BGP ネイバー セッション オプションの設定

このモジュールでは、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ネイバー ピア セッションに関するさまざまなオプションを設定する設定作業について説明します。BGP は、組織間のループのないルーティングを提供するよう設計されたドメイン間ルーティング プロトコルです。このモジュールには、BGP ネイバー セッションのコマンドを使用して、高速セッションを無効に設定し、ピアリング セッションがディセーブルまたはダウン状態のときにルータが BGP ネイバー ピアリング セッションを自動的に再確立するように設定し、自律システムの移行に役立つオプションを設定し、簡単なセキュリティ メカニズムを設定して外部 BGP（eBGP）ピアリング セッションを CPU 利用率に基づく攻撃から防御する作業が含まれます。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「BGP ネイバー セッションのオプション設定の機能情報」（P.46）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

BGP ネイバー セッション オプションの設定の前提条件

BGP の拡張機能を設定する前に、「Cisco BGP Overview」モジュールと「Configuring a Basic BGP Network」モジュールについて十分に理解しておく必要があります。

BGP ネイバー セッション オプションの設定の制約事項

Cisco IOS ソフトウェアを実行するルータは、1 つの BGP ルーティング プロセスだけを実行し、1 つの BGP 自律システムだけのメンバになるように設定できます。ただし、BGP ルーティング プロセスと自律システムでは、複数のアドレス ファミリ設定をサポートできます。

BGP ネイバー セッション オプションの設定に関する情報

このモジュールで BGP 機能を設定するには、次の概念を理解しておく必要があります。

BGP ネイバー セッション

BGP は主に、ローカル ネットワークを外部ネットワークに接続して、インターネットにアクセスしたり、他の組織に接続したりするために使用されます。BGP 対応ルータは、別の BGP 対応デバイスを自動的には検出しません。ネットワーク管理者は、通常、BGP 対応ルータ間の関係を手動で設定します。BGP ネイバー デバイスは、別の BGP 対応デバイスへのアクティブな Transmission Control Protocol（TCP; 伝送制御プロトコル）接続がある BGP 対応ルータです。BGP デバイス間の関係は、多くの場合、ネイバーではなくピアと呼ばれます。これは、ネイバーは、複数の BGP デバイスがその間で他のルータを経由せず直接接続する概念を意味する場合があるためです。BGP ネイバーまたはピア セッションの設定には BGP ネイバー セッションのコマンドが使用されるため、このモジュールではピアではなくネイバーという用語を使用します。

高速ピアリング セッションの非アクティブ化に対する BGP サポート

BGP ホールド タイマー

デフォルトでは、BGP ホールド タイマーは、Cisco IOS ソフトウェアで 180 秒ごとに実行するように設定されます。このタイマー値は、デフォルトとして設定され、BGP ルーティング プロセスを別のルーティング プロトコルを持つピアリング セッションによってもたらされる可能性がある不安定な状態から保護します。BGP ルータは、通常、大きなルーティング テーブルを持っているため、頻繁にセッションをリセットすることは好ましくありません。

BGP の高速ピアリング セッションの非アクティブ化

BGP の高速ピアリング セッションを無効にすると、BGP コンバージェンスおよび BGP ネイバーの隣接変更に対する応答時間が向上します。この機能は、イベントによって引き起こされ、ネイバーごとに設定されます。この機能をイネーブルにすると、BGP は指定したネイバーでピアリング セッションをモニタします。隣接変更が検出され、終了したピアリング セッションがデフォルトのまたは設定した BGP スキャン間隔中に無効にされます。

BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング

Cisco IOS Release 12.4(4)T、12.2(31)SB、12.2(33)SRB、およびこれら以降のリリースでは、BGP の選択的アドレス トラッキング機能により、BGP の高速セッションの非アクティブ化とともにルート マップの使用が導入されました。**route-map** キーワードおよび *map-name* 引数は、**neighbor fall-over** BGP ネイバー セッション コマンドとともに使用され、BGP ピアへのルートが変更されたときに、この BGP ネイバーのあるピアリング セッションをリセットする必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、拒否文が返された場合、ピア セッションがリセットされます。このルート マップはセッションの確立には使用されません。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

最大プレフィクス到達後の BGP ネイバー セッションの再起動

プレフィクス制限および BGP ピアリング セッション

BGP を実行するルータがピア ルータから受信可能なプレフィクスの最大数に関して設定可能な制限があります。この制限は、**neighbor maximum-prefix** コマンドで設定されます。ルータがピア ルータから過剰のプレフィクスを受信し、最大プレフィクス制限を超えると、このピアリング セッションはディセーブルになるか、ダウン状態になります。このセッションは、ネットワーク オペレータが **clear ip bgp** コマンドを入力して、手動でセッションを再アクティブ化するまでダウン状態のままです。**clear ip bgp** コマンドを入力すると、格納されたプレフィクスはクリアされます。

最大プレフィクス制限による BGP ネイバー セッションの再起動

Cisco IOS Release 12.0(22)S、12.2(15)T、12.2(18)S、およびこれら以降のリリースでは、**restart** キーワードが導入され、**neighbor maximum-prefix** コマンドの機能が拡張されています。この機能拡張により、ネットワーク オペレータは、BGP ネイバー ピアリング セッションがディセーブルまたはダウン

状態のときにルータがこのピアリング セッションを自動的に再確立するように設定できます。ピアリングが自動的に再確立できる設定可能な時間間隔があります。**restart** キーワードの設定可能なタイマー引数は、分単位で指定されます。時間の範囲は、
1 ～ 65,535 分です。

BGP ネットワーク自律システムの移行

BGP ネットワークの自律システムの移行

自律システムの移行は、テレコミュニケーションまたはインターネット サービス プロバイダーが別のネットワークを購入したとときに必要になる場合があります。お客様の既存のピアリング環境を中断せずにプロバイダーが 2 番目の自律システムを統合できることが望ましいです。お客様のネットワークで必要な設定の量によっては、サービスを中断せずに完了するのが困難な、煩雑な作業となります。

BGP ネットワーク自律システムの移行に対するデュアル自律システムのサポート

Cisco IOS Release 12.0(29)S、12.3(14)T、12.2(33)SXH、およびこれら以降のリリースでは、デュアル BGP 自律システム設定のサポートが追加され、お客様のピアリング セッションを中断せずにセカンダリ自律システムをプライマリ自律システムの下に結合できます。この機能の設定は、お客様のネットワークに対して透過的です。デュアル BGP 自律システム設定により、自律システムの移行中にルータをセカンダリ自律システムのメンバとして外部ピアに対して表示できます。この機能により、ネットワーク オペレータは、複数の自律システムを結合でき、その後、通常のサービス時間に既存のピアリング環境を中断せずにお客様を新しい設定に移行できます。

neighbor local-as コマンドを使用して、eBGP ネイバーから受信するルートの自律システム番号を追加および削除して、AS_PATH アトリビュートがカスタマイズされます。この機能により、自律システム番号を移行するために、外部ピアに対して別の自律システムのメンバとしてルータを表示できます。この機能は、ネットワーク オペレータがセカンダリ自律システムをプライマリ自律システムに結合し、その後、通常のサービス時間中に既存のピアリング環境を中断せずにお客様の設定をアップデートすることにより、BGP ネットワークでの自律システム番号の変更プロセスを簡略化します。

コンフェデレーション、個別のピアリング セッション、およびピア グループに対する BGP 自律システムの移行サポート

この機能は、コンフェデレーション、個別のピアリング セッション、およびピア グループとピア テンプレートによって適用される設定をサポートします。この機能がグループ ピアに適用されると、個別ピアはカスタマイズできません。

BGP 自律システムの移行中のフィルタリングの入力

自律システム パスのカスタマイゼーションにより、設定ミスによりルーティング ループが作成される可能性が高まります。お客様のピアリング数が増加するにつれ危険が高まります。入力インターフェイスに関するポリシーを適用して、遷移中または **local-as** 設定のないルートの自律システム番号をブロックすることにより、この可能性を低減できます。

注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。この機能は、自律システムの移行のためだけに設定する必要があり、遷移が完了した後設定解除する必要があります。不適切に設定するとルーティング ループが作成される可能性があるため、この手順は、経験を積んだネットワーク オペレータだけが行ってください。

BGP ネットワークの 4 バイト自律システム番号への移行

4 バイト ASN に対する BGP サポート機能により、4 バイト自律システム番号がサポートされるようになりました。自律システム番号の要求の増加に伴い、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 バイト自律システム番号の割り当てを開始します。

Cisco の 4 バイト自律システム番号の実装は、Request For Comments（RFC; コメント要求）4893 をサポートします。RFC 4893 は、2 バイト自律システム番号から 4 バイト自律システム番号への段階的移行を BGP がサポートできるように開発されました。RFC 4893 では新たに 23456 が予約済み（プライベート）自律システム番号に指定され、Cisco IOS CLI ではこの番号を自律システム番号として設定できなくなっています。

ご使用の BGP ネットワークを 4 バイト自律システム番号に移行するには計画が必要です。4 バイト自律システム番号をサポートしているイメージにアップグレードしている場合でも、2 バイト自律システム番号を使用できます。4 バイト自律システム番号に設定された形式にかかわらず、2 バイト自律システムの **show** コマンド出力と正規表現のマッチングは変更されず、asplain（10 進数）形式のままになります。

スムーズな移行を確実に行うには、4 バイト自律システム番号を使用して識別される自律システム内の BGP スピーカーをすべて、4 バイト自律システム番号をサポートするようにアップグレードすることを推奨します。

BGP ネットワークを 4 バイトの自律システムのフル サポートにアップグレードする手順の詳細については、『*Migration Guide for Explaining 4-Byte Autonomous System*』ホワイト ペーパーを参照してください。

BGP ネイバー セッションの TTL セキュリティ チェック

TTL セキュリティ チェックに対する BGP サポート

TTL セキュリティ チェック機能は、BGP に実装されると簡単なセキュリティ メカニズムを導入し、eBGP ネイバー セッションを CPU 利用率に基づく攻撃から防御します。この種の攻撃は、通常、偽造の送信元と宛先の IP アドレスを含む大量の IP パケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せの Denial of Service（DoS; サービス拒絶）攻撃です。

TTL セキュリティ チェックは、受信 IP パケットの TTL フィールドの値を各 eBGP ネイバー セッションにローカルで設定されているホップ カウントと比較して、eBGP ネイバー セッションを防御します。着信 IP パケットの TTL フィールドの値が、ローカルで設定された値以上の場合、この IP パケットは受け入れられ、通常どおり処理されます。IP パケットの TTL 値が、ローカルで設定された値未満の場

合、このパケットはサイレントに廃棄され、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。

IP パケット ヘッダーの TTL フィールドを偽造することは可能ですが、信頼できるピアが属するネットワークが損なわれていない限り、信頼できるピアの TTL カウントと一致するように TTL カウントを正確に偽造することは不可能です。

TTL セキュリティ チェックは、直接接続されているネイバー セッションとマルチホップ eBGP ネイバー セッションの両方をサポートします。BGP ネイバー セッションは、無効な TTL 値を含む着信パケットには影響されません。BGP ネイバー セッションは開いたままで、ルータがサイレントに無効なパケットを廃棄します。ただし、それでも BGP セッションは、セッション タイマーが期限切れになる前にキープアライブ パケットを受信しないと期限切れになることがあります。

BGP ネイバー セッションの TTL セキュリティ チェック

TTL セキュリティ チェックに対する BGP サポート機能は、**neighbor ttl-security** コマンドを使用してルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで設定されます。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能をイネーブルにすると、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。*hop-count* 引数は、2 つのピアを区切るホップの最大数を設定するために使用されます。TTL 値は、設定されたホップ カウントからルータによって決定されます。この引数の値は、1 ～ 254 の数値です。

マルチホップ BGP ネイバー セッションに対する TTL セキュリティ チェックのサポート

TTL セキュリティ チェックに対する BGP サポート機能は、直接接続されているネイバー セッションとマルチホップ ネイバー セッションの両方をサポートします。この機能がマルチホップ ネイバー セッションに設定されている場合、**neighbor ebgp-multihop** ルータ コンフィギュレーション コマンドは設定できず、ネイバー セッションを確立する必要はありません。これらのコマンドは、二者択一で、マルチホップ ネイバー セッションを確立するには 1 つのコマンドだけが必要です。両方のコマンドを同じピアリング セッションに設定しようとすると、コンソールにエラー メッセージが表示されます。

この機能を既存のマルチホップ セッションに設定するには、まず既存のネイバー セッションを **no neighbor ebgp-multihop** コマンドを使用してディセーブルにする必要があります。マルチホップ ネイバー セッションは、この機能を **neighbor ttl-security** コマンドを使用してイネーブルにすると復元されます。

この機能は、参加している各ルータで設定する必要があります。この機能の効果を最大化するには、ローカル ネットワークと外部ネットワークの間のホップ数が一致するように *hop-count* 引数を厳密に設定する必要があります。ただし、この機能をマルチホップ ネイバー セッションに設定する場合は、パスの種類を考慮する必要もあります。

TTL セキュリティ チェックに対する BGP サポートの利点

TTL セキュリティ チェックに対する BGP サポート機能は、eBGP ネイバー セッションを CPU 利用率に基づく攻撃から防御する、効果的で容易に導入できるソリューションを提供します。この機能がイネーブルの場合、ホストがローカル BGP ネットワークまたはリモート BGP ネットワークのメンバでない場合、あるいはホストがローカル BGP ネットワークとリモート BGP ネットワークの間のネットワーク セグメントに直接接続されていない場合、ホストは BGP セッションを攻撃できません。このソリューションは、BGP 自律システムへの DoS 攻撃の効果を大幅に軽減します。

セッションごとの TCP Path 最大伝送ユニット（MTU）Discovery に対する BGP サポート

Path MTU Discovery（PMTUD）

IP プロトコル ファミリは、広範な伝送リンクを使用できるように設計されました。最大 IP パケット長は、65000 バイトです。ほとんどの伝送リンクは、Maximum Transmission Unit（MTU; 最大伝送ユニット）と呼ばれる、より小さい最大パケット長の制限が適用されます。この制限は、伝送リンクの種類によって異なります。IP の設計は、発信リンクに対する必要に応じて中間ルータで IP パケットをフラグメント化することにより、リンク パケット長の制限を受け入れます。IP パケットの最後の宛先は、必要に応じて、フラグメント化されたパケットの再組み立てを行います。

すべての TCP セッションは、単一のパケットで転送可能なバイト数に関する制限によってバインドされます。この制限は、Maximum Segment Size（MSS; 最大セグメント サイズ）と呼ばれます。TCP は、パケットを IP レイヤに渡す前に、送信キューでパケットをチャンクに分割します。小さい MSS は、宛先デバイスへのパスにある IP デバイスで断片化されない場合がありますが、小さいパケットは、パケットを転送するために必要な帯域幅の量を増加します。最大 TCP パケット長は、TCP セットアップ プロセス中に、送信元デバイスのアウトバウンド インターフェイスの MTU と宛先デバイスによって知らされる MSS の両方によって決まります。

Path MTU Discovery（PMTUD）は、最適の TCP パケット長を検出するソリューションとして開発されました。PMTUD は、最適化（RFC 1191 で詳述）で、ここで送信元から宛先へのパスで断片化されない TCP 接続が最長パケットの送信を試行します。PMTUD は、この作業を IP パケットでフラグ Don't Fragment（DF）を使用して行います。このフラグは、パケットが長すぎるため、これをリンクを超えて送信できない中間ルータの動作を変えるためのものです。通常、このフラグはオフで、ルータはパケットをフラグメント化し、このフラグメントを送信する必要があります。ルータが、DF ビットが設定された状態で IP データグラムをパケットのサイズよりも小さい MTU を持つリンクに転送しようとすると、ルータは、パケットをドロップし、インターネット制御メッセージ プロトコル（ICMP）宛先到着不能メッセージを「断片化が必要です。DF が設定されています」ということを示すコードとともにこの IP データグラムの送信元に返します。送信元のデバイスは、ICMP メッセージを受信すると、送信 MSS を低くし、TCP がセグメントを再送信するときに、より小さいセグメント サイズを使用します。

BGP ネイバー セッションの TCP の PMTUD

TCP の PMTUD は、すべての BGP ネイバー セッションに対してデフォルトでイネーブルにされますが、1 つまたはすべての BGP ネイバー セッションに対して TCP の PMTUD をディセーブルにする必要がある場合があります。PMTUD は、大きい伝送リンク（たとえば、Packet over Sonet リンク）では適切に動作しますが、不適切に設定された TCP 実装やファイアウォールでは、任意のパケットから転送された TCP 接続を遅くしたり停止したりする場合があります。この種の状況では、TCP の PMTUD をディセーブルにする必要がある場合があります。Cisco IOS Release 12.2(33)SRA、12.2(31)SB、12.2(33)SXH、12.4(20)T、およびこれら以降のリリースでは、設定オプションが導入され TCP の PMTUD を単一の BGP ネイバー セッションまたはすべての BGP セッションに対してディセーブル、または再度イネーブルにできます。TCP の PMTUD をすべての BGP ネイバーに対してグローバルにディセーブルにするには、**no bgp transport path-mtu-discovery** コマンドをルータ コンフィギュレーション モードで使用します。単一のネイバーに対して TCP の PMTUD をディセーブルにするには、**no neighbor transport path-mtu-discovery** コマンドをルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで使用します。詳細については、「すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化」（P.22）または「単

一の BGP ネイバーに対する TCP の PMTUD のディセーブル化」（P.25）を参照してください。

BGP ダイナミック ネイバー

BGP ダイナミック ネイバーに対するサポートが Cisco Catalyst 6500 シリーズ スイッチの Cisco IOS Release 12.2(33)SXH に導入されました。BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。各範囲は、サブネット IP アドレスとして設定できます。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。サブネットの範囲が BGP ピア グループに対して設定され、TCP セッションがそのサブネットの範囲の IP アドレスに対して別のルータによって開始された後、新しい BGP ネイバーがそのグループのメンバとしてダイナミックに作成されます。サブネットの範囲の初期設定およびピア グループのアクティベーション（*範囲のグループの受信*と呼ばれる）の後、ダイナミック BGP ネイバーの作成には、初期ルータへのさらなるコマンドライン インターフェイス（CLI）設定は必要ありません。その他のルータは、初期ルータを使用する BGP セッションを確立できますが、BGP セッションに使用されるリモート ピアの IP アドレスが設定された範囲内にない場合、この初期ルータは、この BGP セッションを設定する必要はありません。

BGP ダイナミック ネイバー機能をサポートするには、次の 3 つの **show** コマンドの出力がダイナミック ネイバーに関する情報を表示するようにアップデートされている必要があります。コマンドは、**show ip bgp neighbors**、**show ip bgp peer-group**、**show ip bgp summary** コマンドです。

ダイナミック BGP ネイバーは、ピア グループのすべての設定を継承します。大きい BGP ネットワークで BGP ダイナミック ネイバーを実装すると CLI 設定の量と複雑さが軽減され、CPU とメモリの使用量が節約されます。IPv4 ピアリングだけがサポートされます。

BGP ネイバー セッションのオプションの設定方法

ここでは、次の作業または作業グループについて説明します。

高速セッションの非アクティブ化の設定

このセクションの作業は、BGP ネクストホップ アドレス トラッキングの設定方法を示しています。BGP ネクストホップ アドレス トラッキングによって、RIB でのネクストホップの変更に対する BGP の応答時間が大幅に改善されます。ただし、不安定な Interior Gateway Protocol（IGP）ピアにより、BGP ネイバー セッションが不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。ルートのダンプニングの詳細については、「Configuring Internal BGP Features」モジュールを参照してください。

BGP ネイバー の高速セッションの非アクティブ化の設定

BGP ネイバーを持つピアリング セッションを確立し、このピアリング セッションを高速セッションの非アクティブ化に設定して、このピアリング セッションが無効にされた場合のネットワーク コンバージェンス時間を向上するには、次の作業を実行します。

IGP ルートの積極的ダンプニング

この機能をイネーブルにすると、BGP コンバージェンス時間が大幅に向上します。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアは、引き続き BGP ネイバー セッションに不安定な状態をもたらす場合があります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **fall-over**
7. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 50000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router-af)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router-af)# neighbor 10.0.0.1 remote-as 50000`	BGP ネイバーを持つピアリング セッションを確立します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor ip-address fall-over** **例：** `Router(config-router-af)# neighbor 10.0.0.1 fall-over`	高速セッションを無効にするように BGP ピアリングを設定します。 • BGP は、セッションが無効になると、このピアで学習したすべてのルートを削除します。
ステップ 7	**end** **例：** `Router(config-router-af)# 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。

高速セッションの非アクティブ化の選択的アドレス トラッキングの設定

高速セッションの非アクティブ化の選択的アドレス トラッキングを設定するには、次の作業を実行します。**neighbor fall-over** コマンドのオプションの **route-map** キーワードおよび *map-name* 引数を使用して、BGP ピアへのルートが変更されたときに BGP ネイバーを持つピアリング セッション非アクティブ化（リセット）する必要があるかどうかを判断します。このルート マップは、新しいルートに対して評価され、拒否文が返された場合、ピア セッションがリセットされます。

（注） **match ip address** コマンドと **match source-protocol** コマンドだけがルート マップでサポートされます。**set** コマンドやその他の **match** コマンドはサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **fall-over** [**route-map** *map-name*]
6. **exit**
7. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
8. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
9. **match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*]
10. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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*} **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 192.168.1.2 remote-as 40000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**neighbor** *ip-address* **fall-over** [**route-map** *map-name*] **例：** `Router(config-router)# neighbor 192.168.1.2 fall-over route-map CHECK-NBR`	BGP へのルートが変更されるときにルート マップを適用します。 • この例では、ネイバー 192.168.1.2 へのルートが変更されるときに、CHECK-NBR という名前のルート マップが適用されます。
ステップ 6	**exit** **例：** `Router(config-router)# exit`	ルータ 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 7	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length* | **permit** *network*/*length*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28`	BGP ネクストホップ ルート フィルタリングのプレフィクス リストを作成します。 • 選択的ネクストホップ ルート フィルタリングは、アドレス ファミリごとにプレフィクス長のマッチングまたは送信元プロトコルのマッチングをサポートします。 • この例では、マスク長が 28 以上の場合だけルートを許可する FILTER28 という名前のプレフィクス リストが作成されます。
ステップ 8	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map CHECK-NBR 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。 • この例では、CHECK-NBR という名前のルート マップが作成されます。次の **match** コマンドで IP アドレスの一致がある場合、IP アドレスは許可されます。

	コマンドまたはアクション	目的
ステップ 9	**match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*] **例：** `Router(config-route-map)# match ip address prefix-list FILTER28`	指定されたプレフィクス リスト内の IP アドレスのマッチングを行います。 • プレフィクス リストの名前を指定するには、*prefix-list-name* 引数を使用します。省略記号は、複数のプレフィクス リストを指定できることを意味します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 10	**end** **例：** `Router(config-route-map)# end`	ルート マップ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

次の作業

ネクストホップ アドレス トラッキングに対する BGP サポート機能は、ネクストホップの RIB にインストールされたルートの変更に対する BGP の応答時間を向上させます。また、BGP コンバージェンス全体も向上させます。BGP ネクストホップ アドレス トラッキングの詳細については、「Configuring Advanced BGP Features」モジュールを参照してください。

最大プレフィクス制限を超えた後にネイバー セッションを再確立するためのルータの設定

BGP ピアから受信されたプレフィクス数が最大プレフィクス制限を超えたときに、ルータによって BGP ネイバー セッションが再確立される時間間隔を設定するには、次の作業を実行します。

ネイバー セッションの再確立

ネットワーク オペレータは、設定された最大プレフィクス制限を超えたためにダウン状態になったネイバー セッションを自動的に再確立するように BGP を実行しているルータを設定できます。この機能がイネーブルのときには、ネットワーク オペレータの介入は必要ありません。

制約事項

この作業は、ディセーブルになった BGP ネイバー セッションをネットワーク オペレータが指定した時間間隔で再確立しようとします。ただし、再起動タイマーの設定だけでは、超過プレフィクス数を送信しているピアを変更または修正できません。ネットワーク オペレータは、最大プレフィクス制限を再設定するか、そのピアから送信されるプレフィクス数を減らす必要があります。プレフィクスを過剰に送信するように設定されたピアは、ネットワークに不安定な状態をもたらす可能性があり、ネットワークで過剰な数のプレフィクスが即座にアドバタイズされ、除去されます。この場合、ネットワーク オペレータが問題の原因を修正する間に、**warning-only** キーワードを設定し、再起動機能をディセーブルにできます。

手順の概要

1. **enable**

2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
5. **exit**
6. **show ip bgp neighbors** [*ip-address*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(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** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**] **例：** `Router(config-router)# neighbor 10.4.9.5 maximum-prefix 1000 90 restart 60`	BGP を実行しているルータの最大プレフィクス制限を設定します。 • **restart** キーワードおよび *restart-interval* 引数を使用して、最大プレフィクス制限を超えたためにディセーブルになったネイバー セッションを自動的に再確立するようにルータを設定します。*restart-interval* の設定範囲は、1 ～ 65535 分 です。 • **warning-only** キーワードを使用して、過剰なプレフィクスを送信しているピアを修正できるように、再起動機能がディセーブルになるようにルータを設定します。 **（注）** *restart-interval* が設定されていないと、最大プレフィクス制限を超えた後もディセーブルになったセッションはダウン状態のままになります。これがデフォルトの動作です。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router(config-router)# exit`	ルータ 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 6	**show ip bgp neighbors** *ip-address* **例：** `Router# show ip bgp neighbors 10.4.9.5`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、指定したネイバーの最大プレフィクス制限および設定された再起動タイマー値を表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

show ip bgp neighbors コマンドの次の出力例により、ディセーブルになったネイバー セッションを自動的に再確立するようにルータが設定されたことを確認できます。この出力は、ネイバー 10.4.9.5 の最大プレフィクス制限が 1000 プレフィクス、再起動しきい値が 90%、再起動間隔が 60 分に設定されていることを示します。

```
Router# show ip bgp neighbors 10.4.9.5

BGP neighbor is 10.4.9.5,  remote AS 101, internal link
  BGP version 4, remote router ID 10.4.9.5
  BGP state = Established, up for 2w2d
  Last read 00:00:14, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:         23095      23095
    Route Refresh:          0          0
    Total:              23096      23096
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor versions 1/0 1/0
  Output queue sizes : 0 self, 0 replicated
  Index 2, Offset 0, Mask 0x4
  Member of update-group 2
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                  Outbound    Inbound
```

```
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
!Configured maximum number of prefixes and restart interval information!
  Maximum prefixes allowed 1000
  Threshold for warning message 90%, restart interval 60 min
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.4.9.21, Local port: 179
Foreign host: 10.4.9.5, Foreign port: 11871

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x5296BD2C):
Timer          Starts    Wakeups            Next
Retrans         23098          0             0x0
TimeWait            0          0             0x0
AckHold         23096      22692             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1900546793  snduna: 1900985663  sndnxt: 1900985663     sndwnd:  14959
irs: 2894590641  rcvnxt: 2895029492  rcvwnd:      14978  delrcvwnd:   1406

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 316 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 46021 (out of order: 0), with data: 23096, total data bytes: 438850
Sent: 46095 (retransmit: 0, fastretransmit: 0), with data: 23097, total data by9
```

トラブルシューティングのヒント

BGP ソフト再設定を使用して BGP 接続をリセットするには、**clear ip bgp** コマンドを使用します。このコマンドは、格納されたプレフィクスをクリアして、BGP を実行しているルータが最大プレフィクス制限を超えないようにするために使用できます。BGP ソフト再設定の使用方法の詳細については、「Configuring a Basic BGP Network」モジュールの「Monitoring and Maintaining Basic BGP task」を参照してください。

次のエラー メッセージの表示は、ネイバー セッションがディセーブルになる根本的な問題を示す可能性があります。ネットワーク オペレータは、最大プレフィクス制限に設定された値および過剰な数のプレフィクスを送信しているすべてのピアの設定を確認する必要があります。次のエラー メッセージ例は、表示される可能性のあるエラー メッセージと類似しています。

```
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Up
00:01:14:%BGP-4-MAXPFX:No. of unicast prefix received from 10.10.10.2 reaches 5, max 6
00:01:14:%BGP-3-MAXPFXEXCEED:No.of unicast prefix received from 10.10.10.2:7 exceed limit6
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Down - BGP Notification sent
00:01:14:%BGP-3-NOTIFICATION:sent to neighbor 10.10.10.2 3/1 (update malformed) 0 byte
```

bgp dampening コマンドを使用して、ピアが過剰な数のプレフィクスを送信し、ネットワークに不安定な状態をもたらすときにフラッピング ルートまたはインターフェイスのダンプニングを設定できます。このコマンドを使用する必要があるのは、トラブルシューティング時または過剰な数のプレフィクスを送信しているルータを調整する場合だけです。BGP のルートのダンプニングの詳細については、「Configuring Advanced BGP Features」モジュールを参照してください。

ネットワーク移行のためのデュアル AS ピアリングの設定

自律システム番号を移行するために、別の自律システムのメンバとして外部ピアに対して BGP ピア ルータを表示するように設定するには、次の作業を実行します。BGP ピアにデュアル自律システム番号が設定されると、ネットワーク オペレータは、セカンダリ自律システムをプライマリ自律システムに結合し、今後のサービス時間中に既存のピアリング環境を中断せずにお客様の設定をアップデートできます。

show ip bgp コマンドおよび **show ip bgp neighbors** コマンドを使用して、ルーティング テーブルのエントリ用の自律システム番号およびこの機能の状況を確認できます。

制約事項

- この機能は、正しい eBGP ピアリング セッションのためだけに設定できます。この機能は、コンフェデレーションの異なるサブ自律システム内の 2 つのピアには設定できません。
- この機能は、個別のピアリング セッションおよびピア グループとピア テンプレートによって適用される設定に設定できます。このコマンドがピアのグループに適用されると、そのピアは個別にカスタマイズできなくなります。

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* **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]
6. **neighbor** *ip-address* **remove-private-as**
7. **exit**
8. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]
9. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 40000`	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** *ip-address* **remote-as** *autonomous-system-number* **例：** `Router(config-router)# neighbor 10.0.0.1 remote-as 45000`	BGP ネイバーを持つピアリング セッションを確立します。
ステップ 5	**neighbor** *ip-address* **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]] **例：** `Router(config-router)# neighbor 10.0.0.1 local-as 50000 no-prepend replace-as dual-as`	eBGP ネイバーから受信したルートの AS_PATH アトリビュートをカスタマイズします。 • **replace-as** キーワードを使用して、（*ip-address* 引数で設定される）ローカル自律システム番号だけを AS PATH アトリビュートにプリペンドします。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** キーワードを使用し、（ローカル BGP ルーティング プロセスからの）実際の自律システム番号を使用するか、*ip-address* 引数（local-as）で設定された自律システム番号を使用して、ピアリング セッションを確立するように eBGP ネイバーを設定します。 • この例では、実際の自律システム番号および local-as 番号を受け入れるように 10.0.0.1 ネイバーを持つピアリング セッションが設定されます。
ステップ 6	**neighbor** *ip-address* **remove-private-as** **例：** `Router(config-router)# neighbor 10.0.0.1 remove-private-as`	（任意）プライベート自律システム番号をアウトバウンド ルーティング アップデートから削除します。 • このコマンドを **replace-as** 機能とともに使用して、プライベート自律システム番号を削除し、この番号を外部自律システム番号に置き換えることができます。 • このコマンドが設定されると、プライベート自律システム番号（64512 ～ 65535）は、AS_PATH アトリビュートから自動的に削除されます。
ステップ 7	**exit** **例：** `Router(config-router)# exit`	ルータ 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。 • このコマンドを繰り返し、特権 EXEC 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 8	**show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter-prefixes** *mask-length*] **例：** `Router# show ip bgp`	BGP ルーティング テーブル内のエントリを表示します。 • この出力を使用して、実際の自律システム番号または local-as 番号が設定されているかどうかを確認できます。
ステップ 9	**show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*] **例：** `Router(config)# show ip bgp neighbors`	ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この出力は、**local AS**、**no-prepend**、**replace-as**、および **dual-as** を対応する自律システム番号とともに表示します（これらのオプションが設定されている場合）。

BGP ネイバー セッションの TTL セキュリティ チェックの設定

IP パケット ヘッダーの TTL 値が BGP ネイバー セッション用に設定された TTL 値以上の場合だけ BGP がセッションを確立または維持できるようにするには、次の作業を設定します。

前提条件

- この機能の効果を最大化するには、これを参加している各ルータで設定することを推奨します。この機能をイネーブルにすると、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。

制約事項

- この機能がマルチホップ ネイバー セッション用に設定されている場合、**neighbor ebgp-multihop** コマンドは必要なく、この機能を設定する前にこのコマンドをディセーブルにする必要があります。
- 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影響を受けたネイバー セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。
- この機能は、ローカル ネットワークおよびリモート ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、ローカル ネットワークとリモート ネットワークの間のネットワーク セグメント上のピアも含まれます。

手順の概要

1. **enable**
2. **trace** [*protocol*] *destination*
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **neighbor** *ip-address***ttl-security hops** *hop-count*
6. **end**
7. **show running-config**

8. **show ip bgp neighbors** [*ip-address*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**trace** [*protocol*] *destination* **例：** `Router# trace ip 10.1.1.1`	パケットが宛先に移動中、実際に通過する指定されたプロトコルのルートを検出します。 • **trace** コマンドを入力して、指定されたピアへのホップ数を決定します。
ステップ 3	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65000`	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 5	**neighbor** *ip-address* **ttl-security hops** *hop-count* **例：** `Router(config-router)# neighbor 10.1.1.1 ttl-security hops 2`	2 つのピアを区切るホップの最大数を設定します。 • *hop-count* 引数は、ローカル ピアとリモート ピアを区切るホップ数に設定されます。IP パケット ヘッダーの予想される TTL 値が 254 の場合、数値 1 を *hop-count* 引数に設定する必要があります。値の範囲は、1 ～ 254 の数番です。 • この機能がイネーブルの場合、BGP は、予想される TTL 値以上の TTL 値を持つ着信 IP パケットを受け入れます。受け入れられないパケットは、サイレントに廃棄されます。 • この設定例では、予想される着信 TTL 値が 253（255 引く TTL 値の 2）以上に設定されます。これは、BGP ピアから予想される最小 TTL 値です。ローカル ルータは、10.1.1.1 ネイバーが 1 または 2 ホップ離れている場合だけ、このネイバーからのピアリング セッションを受け入れます。
ステップ 6	**end** **例：** `Router(config-router)# exit`	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。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** **例：** `Router# show running-config | begin bgp`	（任意）現在実行中のコンフィギュレーション ファイルの内容を表示します。 • このコマンドの出力は、各ピアの **neighbor ttl-security** コマンドの設定を BGP コンフィギュレーション セクションの下に表示します。ここには、ネイバー アドレスおよび構成されたホップ カウントが含まれます。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 8	**show ip bgp neighbors** [*ip-address*] **例：** `Router# show ip bgp neighbors 10.4.9.5`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このコマンドは、この機能がイネーブルの場合、「External BGP neighbor may be up to *number* hops away」と表示します。この *number* 値は、ホップ カウントを表します。これは、1 ～ 254 の数値です。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

TTL セキュリティ チェックに対する BGP サポート機能の設定は、**show running-config** コマンドおよび **show ip bgp neighbors** コマンドを使用して確認できます。この機能は、各ピアでローカルに設定されるため、確認するリモート設定はありません。

次に、**show running-config** コマンドの出力例を示します。この出力は、着信 IP パケットの予想される TTL カウントが 253 または 254 の場合だけ、ネイバー 10.1.1.1 がネイバー セッションを確立または維持するように設定されていることを示します。

```
Router# show running-config | begin bgp

router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 55000
 neighbor 10.1.1.1 ttl-security hops 2
 no auto-summary
.
.
.
```

次に、**show ip bgp neighbors** コマンドの出力例を示します。この出力は、10.1.1.1 ネイバーが 2 ホップ以下離れている場合だけ、ローカル ルータがパケットをこのネイバーから受け入れることを示します。この機能の設定は、出力のアドレス ファミリ セクションに表示されます。関連行は、出力に太字で表示されます。

```
Router# show ip bgp neighbors 10.1.1.1

BGP neighbor is 10.1.1.1,  remote AS 55000, external link
  BGP version 4, remote router ID 10.2.2.22
```

```
  BGP state = Established, up for 00:59:21
  Last read 00:00:21, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  2          2
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           226        227
    Route Refresh:          0          0
    Total:                228        229
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue sizes : 0 self, 0 replicated
  Index 1, Offset 0, Mask 0x2
  Member of update-group 1
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 2; dropped 1
  Last reset 00:59:50, due to User reset
  External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.2.2.22, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 11001

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xCC28EC):
Timer          Starts    Wakeups            Next
Retrans            63          0             0x0
TimeWait            0          0             0x0
AckHold            62         50             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  712702676  snduna:  712703881  sndnxt:  712703881     sndwnd:  15180
irs: 2255946817  rcvnxt: 2255948041  rcvwnd:      15161  delrcvwnd:   1223

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
```

```
Rcvd: 76 (out of order: 0), with data: 63, total data bytes: 1223
Sent: 113 (retransmit: 0, fastretransmit: 0), with data: 62, total data bytes: 4
```

セッションごとの TCP の PMTUD に対する BGP サポートの設定

ここでは、次の作業について説明します。

- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化」（P.22）
- 「単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化」（P.25）
- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化」（P.27）
- 「単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化」（P.29）

すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化

すべての BGP セッションに対して TCP の PMTUD をディセーブルにするには、次の作業を実行します。BGP セッションを設定するときに TCP の PMTUD は、デフォルトでイネーブルになりますが、**show ip bgp neighbors** コマンドを入力して、TCP の PMTUD がイネーブルになっていることを確認することを推奨します。

前提条件

この作業は、アクティブな TCP 接続を持つ BGP ネイバーを事前に設定済みであることを前提としています。

手順の概要

1. **enable**
2. **show ip bgp neighbors** [*ip-address*]
3. **configure terminal**
4. **router bgp** *autonomous-system-number*
5. **no bgp transport path-mtu-discovery**
6. **end**
7. **show ip bgp neighbors** [*ip-address*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip bgp neighbors** [*ip-address*] **例：** `Router# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • このコマンドを使用して、BGP ネイバーで TCP の PMTUD がイネーブルかどうかを判断します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。
ステップ 3	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 50000`	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 5	**no bgp transport path-mtu-discovery** **例：** `Router(config-router)# no bgp transport path-mtu-discovery`	すべての BGP セッションに対して TCP の PMTUD をディセーブルにします。
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp neighbors** **例：** `Router# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、任意のネイバーで TCP の PMTUD がイネーブルであることは、このコマンドの出力によっては表示されません。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対してイネーブルになっていることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD がイネーブルであることを示します。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

次に、**no bgp transport path-mtu-discovery** コマンドが入力された後の **show ip bgp neighbors** コマンドの出力例を示します。path mtu エントリが欠落していることに注意してください。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle
```

単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化

internal BGP（iBGP; 内部 BGP）ネイバーを持つピアリング セッションを確立してから BGP ネイバー セッションに対して TCP の PMTUD をディセーブルにするには、次の作業を実行します。**neighbor transport** コマンドは、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで使用できます。

前提条件

この作業では、TCP の PMTUD がすべての BGP ネイバーに対してデフォルトでイネーブルになっていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **no neighbor** {*ip-address*| *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**}
8. **end**
9. **show ip bgp neighbors**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} **例：** `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(config-router-af)# neighbor 172.16.1.1 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。 • この例では、ネイバー 172.16.1.1 がアクティブ化されます。
ステップ 7	**no neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**} **例：** `Router(config-router-af)# no neighbor 172.16.1.1 transport path-mtu-discovery`	単一の BGP ネイバーに対して TCP の PMTUD をディセーブルにします。 • この例では、TCP の PMTUD がネイバー 172.16.1.1 に対してディセーブルになります。
ステップ 8	**end** **例：** `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp neighbors** **例：** `Router# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、このネイバーが TCP の PMTUD をイネーブルにしたことを表示しません。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の出力例は、TCP の PMTUD が BGP ネイバー 172.16.1.1 に対してディセーブルにされたが、BGP ネイバー 192.168.2.2 に対しては引き続きイネーブルであることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD がイネーブルであることを示します。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.1,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.17.1.99
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.1
  Address tracking requires at least a /24 route to the peer
  Connections established 1; dropped 0
  Last reset never
.
.
.
SRTT: 165 ms, RTTO: 1172 ms, RTV: 1007 ms, KRTT: 0 ms
```

```
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle
.
.
.
BGP neighbor is 192.168.2.2,  remote AS 50000, external link
  BGP version 4, remote router ID 10.2.2.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 192.168.2.2
  Address tracking requires at least a /24 route to the peer
  Connections established 2; dropped 1
  Last reset 00:05:11, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 210 ms, RTTO: 904 ms, RTV: 694 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化

すべての BGP セッションに対して TCP の PMTUD をイネーブルにするには、次の作業を実行します。BGP セッションを設定するときに TCP の PMTUD は、デフォルトでイネーブルになりますが、この機能がディセーブルになっている場合、この作業によってこの機能を再度イネーブルにできます。TCP の PMTUD がイネーブルであることを確認するには、**show ip bgp neighbors** コマンドを使用します。

前提条件

この作業は、アクティブな TCP 接続を持つ BGP ネイバーを事前に設定済みであることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp transport path-mtu-discovery**
5. **end**
6. **show ip bgp neighbors**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	**bgp transport path-mtu-discovery** **例：** `Router(config-router)# bgp transport path-mtu-discovery`	すべての BGP セッションに対して TCP の PMTUD をイネーブルにします。
ステップ 5	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show ip bgp neighbors** **例：** `Router# show ip bgp neighbors`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、すべてのネイバーが TCP の PMTUD をイネーブルにしたことを表示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次の **show ip bgp neighbors** コマンドの出力例は、TCP の PMTUD が BGP ネイバーに対してイネーブルになっていることを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD がイネーブルであることを示します。

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
```

```
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化

外部 BGP（eBGP）ネイバーを持つピアリング セッションを確立してから BGP ネイバー セッションに対して TCP の PMTUD をイネーブルにするには、次の作業を実行します。**neighbor transport** コマンドは、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで使用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]}
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**}
8. **end**
9. **show ip bgp neighbors** [*ip-address*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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	**address-family** {**ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]} **例：** `Router(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **例：** `Router(config-router-af)# neighbor 192.168.2.2 remote-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.2 activate`	このネイバーを IPv4 アドレス ファミリの下でアクティブ化します。 • この例では、eBGP ネイバー 192.168.2.2 がアクティブ化されます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery**} **例：** `Router(config-router-af)# neighbor 192.168.2.2 transport path-mtu-discovery`	単一の BGP ネイバーに対して TCP の PMTUD をイネーブルにします。 • この例では、TCP の PMTUD が eBGP ネイバー 192.168.2.2 に対してイネーブルにされます。
ステップ 8	**end** **例：** `Router(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip bgp neighbors** [*ip-address*] **例：** `Router# show ip bgp neighbors 192.168.2.2`	（任意）ネイバーへの TCP 接続および BGP 接続の情報を表示します。 • この例では、このコマンドの出力は、ネイバー 192.168.2.2 が TCP の PMTUD をイネーブルにしたことを示します。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

show ip bgp neighbors コマンドの次の出力例は、TCP の PMTUD が BGP ネイバー 192.168.2.2 に対してイネーブルにされたことを示します。この出力の 2 つのエントリ（Transport(tcp) path-mtu-discovery is enabled および path mtu capable）は、TCP の PMTUD がイネーブルであることを示します。

```
Router# show ip bgp neighbors 192.168.2.2

BGP neighbor is 192.168.2.2,  remote AS 50000, external link
  BGP version 4, remote router ID 10.2.2.99
```

```
.
.
.
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 192.168.2.2
  Address tracking requires at least a /24 route to the peer
  Connections established 2; dropped 1
  Last reset 00:05:11, due to User reset
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 210 ms, RTTO: 904 ms, RTV: 694 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

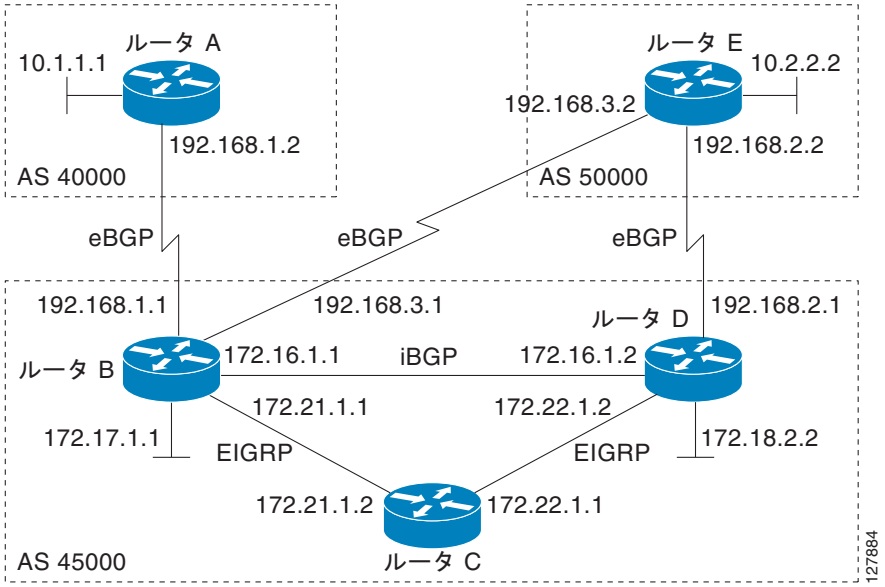
サブネット範囲を使用する BGP ダイナミック ネイバーの実装

Cisco IOS Release 12.2(33)SXH では、BGP ダイナミック ネイバーに対するサポートが導入されました。サブネット範囲を使用する BGP ネイバーのダイナミックな作成を実装するには、次の作業を実行します。

この作業では、BGP ピア グループが図 1 のルータ B に作成され、ダイナミック BGP ネイバー数に関してグローバル制限が設定されて、サブネット範囲がピア グループに関連付けられます。サブネット範囲を設定すると、ダイナミック BGP ネイバー プロセスがイネーブルになります。ピア グループがローカル ルータの BGP ネイバー テーブルに追加され、代替自律システム番号も設定されます。ピア グループは、IPv4 アドレス ファミリの下でアクティブ化されます。

次の手順では、別のルータ（図 1 のルータ E）に移動します。ここで、BGP セッションが開始され、隣接ルータであるルータ B がリモート BGP ピアとして設定されます。このピアリング設定は、TCP セッション（192.168.3.2）を開始する IP アドレスがダイナミック BGP ピアに対して設定されたサブネット範囲内にあるため、TCP セッションを開き、ルータ B にダイナミック BGP ネイバーを作成させます。この作業では、最初のルータであるルータ B に戻り、ダイナミック BGP ピア情報を表示するように変更された 3 つの **show** コマンドが実行されます。

図 1　BGP ダイナミック ネイバー トポロジ



前提条件

この作業では、Cisco IOS Release 12.2(33)SXH、またはこれ以降のリリースが実行中である必要があります。

制約事項

この作業は、IPv4 BGP ピアリングだけをサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **neighbor** *peer-group-name* **peer-group**
6. **bgp listen** [**limit** *max-number*]
7. **bgp listen** [**limit** *max-number* | **range** *network/length***peer-group** *peer-group-name*]
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
9. **neighbor** *peer-group-name***remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
10. **address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]]
11. **neighbor** {*ip-address* | *peer-group-name*} **activate**
12. **end**
13. この作業で設定された BGP ピア グループのサブネット範囲内にインターフェイスを持つ別のルータに移動します。

14. **enable**
15. **configure terminal**
16. **router bgp** *autonomous-system-number*
17. **neighbor** *peer-group-name***remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*]
18. 最初のルータに戻ります。
19. **show ip bgp summary**
20. **show ip bgp peer-group**
21. **show ip bgp neighbors** [*ip-address*]

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：** `RouterB> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。 • この設定はルータ B に入力されます。
ステップ 2	**configure terminal** **例：** `RouterB# 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-number* **例：** `RouterB(config)# router bgp 45000`	指定されたルーティング プロセスでルータ 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 log-neighbor-changes** **例：** `RouterB(config-router)# bgp log-neighbor-changes`	（任意）BGP ネイバー ステータスの変更（アップまたはダウン）およびネイバーのリセットのロギングをイネーブルにします。 • このコマンドは、ネットワーク接続の問題のトラブルシューティングと、ネットワークの安定性の測定に使用します。予期しないネイバーのリセットは、ネットワークでのエラー率が高いことまたはパケット損失が高いことを示す場合があり、調査する必要があります。
ステップ 5	**neighbor** *peer-group-name* **peer-group** **例：** `RouterB(config-router)# neighbor group192 peer-group`	BGP ピア グループを作成します。 • この例では、グループ 192 という名前のピア グループが作成されます。このグループは、受信範囲グループとして使用されます。

	コマンドまたはアクション	目的
ステップ 6	**bgp listen** [**limit** *max-number*] **例：** `RouterB(config-router)# bgp listen limit 200`	BGP ダイナミック サブネット範囲ネイバーのグローバル制限を設定します。 • オプションの **limit** キーワードおよび *max-number* 引数を使用して、作成可能な BGP ダイナミック サブネット範囲ネイバーの最大数を定義します。 • この例では、作成可能なダイナミック ネイバーの最大数は、200 です。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細な構文については、ステップ 7 を参照してください。
ステップ 7	**bgp listen** [**limit** *max-number* | **range** *network/length* **peer-group** *peer-group-name*] **例：** `RouterB(config-router)# bgp listen range 192.168.0.0/16 peer-group group192`	サブネット範囲を BGP ピア グループと関連付け、BGP ダイナミック ネイバー機能をアクティブにします。 • オプションの **limit** キーワードおよび *max-number* 引数を使用して、作成可能な BGP ダイナミック ネイバーの最大数を定義します。 • オプションの **range** キーワードおよび *network/length* 引数を使用して、指定したピア グループに関連付けられるプレフィクス範囲を定義します。 • この例では、プレフィクス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲グループに関連付けられます。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] **例：** `RouterB(config-router)# neighbor group192 ebgp-multihop 255`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 9	**neighbor** *peer-group-name* **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] **例：** `RouterB(config-router)# neighbor group192 remote-as 40000 alternate-as 50000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • オプションの **alternate-as** キーワードおよび *autonomous-system-number* 引数を使用して、受信範囲ネイバーに対して最大 5 つの代替自律システム番号を特定します。 • この例では、グループ 192 という名前のピア グループが 2 つの可能な自律システム番号とともに設定されます。 **（注）** **alternate-as** キーワードは、受信範囲ピア グループだけとともに使用され、個別の BGP ネイバーとは使用されません。
ステップ 10	**address-family ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*]] **例：** `RouterB(config-router)# address-family ipv4 unicast`	アドレス ファミリ コンフィギュレーション モードを開始して、アドレス ファミリ固有の設定を受け入れるよう BGP ピアを設定します。 • この例では、IPv4 ユニキャスト アドレス ファミリ セッションを作成します。

	コマンドまたはアクション	目的
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **activate** **例：** `RouterB(config-router-af)# neighbor group192 activate`	設定されたアドレス ファミリに対してネイバーまたは受信範囲ピア グループをアクティブにします。 • この例では、ネイバー 172.16.1.1 が IPv4 アドレス ファミリに対してアクティブにされます。 **（注）** 通常、BGP ピア グループは、このコマンドを使用してアクティブにできませんが、受信範囲ピア グループは特別です。
ステップ 12	**end** **例：** `RouterB(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 13	この作業で設定された BGP ピア グループのサブネット範囲内にインターフェイスを持つ別のルータに移動します。	—
ステップ 14	**enable** **例：** `RouterE> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。 • この設定はルータ E に入力されます。
ステップ 15	**configure terminal** **例：** `RouterE# 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 16	**router bgp** *autonomous-system-number* **例：** `RouterE(config)# router bgp 50000`	指定されたルーティング プロセスでルータ コンフィギュレーション モードを開始します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number...*] **例：** `RouterE(config-router)# neighbor 192.168.3.1 remote-as 45000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • この例では、ルータ E のインターフェイス（図 1 の 192.168.3.2）が BGP 受信範囲グループであるグループ 192 用に設定されたサブネット範囲とともにあります。TCP がルータ B のピアに対してセッションを開くと、ルータ B はこのピアをダイナミックに作成します。
ステップ 18	最初のルータに戻ります。	—
ステップ 19	**show ip bgp summary** **例：** `RouterB# show ip bgp summary`	（任意）BGP ネイバーへのすべての接続の BGP パス、プレフィクス、およびアトリビュート情報を表示します。 • この手順では、この設定はルータ B に戻っています。

	コマンドまたはアクション	目的
ステップ 20	**show ip bgp peer-group** [*peer-group-name*] [**summary**] **例：** `RouterB# show ip bgp peer-group group192`	（任意）BGP ピア グループの情報を表示します。 • この例では、受信範囲グループであるグループ 192 の情報が表示されます。
ステップ 21	**show ip bgp neighbors** [*ip-address*] **例：** `RouterB# show ip bgp neighbors 192.168.3.2`	（任意）ネイバーへの BGP 接続および TCP 接続の情報が表示されます。 • この例では、ダイナミックに作成されたネイバー 192.168.3.2 の情報が表示されます。この BGP ネイバーの IP アドレスは、**show ip bgp summary** コマンドまたは **show ip bgp peer-group** コマンドの出力にあります。 **（注）** この例では、この作業に適用される構文だけが使用されます。詳細については、『*Cisco IOS IP Routing: BGP Command Reference*』を参照してください。

例

次に示す出力例は、この作業の適切な設定手順がルータ B とルータ E の両方で完了した後に、図 1 のルータ B から取得されました。

show ip bgp summary コマンドの次の出力は、BGP ネイバー 192.168.3.2 がダイナミックに作成され、この受信範囲グループであるグループ 192 のメンバであることを示します。この出力は、IP プレフィクス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲に定義されることも示します。

```
Router# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

show ip bgp peer-group コマンドの次の出力は、この作業で設定された受信範囲グループであるグループ 192 の情報を示します。

```
Router# show ip bgp peer-group group192

BGP peer-group is group192,  remote AS 40000
  BGP peergroup group192 listen range group members:
  192.168.0.0/16
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP neighbor is group192, peer-group external, members:
  *192.168.3.2
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
```

show ip bgp neighbors コマンドの次の出力例は、ネイバー 192.168.3.2 がこのピア グループであるグループ 192 のメンバで、このピアがダイナミックに作成されたことを示すサブセット範囲グループ 192.168.0.0/16 に属していることを示します。

```
Router# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

BGP ネイバー セッション オプションの設定例

ここでは、次の設定例について説明します。

BGP ネイバー の高速セッションの非アクティブ化の設定：例

次の例では、BGP ルーティング プロセスがルータ A およびルータ B で設定され、この 2 つのルータ間でネイバー セッションの高速ピアリング セッションの非アクティブ化をモニタし、使用します。高速ピアリング セッションの非アクティブ化は、このネイバー セッションの両方のルータで必要ではありませんが、このネイバー セッションが無効にされている場合、両方の自律システムの BGP ネットワークのより高速なコンバージェンスに役立ちます。

ルータ A

```
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 neighbor 192.168.1.1 fall-over
 end
```

ルータ B

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

高速セッション非アクティブ化の選択的アドレス トラッキングの設定：例

次に、/28 のプレフィクスを持つルートまたはピアの宛先へのさらに特定されたルートを使用できなくなった場合に、BGP ピアリング セッションをリセットするようにこのセッションを設定する方法の例を示します。

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 end
```

最大プレフィクス制限設定後のセッションの再起動：例

次の例では、ネイバー 192.168.6.6 で許可されるプレフィクスの最大数が 2000 に設定され、ピアリング セッションがディセーブルになった場合に、30 分後にそのピアリング セッションを再確立するようにルータが設定されます。

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 2000 restart 30
```

ネットワーク移行のためのデュアル AS ピアリングの設定：例

次に、この機能の設定方法および確認方法の例を示します。

- 「デュアル AS の設定：例」（P.39）
- 「デュアル AS コンフェデレーションの設定：例」（P.39）
- 「Replace-AS の設定：例」（P.40）

デュアル AS の設定：例

次に、この機能を使用して、お客様のネットワークのピアリング環境を中断せずに 2 つの自律システムを結合する方法の例を示します。**neighbor local-as** コマンドを設定して、ルータ 1 で自律システム 40000 と自律システム 45000 を使用してピアリング セッションを維持できるようにします。ルータ 2 は、BGP ルーティング プロセスを自律システム 50000 で実行するお客様のルータで、自律システム 45000 を持つピアに対して設定されます。

自律システム 40000（プロバイダーのネットワーク）のルータ 1

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 40000
 no synchronization
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
 neighbor 10.3.3.33 local-as 45000 no-prepend replace-as dual-as
```

自律システム 45000（プロバイダーのネットワーク）のルータ 1

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 45000
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
```

自律システム 50000（お客様のネットワーク）のルータ 2

```
interface Serial3/0
 ip address 10.3.3.33 255.255.255.0
!
router bgp 50000
 bgp router-id 10.0.0.3
 neighbor 10.3.3.11 remote-as 45000
```

遷移完了後、通常のメンテナンス時間中またはその他のスケジュール済みのダウンタイム中にルータ 50000 の設定を自律システム 40000 を持つピアに対してアップデートできます。

```
 neighbor 10.3.3.11 remote-as 100
```

デュアル AS コンフェデレーションの設定：例

次の例は、前の例のルータ 1 の設定で使用できます。これらの設定の唯一の相違は、ルータ 1 がコンフェデレーションの一部になるように設定されていることです。

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 65534
 no synchronization
 bgp confederation identifier 100
 bgp router-id 10.0.0.11
 neighbor 10.3.3.33 remote-as 50000
 neighbor 10.3.3.33 local-as 45000 no-prepend replace-as dual-as
```

Replace-AS の設定：例

次の例では、プライベート自律システム 64512 を 10.3.3.33 ネイバーに対するアウトバウンド ルーティング アップデートから取り除き、これを自律システム 50000 に置き換えます。

```
router bgp 64512
 neighbor 10.3.3.33 local-as 50000 no-prepend replace-as
```

TTL セキュリティ チェックの設定：例

このセクションの設定例は、TTL セキュリティ チェックに対する BGP サポート機能を設定する方法を示します。

次の例では、**trace** コマンドを使用して、eBGP ピアへのホップ カウントを決定します。このホップ カウント数は、指定されたネイバーに到着するために IP パケットが通過する各ネットワーキング デバイスの出力に表示されます。次の例では、10.1.1.1 ネイバーのホップ カウントは 1 です。

```
Router# trace ip 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1 10.1.1.1 0 msec *  0 msec
```

次の例では、10.1.1.1 ネイバーのホップ カウントを 2 に設定します。*hop-count* 引数が 2 に設定されるため、BGP は、ヘッダーの TTL カウントが 253 以上の IP パケットだけを受け入れます。

```
Router(config-router)# neighbor 10.1.1.1 ttl-security hops 2
```

セッションごとの TCP の PMTUD に対する BGP サポートの設定：例

ここでは、次の設定例について説明します。

- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化：例」（P.40）
- 「単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化：例」（P.41）
- 「すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化：例」（P.41）
- 「単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化：例」（P.41）

すべての BGP セッションに対する TCP の PMTUD のグローバルなディセーブル化：例

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD をディセーブルにする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD がディセーブルになっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  no bgp transport path-mtu-discovery
  end
show ip bgp neighbors
```

単一の BGP ネイバーに対する TCP の PMTUD のディセーブル化：例

次に、外部 BGP（eBGP）ネイバー 192.168.2.2 に対して TCP の PMTUD をディセーブルにする方法の例を示します。

```
enable
configure terminal
 router bgp 45000
  neighbor 192.168.2.2 remote-as 50000
  neighbor 192.168.2.2 activate
  no neighbor 192.168.2.2 transport path-mtu-discovery
  end
show ip bgp neighbors 192.168.2.2
```

すべての BGP セッションに対する TCP の PMTUD のグローバルなイネーブル化：例

次に、すべての BGP ネイバー セッションに対して TCP の PMTUD をイネーブルにする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD がイネーブルになっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  bgp transport path-mtu-discovery
  end
show ip bgp neighbors
```

単一の BGP ネイバーに対する TCP の PMTUD のイネーブル化：例

次に、外部 BGP（eBGP）ネイバー 192.168.2.2 に対して TCP の PMTUD をイネーブルにする方法の例を示します。**show ip bgp neighbors** コマンドを使用して、TCP の PMTUD がイネーブルになっていることを確認します。

```
enable
configure terminal
 router bgp 45000
  neighbor 192.168.2.2 remote-as 50000
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 transport path-mtu-discovery
  end
show ip bgp neighbors 192.168.2.2
```

サブネット範囲を使用する BGP ダイナミック ネイバーの実装：例

Cisco IOS Release 12.2(33)SXH では、BGP ダイナミック ネイバーに対するサポートが導入されました。次の設定例は、サブネット範囲を使用する BGP ダイナミック ネイバーを実装する方法を示します。

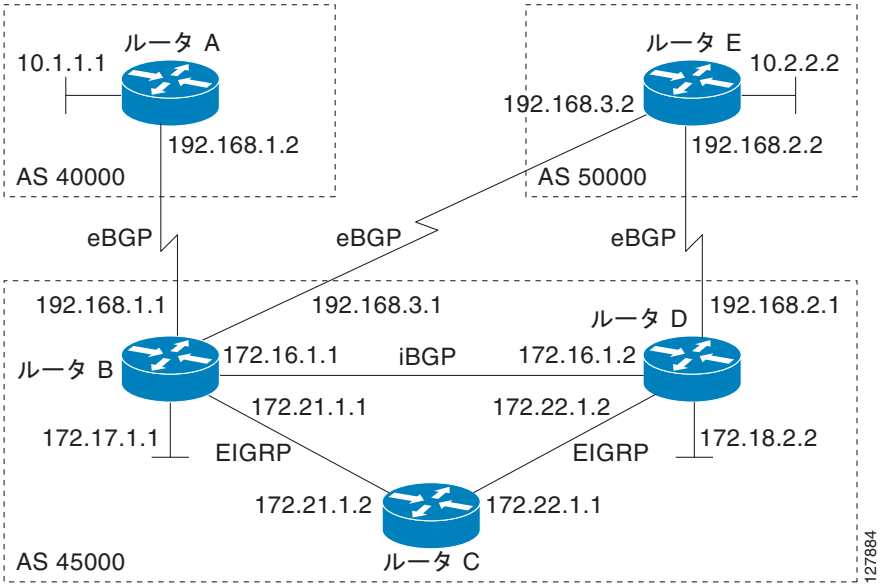
次の例では、2 つの BGP ピア グループが図 2 のルータ B に作成され、ダイナミック BGP ネイバー数に関してグローバル制限が設定され、サブネット範囲がピア グループに関連付けられます。サブネット範囲を設定すると、ダイナミック BGP ネイバー プロセスがイネーブルになります。このピア グループは、ローカル ルータの BGP ネイバー テーブルに追加され、代替自律システム番号もこのピア グループの 1 つであるグループ 192 に設定されます。このサブネット範囲ピア グループおよび標準 BGP ピアは、その後 IPv4 アドレス ファミリの下でアクティブ化されます。

この設定は、別のルータ（図 2 のルータ A）に移動します。ここで、BGP セッションが開始され、隣接ルータであるルータ B がリモート BGP ピアとして設定されます。このピアリング設定は、TCP セッション（192.168.1.2）を開始する IP アドレスがダイナミック BGP ピアに対して設定されたサブネット範囲内にあるため、TCP セッションを開き、ルータ B にダイナミック BGP ネイバーを作成させます。

3 番目のルータ（図 2 のルータ E）もルータ B を持つ BGP ピアリング セッションを開始します。ルータ E は、代替自律システムに設定されている自律システム 50000 にあります。ルータ B は、別のダイナミック BGP ピアを作成することにより、結果として得られた TCP セッションに応答します。

この例は、**show ip bgp summary** コマンドの出力がルータ B に入力されて終了します。

図 2　　BGP ダイナミック ネイバー トポロジ



ルータ B

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 bgp listen limit 200
 bgp listen range 172.21.0.0/16 peer-group group172
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group172 peer-group
 neighbor group172 remote-as 45000
 neighbor group192 peer-group
 neighbor group192 remote-as 40000 alternate-as 50000
 neighbor 172.16.1.2 remote-as 45000
 address-family ipv4 unicast
 neighbor group172 activate
 neighbor group192 activate
 neighbor 172.16.1.2 activate
 end
```

ルータ A

```
enable
configure terminal
router bgp 40000
 neighbor 192.168.1.1 remote-as 45000
 exit
```

ルータ E

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

ルータ A とルータ E の両方が設定された後、**show ip bgp summary** コマンドは、ルータ B で実行されます。この出力は、正規 BGP ネイバー 172.16.1.2 およびルータ A とルータ E がルータ B に対する BGP ピアリングの TCP セッションを開始したときにダイナミックに作成された 2 つの BGP ネイバーを表示します。この出力は、設定された受信範囲サブネット グループに関する情報も表示します。

```
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.2      4 45000      15      15        1    0    0 00:12:20        0
*192.168.1.2    4 40000       3       3        1    0    0 00:00:37        0
*192.168.3.2    4 50000       6       6        1    0    0 00:04:36        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 2/(200 max), Subnet ranges: 2

BGP peergroup group172 listen range group members:
  172.21.0.0/16
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

次の作業

- 外部サービス プロバイダーに接続して、他の外部 BGP 機能を使用するには、「Connecting to a Service Provider Using External BGP」モジュールを参照してください。
- 一部の内部 BGP 機能を設定するには、『*Cisco IOS IP Routing Protocols Configuration Guide*』の BGP セクションで、「Configuring Internal BGP Features」の章を参照してください。
- BGP ネクストホップ アドレス トラッキングやルート ダンプニングなどの BGP の拡張機能の一部を設定する場合は、「Configuring Advanced BGP Features」モジュールを参照してください。

参考資料

ここでは、BGP の拡張機能の設定に関連する参考資料について説明します。

関連資料

関連項目	参照先
BGP コマンド：コマンド構文の詳細、コマンド モード、デフォルト、コマンド履歴、使用上の注意事項、および例	『*Cisco IOS IP Routing: BGP Command Reference*』
Cisco BGP のコンセプト情報の概要と各 BGP モジュールへのリンク	「Cisco BGP Overview」モジュール
BGP の基本作業のコンセプトと設定の詳細。	「Configuring a Basic BGP Network」モジュール
高度な BGP 作業の概念および設定の詳細	「Configuring Advanced BGP Features」モジュール

規格

規格	タイトル
MDT SAFI	MDT SAFI

MIB

MIB	MIB リンク
CISCO-BGP4-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1191	『*Path MTU Discovery*』
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1773	『*Experience with the BGP Protocol*』
RFC 1774	『*BGP-4 Protocol Analysis*』
RFC 1930	『*Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2918	『*Route Refresh Capability for BGP-4*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

BGP ネイバー セッションのオプション設定の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。Cisco IOS リリース 12.2(1)、12.0(3)S、12.2(33)SRA、12.2(31)SB、12.2(33)SXH、またはこれら以降のリリースで導入または変更された機能だけがこのテーブルに表示されます。

このテクノロジーの機能でここに記載されていないものについては、『Cisco BGP Features Roadmap』を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　BGP ネイバー セッションのオプション機能設定の機能情報

機能名	リリース	機能の設定情報
BGP ダイナミック ネイバー	12.2(33)SXH 15.0(1)S	BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。各範囲は、サブネット IP アドレスとして設定できます。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。サブネットの範囲が BGP ピア グループに対して設定され、TCP セッションがそのサブネットの範囲の IP アドレスに対して開始された後、新しい BGP ネイバーがそのグループのメンバとしてダイナミックに作成されます。この新しい BGP ネイバーは、ピア グループのすべての設定を継承します。3 つの **show** コマンドの出力は、ダイナミック ネイバーに関する情報を表示するようにアップデートされています。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ダイナミック ネイバー」（P.8） • 「サブネット範囲を使用する BGP ダイナミック ネイバーの実装」（P.31） • 「サブネット範囲を使用する BGP ダイナミック ネイバーの実装：例」（P.41） 次のコマンドがこの機能によって導入または変更されました。**bgp listen**、**debug ip bgp range**、**neighbor remote-as**、**show ip bgp neighbors**。**show ip bgp peer-group**、**show ip bgp summary**。
最大プレフィクス制限後の BGP 再起動セッション	12.0(22)S 12.2(15)T 12.2(18)S 15.0(1)S	最大プレフィクス制限後の BGP 再起動セッション機能により、**restart** キーワードが導入されて、**neighbor maximum-prefix** コマンドの機能が拡張されます。この機能拡張により、ネットワーク オペレータは、ピアから受信したプレフィクス数が最大プレフィクス制限を超えたときに、ピアリング セッションが別のルータによって再確立される時間間隔を設定できます。 次のセクションで、この機能に関する情報を参照できます。 • 「最大プレフィクス到達後の BGP ネイバー セッションの再起動」（P.3） • 「最大プレフィクス制限を超えた後にネイバー セッションを再確立するためのルータの設定」（P.12） • 「最大プレフィクス制限設定後のセッションの再起動：例」（P.38） 次のコマンドが変更されました。**neighbor maximum-prefix**、**show ip bgp neighbors**。

表 1　BGP ネイバー セッションのオプション機能設定の機能情報 （続き）

機能名	リリース	機能の設定情報
BGP の選択的アドレス トラッキング	12.4(4)T 12.2(31)SB 12.2(33)SRB	BGP の選択的アドレス トラッキング機能によって、ネクストホップ ルート フィルタリングと高速なセッション非アクティブ化にルート マップが使用されるようになりました。選択的ネクストホップ フィルタリングは、ルート マップを使用して、BGP ネクストホップの解決に役立つルートを選択的に定義します。または、ルート マップを使用して、BGP ピアへのルートの変更時に BGP ネイバーとのピアリング セッションをリセットする必要があるかどうかを判別できます。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP 高速セッションの非アクティブ化の選択的アドレス トラッキング」（P.3） • 「高速セッションの非アクティブ化の選択的アドレス トラッキングの設定」（P.10） • 「高速セッション非アクティブ化の選択的アドレス トラッキングの設定：例」（P.38） この機能によって、**bgp nexthop** コマンドおよび **neighbor fall-over** コマンドが変更されました。

表 1　BGP ネイバー セッションのオプション機能設定の機能情報 （続き）

機能名	リリース	機能の設定情報
4 バイト ASN に対する BGP サポート	12.0(32)S12 12.0(32)SY8 12.0(33)S3 12.2(33)SRE 12.2(33)XNE 12.2(33)SXI1 12.4(24)T 15.0(1)S	4 バイト ASN に対する BGP サポート機能により、4 バイト自律システム番号がサポートされるようになりました。自律システム番号の要求の増加に伴い、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 バイト自律システム番号の割り当てを開始します。 Cisco IOS Release 12.0(32)SY8、12.0(33)S3、12.2(33)SRE、12.2(33)XNE、および 12.2(33)SXI1 では、4 バイト自律システム番号の Cisco による実装は、自律システム番号のデフォルトの正規表現一致および出力表示形式として asplain 形式を使用しますが、RFC 5396 で説明されているように、4 バイト自律システム番号を asplain 形式と asdot 形式の両方に設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドを使用します。 Cisco IOS Release 12.0(32)S12 および 12.4(24)T では、4 バイト自律システム番号の設定形式、正規表現マッチング、出力表示の実装として、シスコは asdot だけを使用しており、asplain はサポートされていません。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネットワーク自律システムの移行」（P.4） この機能により、次の各コマンドが追加または変更されています。**bgp asnotation dot**、**bgp confederation identifier**、**bgp confederation peers**、自律システム番号を設定するすべての **clear ip bgp** コマンド、**ip as-path access-list**、**ip extcommunity-list**、**match source-protocol**、**neighbor local-as**、**neighbor remote-as**、**neighbor soo**、**redistribute** (IP)、**router bgp**、**route-target**、**set as-path**、**set extcommunity**、**set origin**、**soo**、自律システム番号を表示するすべての **show ip bgp** コマンド、および **show ip extcommunity-list**。

表 1　BGP ネイバー セッションのオプション機能設定の機能情報 （続き）

機能名	リリース	機能の設定情報
ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート	12.0(27)S 12.2(25)S 12.3(11)T 12.2(33)SRA 12.2(33)SXH 15.0(1)S	ネットワーク AS 移行に対するデュアル AS 設定に対する BGP サポート機能により、自律システム パスのカスタマイズ設定オプションが追加され、BGP Local-AS 機能が拡張されます。この機能の設定は、お客様のピアリング セッションに対して透過的で、お客様のピアリング環境を中断せずにプロバイダーが 2 つの自律システムを結合することを可能にします。お客様のピアリング セッションは、その後メンテナンス時間中またはその他のスケジュール済みのダウンタイム中に更新できます。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネットワーク自律システムの移行」（P.4） • 「ネットワーク移行のためのデュアル AS ピアリングの設定」（P.16） • 「ネットワーク移行のためのデュアル AS ピアリングの設定：例」（P.38） 次のコマンドがこの機能によって変更されました。**neighbor local-as**。
高速ピアリング セッションの非アクティブ化に対する BGP サポート	12.0(29)S 12.3(14)T 12.2(33)SRA 12.2(31)SB 12.2(33)SXH 15.0(1)S	高速ピアリング セッションの非アクティブ化に対する BGP サポート機能により、イベントによって起動される通知システムが導入され、ボーダー ゲートウェイ プロトコル（BGP）プロセスでネイバーごとに BGP ピアリング セッションをモニタできるようになりました。この機能により、BGP が隣接変更を検出し、標準の BGP スキャン間隔中に終了したセッションを無効にできるようになり、BGP の隣接変更に対する応答時間が向上します。この機能をイネーブルにすると、BGP コンバージェンス全体が向上します。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP の高速ピアリング セッションの非アクティブ化」（P.3） • 「BGP ネイバー の高速セッションの非アクティブ化の設定」（P.9） • 「BGP ネイバー の高速セッションの非アクティブ化の設定：例」（P.38） 次のコマンドがこの機能によって変更されました。**neighbor fall-over**。

表 1　BGP ネイバー セッションのオプション機能設定の機能情報 （続き）

機能名	リリース	機能の設定情報
セッションごとの TCP の PMTUD に対する BGP サポート	12.2(33)SRA 12.2(31)SB 12.2(33)SXH 12.4(20)T 15.0(1)S	伝送制御プロトコル（TCP）の Path MTU Discovery（PMTUD）に対するボーダー ゲートウェイ プロトコル（BGP）のサポートにより、各 BGP セッションに対する最良 TCP の Path MTU を BGP が自動的に検出する機能が導入されました。この TCP の Path MTU はすべての BGP ネイバー セッションに対してデフォルトでイネーブルになりますが、すべての BGP セッションに対してグローバルにまたは個別の BGP ネイバー セッションに対してディセーブルにでき、その後イネーブルにできます。 次のセクションで、この機能に関する情報を参照できます。 • 「セッションごとの TCP Path 最大伝送ユニット（MTU）Discovery に対する BGP サポート」（P.7） • 「セッションごとの TCP の PMTUD に対する BGP サポートの設定」（P.22） • 「セッションごとの TCP の PMTUD に対する BGP サポートの設定：例」（P.40） 次のコマンドがこの機能によって導入または変更されました。**bgp transport**、**neighbor transport**、**show ip bgp neighbors**。
TTL セキュリティ チェックに対する BGP サポート	12.0(27)S 12.3(7)T 12.2(25)S 12.2(18)SXE 15.0(1)S	TTL セキュリティ チェックに対する BGP サポート機能により、簡単なセキュリティ メカニズムが導入され、external Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）ピアリング セッションを偽造 IP パケットを使用する CPU 利用率に基づく攻撃から防御します。この機能をイネーブルにすると、どちらの BGP ネットワークの一部でもないネットワーク セグメント上のホストまたは eBGP ピア間にないネットワーク セグメント上のホストによる eBGP ピアリング セッションを乗っ取ろうとする試みを防ぐことができます。 次のセクションで、この機能に関する情報を参照できます。 • 「BGP ネイバー セッションの TTL セキュリティ チェック」（P.5） • 「BGP ネイバー セッションの TTL セキュリティ チェックの設定」（P.18） • 「TTL セキュリティ チェックの設定：例」（P.40） 次のコマンドがこの機能によって導入または変更されました。**neighbor ttl-security**、**show ip bgp neighbors**。