュレーション モードを開始し、ピア ポリシー テンプレートを作成します。

	コマンドまたはアクション	目的
ステップ 5	route-map <i>map-name</i> { in out } 例 : Device(config-router-ptmp) # route-map ROUTE in	(任意) 指定されたルート マップをインバウンド ルート、またはアウトバウンド ルートに適用します。 (注) ここでは、サポートされている BGP ポリシー コンフィギュレーション コマンドならどれでも使用できます。
ステップ 6	inherit peer-policy <i>policy-template-name</i> <i>sequence-number</i> 例 : Device(config-router-ptmp) # inherit peer-policy GLOBAL 10	別のピアポリシーテンプレートのコンフィギュレーションを継承するように、このピアポリシー テンプレートを設定します。 <ul style="list-style-type: none"> • <i>sequence-number</i> 引数は、ピア ポリシー テンプレートの評価順序を設定します。ルートマップのシーケンス番号と同様、最も小さいシーケンス番号が最初に評価されます。 • この例では、GLOBAL からコンフィギュレーションを継承するようにピアポリシーテンプレートを設定しています。これらの手順で作成されたテンプレートをネイバーに適用すると、コンフィギュレーション GLOBAL も間接継承され、適用されます。GLOBAL からはさらに最高 6 個のピアポリシーテンプレートが間接継承され、合計 8 個のピアポリシーテンプレートが直接適用、および間接継承されます。 • 他のテンプレートで、これより小さいシーケンス番号が設定されていないならば、この例のこのテンプレートが最初に評価されます。
ステップ 7	end 例 : Device(config-router-ptmp) # end	ポリシーテンプレートコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 8	show ip bgp template peer-policy [<i>policy-template-name</i>] [detail] 例 : Device# show ip bgp template peer-policy NETWORK1 detail	ローカルに設定されたピアポリシーテンプレートを表示します。 <ul style="list-style-type: none"> • <i>policy-template-name</i> 引数を使用して、ピアポリシーテンプレートが 1 つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 詳細なポリシー情報を表示するには、detail キーワードを使用します。

例

次の例は、**show ip bgp template peer-policy** コマンドに **detail** キーワードを付けた場合の出力で、NETWORK1 というポリシーの詳細が表示されています。この例の出力からは、GLOBAL テンプレートが継承されたことがわかります。ルートマップおよびプレフィックス リスト コンフィギュレーションの詳細も表示されています。

```
Device# show ip bgp template peer-policy NETWORK1 detail
Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
  seq 5 permit 10.1.1.0/24
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
  seq 5 deny 10.2.2.0/24
```

neighbor inherit peer-policy コマンドを使用したピア ポリシー テンプレートの継承の設定

この作業では、**neighbor inherit peer-policy** コマンドを使用して、ピアポリシーテンプレートをネイバーに送信し、継承させるようにデバイスを設定します。次の手順に従って、ピアポリシー テンプレート コンフィギュレーションをネイバーに送信し、継承させます。

BGP ネイバーが複数レベルのピア テンプレートを使用する場合、ネイバーに適用されているポリシーを判断するのが難しいことがあります。**show ip bgp neighbors** コマンドの **policy** および **detail** キーワードは、指定されたネイバーに継承されたポリシーおよび直接設定されたポリシーを表示します。

手順の概要

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*
7. **end**
8. **show ip bgp neighbors** [*ip-address* [**policy** [**detail**]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp <i>autonomous-system-number</i> 例： Device (config)# router bgp 45000	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	neighbor <i>ip-address</i> remote-as <i>autonomous-system-number</i> 例： Device (config-router)# neighbor 192.168.1.2 remote-as 40000	指定されたネイバーを使ってピアリングセッションを設定します。 <ul style="list-style-type: none"> 手順 6 の neighbor inherit 文を動作させるには、remote-as 文を明示的に使用する必要があります。ピアリングが設定されていない場合、手順 6 で指定されたネイバーはセッション テンプレートを受け付けません。
ステップ 5	address-family ipv4 [multicast unicast vrf <i>vrf-name</i>] 例： Device (config-router)# address-family ipv4 unicast	アドレスファミリー固有のコマンド コンフィギュレーションを使用するようにネイバーを設定するために、アドレスファミリー コンフィギュレーション モードを開始します。
ステップ 6	neighbor <i>ip-address</i> inherit peer-policy <i>policy-template-name</i> 例： Device (config-router-af)# neighbor 192.168.1.2 inherit peer-policy GLOBAL	ネイバーが設定を継承できるように、ピアポリシー テンプレートをこのネイバーに送信します。 この例では、ピアポリシー テンプレート GLOBAL を 192.168.1.2 ネイバーに送信し、継承させるようにルータを設定しています。このテンプレートはネイバーに適用できます。また、別のピアポリシー テンプレートが GLOBAL から間接継承された場合、

	コマンドまたはアクション	目的
		間接継承されたコンフィギュレーションも適用されます。GLOBAL からは、さらに最高7個のピアポリシー テンプレートを間接継承できます。
ステップ 7	end 例： Device(config-router-af)# end	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	show ip bgp neighbors [ip-address[policy [detail]]] 例： Device# show ip bgp neighbors 192.168.1.2 policy	ローカルに設定されたピアポリシー テンプレートを表示します。 <ul style="list-style-type: none"> • <i>policy-template-name</i> 引数を使用して、ピアポリシー テンプレートが1つだけ表示されるように、出力をフィルタ処理できます。また、このコマンドは、標準出力修飾子すべてをサポートしています。 • このネイバーに適用されているポリシーをアドレスファミリごとに表示するには、policy キーワードを使用します。 • 詳細なポリシー情報を表示するには、detail キーワードを使用します。

例

次の出力例に表示されているのは、192.168.1.2 にあるネイバーに適用されたポリシーです。この出力には、継承されたポリシーと、このネイバーデバイスで設定されたポリシーの両方が表示されています。継承されたポリシーは、ピアグループ、またはピアポリシー テンプレートからネイバーが継承したポリシーです。

```
Device# show ip bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
  route-map ROUTE in
Inherited polices:
  prefix-list NO-MARKETING in
  route-map ROUTE in
  weight 300
  maximum-prefix 10000
```

BGP ルートマップの next-hop self の設定

ip next-hop self 設定を追加し、bgp next-hop unchanged 設定と bgp next-hop unchanged allpaths 設定をオーバーライドして、既存のルートマップを変更するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map map-tag permit sequence-number**
4. **match source-protocol source-protocol**
5. **set ip next-hop self**
6. **exit**
7. **route-map map-tag permit sequence-number**
8. **match route-type internal**
9. **match route-type external**
10. **match source-protocol source-protocol**
11. **exit**
12. **router bgp autonomous-system-number**
13. **neighbor {ip-address | ipv6-address | peer-group-name} remote-as autonomous-system-number**
14. **address-family vpvv4**
15. **neighbor {ip-address | ipv6-address | peer-group-name} activate**
16. **neighbor {ip-address | ipv6-address | peer-group-name} next-hop unchanged allpaths**
17. **neighbor {ip-address | ipv6-address | peer-group-name} route-map map-name out**
18. **exit**
19. **address-family ipv4 [unicast | multicast| vrf vrf-name]**
20. **bgp route-map priority**
21. **redistribute protocol**
22. **redistribute protocol**
23. **exit-address-family**
24. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	route-map map-tag permit sequence-number 例 : Device(config)# route-map static-next-hop-rewrite permit 10	ルーティング プロトコル間でルート再配布する条件を定義し、ルートマップコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	match source-protocol <i>source-protocol</i> 例 : Device(config-route-map)# match source-protocol static	送信元プロトコルに基づいて、Enhanced Interior Gateway Routing Protocol (EIGRP) の外部ルートを照合します。
ステップ 5	set ip next-hop self 例 : Device(config-route-map)# set ip next-hop self	自身をネクスト ホップとるようにローカル ルート (BGP の場合のみ) を設定します。
ステップ 6	exit 例 : Device(config-route-map)# exit	ルートマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	route-map map-tag permit sequence-number 例 : Device(config)# route-map static-nexthop-rewrite permit 20	ルーティング プロトコル間でルートを再配布する条件を定義し、ルートマップ コンフィギュレーション モードを開始します。
ステップ 8	match route-type internal 例 : Device(config-route-map)# match route-type internal	指定されたタイプのルートを再配布します。
ステップ 9	match route-type external 例 : Device(config-route-map)# match route-type external	指定されたタイプのルートを再配布します。
ステップ 10	match source-protocol <i>source-protocol</i> 例 : Device(config-route-map)# match source-protocol connected	送信元プロトコルに基づいて、Enhanced Interior Gateway Routing Protocol (EIGRP) の外部ルートを照合します。
ステップ 11	exit 例 : Device(config-route-map)# exit	ルートマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 12	router bgp <i>autonomous-system-number</i> 例 :	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

	コマンドまたはアクション	目的
	Device(config)# router bgp 45000	
ステップ 13	neighbor { <i>ip-address</i> <i>ipv6-address</i> <i>peer-group-name</i> } remote-as <i>autonomous-system-number</i> 例 : Device(config-router)# neighbor 172.16.232.50 remote-as 65001	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 14	address-family vpv4 例 : Device(config-router)# address-family vpv4	VPNv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーションモードを開始します。
ステップ 15	neighbor { <i>ip-address</i> <i>ipv6-address</i> <i>peer-group-name</i> } activate 例 : Device(config-router-af)# neighbor 172.16.232.50 activate	ボーダーゲートウェイプロトコル (BGP) ネイバーとの情報交換を有効にします。
ステップ 16	neighbor { <i>ip-address</i> <i>ipv6-address</i> <i>peer-group-name</i> } next-hop unchanged allpaths 例 : Device(config-router-af)# neighbor 172.16.232.50 next-hop unchanged allpaths	マルチホップとして設定されている外部 EBGP ピアで、ネクスト ホップを変更せずに伝播できるようにします。
ステップ 17	neighbor { <i>ip-address</i> <i>ipv6-address</i> <i>peer-group-name</i> } route-map <i>map-name</i> out 例 : Device(config-router-af)# neighbor 172.16.232.50 route-map static-nexthop-rewrite out	発信ルートにルート マップを適用します。
ステップ 18	exit 例 : Device(config-router-af)# exit	アドレスファミリ コンフィギュレーションモードを終了して、ルータ コンフィギュレーションモードを開始します。
ステップ 19	address-family ipv4 [unicast multicast vrf <i>vrf-name</i>] 例 : Device(config-router)# address-family ipv4 unicast vrf inside	IPv4 アドレスファミリを指定し、アドレスファミリ コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 20	bgp route-map priority 例 : Device(config-router-af)# bgp route-map priority	ローカル BGP ルーティングプロセスについてルートマップを優先することを設定します。
ステップ 21	redistribute protocol 例 : Device(config-router-af)# redistribute static	ルートを1つのルーティングドメインから他のルーティングドメインに再配布します。
ステップ 22	redistribute protocol 例 : Device(config-router-af)# redistribute connected	ルートを1つのルーティングドメインから他のルーティングドメインに再配布します。
ステップ 23	exit-address-family 例 : Device(config-router-af)# exit address-family	アドレスファミリー コンフィギュレーションモードを終了し、ルータ コンフィギュレーションモードを開始します。
ステップ 24	end 例 : Device(config-router)# end	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードを開始します。

BGP の設定例

例：条件付き BGP ルートの注入の設定

次の出力例は、**show ip bgp injected-paths** コマンドを入力したときに表示される出力に類似しています。

```
Device# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop           Metric LocPrf Weight Path
*> 172.16.0.0        10.0.0.2              0 ?
*> 172.17.0.0/16    10.0.0.2              0 ?
```

例：ピアセッションテンプレートの設定

次の例は、セッションテンプレート コンフィギュレーション モードで、INTERNAL-BGP という名前のピアセッションテンプレートを作成します。

```
router bgp 45000
  template peer-session INTERNAL-BGP
  remote-as 50000
  timers 30 300
  exit-peer-session
```

次の例は、ピアセッションテンプレート CORE1 を作成します。この例は、INTERNAL-BGP というピアセッションテンプレートのコンフィギュレーションを継承します。

```
router bgp 45000
  template peer-session CORE1
  description CORE-123
  update-source loopback 1
  inherit peer-session INTERNAL-BGP
  exit-peer-session
```

次の例は、CORE1 ピアセッションテンプレートを継承するように、192.168.3.2 ネイバーを設定します。192.168.3.2 ネイバーも、ピアセッションテンプレート INTERNAL-BGP から間接的にコンフィギュレーションを継承します。neighbor inherit 文を動作させるには、remote-as 文を明示的に使用する必要があります。ピアリングが設定されていない場合、指定されたネイバーはセッションテンプレートを受け付けません。

```
router bgp 45000
  neighbor 192.168.3.2 remote-as 50000
  neighbor 192.168.3.2 inherit peer-session CORE1
```

例：ピアポリシーテンプレートの設定

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

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

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

```
router bgp 45000
  template peer-policy PRIMARY-IN
  prefix-list ALLOW-PRIMARY-A in
  route-map SET-LOCAL in
  weight 2345
  default-originate
  exit-peer-policy
```

例 : BGP ルート マップの next-hop self の設定

次の例は、ピア ポリシー テンプレート CUSTOMER-A を作成します。このピア ポリシー テンプレートは、PRIMARY-IN および GLOBAL という名前のピア ポリシー テンプレートからコンフィギュレーションを継承するように設定されています。

```
router bgp 45000
  template peer-policy CUSTOMER-A
  route-map SET-COMMUNITY in
  filter-list 20 in
  inherit peer-policy PRIMARY-IN 20
  inherit peer-policy GLOBAL 10
  exit-peer-policy
```

次の例は、アドレス ファミリ モードでピア ポリシー テンプレート CUSTOMER-A を継承するように 192.168.2.2 ネイバーを設定します。この例は上の例の続きと仮定しており、上のピア ポリシー テンプレート CUSTOMER-A は PRIMARY-IN および GLOBAL という名前のテンプレートからコンフィギュレーションを継承しているため、192.168.2.2 ネイバーもピア ポリシー テンプレート PRIMARY-IN および GLOBAL から間接継承します。

```
router bgp 45000
  neighbor 192.168.2.2 remote-as 50000
  address-family ipv4 unicast
    neighbor 192.168.2.2 inherit peer-policy CUSTOMER-A
  end
```

例 : BGP ルート マップの next-hop self の設定

この項では、BGP ルート マップの next-hop self を設定する方法の例を示します。

この例では、bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定をオーバーライドするネットワークを照合するルート マップを設定します。次に、next-hop self を設定します。その後、指定したアドレス ファミリに対して bgp route-map priority を設定して、指定済みのルート マップが bgp next-hop unchanged と bgp next-hop unchanged allpaths の設定よりも優先されるようにします。この設定により、スタティック ルートは自身をネクスト ホップとして再配布されますが、接続されたルートおよび IBGP または EBGP を介して学習されたルートは引き続きネクスト ホップを変更せずに再配布されます。

```
route-map static-nexthop-rewrite permit 10
  match source-protocol static
  set ip next-hop self
route-map static-nexthop-rewrite permit 20
  match route-type internal
  match route-type external
  match source-protocol connected
!
router bgp 65000
  neighbor 172.16.232.50 remote-as 65001
  address-family vpnv4
    neighbor 172.16.232.50 activate
    neighbor 172.16.232.50 next-hop unchanged allpaths
    neighbor 172.16.232.50 route-map static-nexthop-rewrite out
  exit-address-family
  address-family ipv4 unicast vrf inside
    bgp route-map priority
    redistribute static
```

```

    redistribute connected
  exit-address-family
end

```

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になった場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティングパスを検出することもできます。

下の図に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。

表 3: IP BGP の *clear* および *show* コマンド

<code>clear ip bgp address</code>	特定の BGP 接続をリセットします。
<code>clear ip bgp *</code>	すべての BGP 接続をリセットします。
<code>clear ip bgp peer-group tag</code>	BGP ピア グループのすべてのメンバを削除します。
<code>show ip bgp prefix</code>	プレフィックスがアドバタイズされるピア グループとピア グループに含まれないピアを表示します。ブやローカルプレフィックスなどのプレフィックスも表示されます。
<code>show ip bgp cidr-only</code>	サブネットおよびスーパーネット ネットワーク すべてを BGP ルートを表示します。
<code>show ip bgp community [community-number] [exact]</code>	指定されたコミュニティに属するルートを表示します。
<code>show ip bgp community-list community-list-number [exact-match]</code>	コミュニティ リストで許可されたルートを表示します。
<code>show ip bgp filter-list access-list-number</code>	指定された AS パス アクセス リストによって許可されたルートを表示します。
<code>show ip bgp inconsistent-as</code>	送信元の AS と矛盾するルートを表示します。
<code>show ip bgp regexp regular-expression</code>	コマンドラインに入力された特定の正規表現と一致するルートを表示します。
<code>show ip bgp</code>	BGP ルーティング テーブルの内容を表示します。

<code>show ip bgp neighbors [address]</code>	各ネイバーとの BGP 接続および TCP 接続に関する表示します。
<code>show ip bgp neighbors [address] [advertised-routes dampened-routes flap-statistics paths regular-expression received-routes routes]</code>	特定の BGP ネイバーから取得されたルートを表示
<code>show ip bgp paths</code>	データベース内のすべての BGP パスを表示します
<code>show ip bgp peer-group [tag] [summary]</code>	BGP ピア グループに関する情報を表示します。
<code>show ip bgp summary</code>	BGP 接続すべての状況を表示します。

`bgp log-neighbor changes` コマンドは、デフォルトでは有効です。そのため、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージをログに記録できます。

ボーダー ゲートウェイ プロトコルの機能情報

表 4: ボーダー ゲートウェイ プロトコルの機能情報

機能名	リリース	機能情報
ボーダー ゲートウェイ プロトコル	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。
条件付き BGP ルートの挿入	Cisco IOS XE Gibraltar 16.11.1	この機能が導入されました。
BGP ピア テンプレート	Cisco IOS XE Gibraltar 16.11.1	この機能が導入されました。
BGP ルートマップネクスト ホップセルフ	Cisco IOS XE Gibraltar 16.11.1	この機能が導入されました。

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。