



ルーティングポリシーの設定



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

この章は次のトピックで構成されています。

- [Cisco IOS ルータにおける BGP ルーティング](#) (1 ページ)
- [\[BGP\] ルーティング ポリシー ページ](#) (5 ページ)
- [Cisco IOS ルータにおける EIGRP ルーティング](#) (10 ページ)
- [\[EIGRP\] ルーティング ポリシー ページ](#) (16 ページ)
- [Cisco IOS ルータにおける OSPF ルーティング](#) (25 ページ)
- [\[OSPF Interface\] ポリシー ページ](#) (38 ページ)
- [\[OSPF Process\] ポリシー ページ](#) (44 ページ)
- [Cisco IOS ルータにおける RIP ルーティング](#) (54 ページ)
- [\[RIP\] ルーティング ポリシー ページ](#) (58 ページ)
- [Cisco IOS ルータにおけるスタティック ルーティング](#) (64 ページ)
- [\[Static Routing\] ポリシー ページ](#) (66 ページ)

Cisco IOS ルータにおける BGP ルーティング



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

BGP は、Autonomous System (AS; 自律システム) 間でのルーティング情報のループフリー交換を保証する Exterior Gateway Protocol (EGP; エクステリア ゲートウェイ プロトコル) です。BGP システムの主要な機能は、到達可能なネットワークに関する情報 (AS パス情報など) を他の BGP システムと交換することです。この情報を使用して AS 接続のグラフを作成できま

す。このグラフを使用して、ルーティンググループを排除し、AS レベルのポリシーを決定できます。

BGP は、インターネット上で使用されるルーティングプロトコルであり、インターネットサービスプロバイダー間で一般的に使用されています。このレベルでスケーラビリティを実現するために、BGP は複数のルートパラメータ（属性）を使用して、ルーティングポリシーを定義し、安定したルーティング環境を維持します。また、BGP は Classless InterDomain Routing（CIDR）を使用して、インターネットルーティングテーブルのサイズを大幅に削減しています。

BGP ルートは、ネットワーク番号、情報が通過した AS のリスト（自律システムパスと呼ばれる）、および定義されたパス属性で構成されます。

BGP ルータは、ネイバーとして定義されたルータだけとルーティング情報を交換します。BGP ネイバーは、ルータ間で TCP 接続が確立されたときに、完全なルーティング情報を交換します。更新は、ルーティングテーブルの変更が検出された場合にだけネイバーに送信されます。BGP ルータでは、定期的な更新は送信されません。

ここでは、BGP ルーティングポリシーを作成するために実行するタスクについて説明します。

- [BGP ルートの定義（2 ページ）](#)
- [BGP へのルートの再配布（4 ページ）](#)



（注） Security Manager では、RFC 1163、1267、および 1771 で規定されているバージョン 2、3、および 4 の BGP がサポートされます。

関連項目

- [Cisco IOS ルータにおけるスタティックルーティング（64 ページ）](#)
- [Cisco IOS ルータにおける RIP ルーティング（54 ページ）](#)
- [Cisco IOS ルータにおける OSPF ルーティング（25 ページ）](#)
- [Cisco IOS ルータにおける EIGRP ルーティング（10 ページ）](#)

BGP ルートの定義

BGP ルーティングポリシーを設定する場合は、すべての EGP と同様に、ルータとそのネイバーとの関係を定義する必要があります。BGP では、内部（同じ AS 内に配置）と外部（異なる AS 内に配置）という 2 種類のネイバーがサポートされます。通常、外部ネイバーは相互に隣接しており、サブネットを共有しています。内部ネイバーは同じ AS 内の任意の場所に存在できます。

また、次のオプション機能をイネーブルにするかどうかを選択できます。

- 自動サマライズ

- 同期
- ネイバー ロギング

自動サマライズを有効にすると、OSPF や EIGRP などの内部ゲートウェイプロトコル (IGP) から BGP にサブネットが再配布されるときに、ネットワークルートだけが挿入されます。同期は、1つの AS から別の AS にトラフィックを渡す媒介として AS が機能する場合に役立ちます。同期によって、アドバタイズするルートに関して AS の一貫性が確保されるためです。たとえば、ネットワーク内のすべてのルータが IGP を介してルートを学習する前に BGP がルートをアドバタイズすると、一部のルータでまだルーティングできないトラフィックを AS が受信する可能性があります。ネイバーロギングでは、BGP ネイバーがリセットされた場合、到達不能になった場合、またはネットワークへの接続を復元した場合に、ルータは BGP ネイバーによって発行されたメッセージを追跡できます。

ここでは、BGP ルートを定義する方法について説明します。各ルータで定義できる BGP ルートは 1 つだけです。

関連項目

- [BGP へのルートの再配布 \(4 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択し、作業領域の [セットアップ (Setup)] タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ (Setup)] タブをクリックします。

BGP の [Setup] が表示されます。このタブのフィールドの説明については、[表 1 : BGP の \[Setup\] タブ \(6 ページ\)](#) を参照してください。

ステップ 2 BGP の [Setup] タブで、ルータが属する AS 番号を入力します。

ステップ 3 (任意) この AS に対してローカルなネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用できます。または [選択 (Select)] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。

ステップ 4 ルータの外部および内部 BGP ネイバーを定義します。

- a) [ネイバー (Neighbors)] の下にある [追加 (Add)] をクリックして、[BGP ネイバー (BGP Neighbors)] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、[表 2 : \[Neighbors\] ダイアログボックス \(8 ページ\)](#) を参照してください。
- b) AS 番号を入力し、[選択 (Select)] をクリックして、定義されている AS 内のネイバーであるホストを選択します。内部ネイバーはルータと同じ AS 内に配置されており、外部ネイバーは異なる AS 内に配置されています。

- c) [OK] をクリックして定義を保存し、[BGPネイバー (BGP Neighbors)] ダイアログボックスに戻ります。
- d) (任意) [4.b \(3 ページ\)](#) ~ [4.c \(4 ページ\)](#) を繰り返して、その他の AS 内のネイバーを定義します。

(注) BGP ネイバーを定義する場合、IP アドレスは選択したルータのインターフェイスに属することができません。また、複数の AS に同じ IP アドレスは定義できません。

終了したら、[BGPネイバー (BGP Neighbors)] ダイアログボックスの[OK]をクリックして[BGPのセットアップ (BGP Setup)] タブに戻ります。選択内容が [Neighbors] フィールドに表示されます。

ステップ 5 (任意) [Auto-Summary] チェックボックスをオンにして、自動サマライズをイネーブルにします。自動サマライズをイネーブルにすると、サブネットが IGP (OSPF や EIGRP など) から BGP に再配布されるときに、ネットワーク ルートだけが BGP テーブルに注入されます。

ステップ 6 (任意) [同期 (Synchronization)] チェックボックスをオンにして、BGP を IGP と同期します。この機能をイネーブルにすると、BGP は、IGP がルーティング情報を AS 全体に伝播するまで待機します。

AS が 1 つの AS から受信したトラフィックを別の AS に渡さない場合、または AS 内のすべてのルータが BGP を実行している場合、同期は必要ありません。同期をディセーブルにすると、BGP の収束が速くなります。

ステップ 7 (任意) [ネイバーのロギング (Log-Neighbor)] チェックボックスをオンにして、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のロギングをイネーブルにします。

BGP へのルートの再配布

再配布とは、BGP などのルーティングプロトコルを使用して、他の方法 (別のルーティングプロトコルなど) で学習されたルート、スタティックルート、または直接接続されたルートをアドバタイズすることです。たとえば、OSPF ルーティングプロトコルから BGP 自律システム (AS) にルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベースルーティングプロトコルに適用できます。

はじめる前に

- BGP AS を定義します。 [BGP ルートの定義 \(2 ページ\)](#) を参照してください。

関連項目

- [BGP ルートの定義 \(2 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択し、作業領域の [再配布 (Redistribution)] タブをクリックします。

- (ポリシービュー) ポリシータイプセレクトから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布 (Redistribution)] タブをクリックします。

BGP の [Redistribution] タブが表示されます。このタブのフィールドの説明については、[表 3 : BGP の \[Redistribution\] タブ \(9 ページ\)](#) を参照してください。

ステップ 2 BGP の [再配布 (Redistribution)] タブで、[BGP 再配布マッピング (BGP Redistribution Mappings)] テーブルから行を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックしてマッピングを作成します。[BGP Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 4 : \[BGP Redistribution Mapping\] ダイアログボックス \(10 ページ\)](#) を参照してください。

ステップ 3 BGP にルートを再配布するプロトコルを選択します。

(注) スタティックルート、RIP ルート、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 4 (任意) 再配布されたルートのデフォルトのメトリック (コスト) を修正します。メトリックによって、ルートのプライオリティが決まります。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、BGP の [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

[BGP] ルーティングポリシー ページ

ボーダー ゲートウェイ プロトコル (BGP) は、複数の自律システムまたはドメイン間でルーティングを実行し、ルーティングおよび到着可能性情報を他の BGP システムと交換する Exterior Gateway Protocol (EGP; エクステリア ゲートウェイ プロトコル) です。BGP は、インターネット上でルーティング情報を交換するために使用され、インターネット サービス プロバイダー間で使用されるプロトコルです。

[BGP] ルーティング ページの次のタブから、BGP ルーティング ポリシーを設定できます。

- [\[BGP\] ページ - \[Setup\] タブ \(6 ページ\)](#)
- [\[BGP\] ページ - \[Redistribution\] タブ \(8 ページ\)](#)

詳細については、[Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#) を参照してください。

ナビゲーションパス

- (デバイスビュー) ポリシーセレクトから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択します。
- (ポリシービュー) ポリシータイプセレクトから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [BGP] を選択します。[BGP] を右クリックしてポリシーを作成するか、共有ポリシーセレクトから既存のポリシーを選択します。

[BGP] ページ - [Setup] タブ

BGP の [Setup] タブを使用して、選択したルータが配置されている自律システム (AS) の番号を定義します。次に、AS に含まれるネットワークと、ルータの内部ネイバーおよび外部ネイバーであるネットワークを定義する必要があります。さらに、BGP と OSPF や EIGRP などの Interior Gateway Protocol (IGP) 間の相互作用を制御するオプションをイネーブルまたはディセーブルにすることができます。3 番目のオプションを使用して、BGP ネイバーからのメッセージのログギングをイネーブルにします。

ナビゲーションパス

[BGP] ルーティングポリシー ページ (5 ページ) に移動し、[セットアップ (Setup)] タブをクリックします。

関連項目

- BGP ルートの定義 (2 ページ)
- [BGP] ページ - [Redistribution] タブ (8 ページ)
- ポリシー定義中の IP アドレスの指定
- ネットワーク/ホストオブジェクトについて

フィールドリファレンス

表 1: BGP の [Setup] タブ

要素	説明
AS 番号 (AS Number)	ルータが配置されている自律システムの数。有効な値の範囲は 1 ~ 65535 です。この番号によって、BGP ルーティングプロセスがイネーブルになります。 BGP がデバイスですでに設定されている場合、この番号を変更して展開することはできません。AS 番号を変更する必要がある場合は、最初に BGP ポリシーの割り当てを解除し、変更を展開し (したがって BGP 設定をデバイスから削除し)、新しい番号で BGP ポリシーを設定して、設定を再展開します。
ネットワーク	BGP ルートに関連付けられるネットワーク。1 つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 (注) ルートからネットワークを削除するには、[ネットワーク (Network)] フィールドからネットワークを選択し、[削除 (Delete)] をクリックします。

要素	説明
ネイバー	ルータの内部ネイバー（ルータと同じ AS 内に配置）および外部ネイバー（異なる AS 内に配置）。 [Neighbors] ダイアログボックス（7 ページ） を参照してください。
自動集約 (Auto-Summary)	<p>選択すると、自動サマライズがイネーブルになります。サブネットが IGP（RIP、OSPF、EIGRP など）から BGP に再配布されるときに、この BGP バージョン 3 機能によってネットワーク ルートだけが BGP テーブルに注入されます。自動サマライズによって、ルータで保持する必要があるルーティングテーブルのサイズと複雑さが低減します。</p> <p>選択解除されている場合、自動サマライズはディセーブルになります。これがデフォルトです。</p>
同期	<p>選択すると、同期がイネーブルになります。この機能を使用して、アドバタイズするルートに関してネットワーク内のすべてのルータの一貫性が確保されるようにします。同期によって、BGP は、IGP がルーティング情報を AS 全体に伝播するまで待機します。</p> <p>選択を解除すると、同期がディセーブルになります。このルータが別の AS からのトラフィックを第三の AS に渡さない場合、または AS 内のすべてのルータが BGP を実行している場合、同期をディセーブルにすることができます。この機能をディセーブルにすると、IGP が伝送する必要があるルートの数が減少し、コンバージェンス時間が向上するという利点があります。これがデフォルトです。</p>
Log-Neighbor	<p>選択すると、BGP ネイバーのリセット、ネットワークへの接続、または切断時に生成されるメッセージのロギングがイネーブルになります。これがデフォルトです。</p> <p>選択を解除すると、メッセージロギングがディセーブルになります。</p>

[Neighbors] ダイアログボックス

[Neighbors] ダイアログボックスを使用して、選択したルータの内部および外部ネイバーを定義します。

ナビゲーションパス

[\[BGP\] ページ - \[Setup\] タブ（6 ページ）](#) に移動してから、[ネイバー (Neighbors)] フィールドにある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [BGP ルートの定義（2 ページ）](#)
- [ポリシー定義中の IP アドレスの指定](#)

- [ネットワーク/ホストオブジェクトについて](#)

フィールド リファレンス

表 2: [Neighbors] ダイアログボックス

要素	説明
AS 番号 (AS Number)	BGP ネイバーを含む AS の番号。内部ネイバーは、選択したルータのネットワークと同じ AS 番号を持ちます。外部ネイバーは、異なる AS 番号を持ちます。
IP アドレス	<p>ルータのネイバーであるホストの IP アドレス。ルーティングテーブルの変更が検出されると常に、BGP ネイバーは相互にルーティング情報を交換します。</p> <p>BGP ネイバーを定義する場合、IP アドレスは選択したルータのインターフェイスに属することができません。また、複数の AS に同じ IP アドレスは定義できません。</p> <p>1つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。</p> <p>(注) BGP ネイバーのリストからホストを削除するには、[ホスト (Hosts)] フィールドからホストを選択し、[削除 (Delete)] をクリックします。</p>

[BGP] ページ - [Redistribution] タブ

BGP の [Redistribution] タブを使用して、BGP 自律システム (AS) への再配布を実行するときの再配布設定を表示、作成、編集、および削除します。



- (注) RIP の [再配布 (Redistribution)] タブにアクセスする前に、RIP 設定パラメータを定義する必要があります。 [\[BGP\] ページ - \[Setup\] タブ \(6 ページ\)](#) を参照してください。

ナビゲーションパス

[\[BGP\] ルーティングポリシー ページ \(5 ページ\)](#) に移動し、[再配布 (Redistribution)] タブをクリックします。

関連項目

- [BGP へのルートの再配布 \(4 ページ\)](#)
- [\[BGP\] ページ - \[Setup\] タブ \(6 ページ\)](#)

- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 3: BGP の [Redistribution] タブ

要素	説明
プロトコル	再配布されているプロトコル。
[AS/プロセスID (AS/Process ID)]	再配布されているルートの AS 番号またはプロセス ID。
メトリック (Metric)	再配布されるルートのプライオリティを決定する値。
一致 (Match)	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
[静的タイプ (Static Type)]	スタティック ルートを再配布する場合、スタティック ルートのタイプ (IP または OSI) を指定します。
[追加 (Add)] ボタン	[BGP Redistribution Mapping] ダイアログボックス (9 ページ) が開きます。ここから、BGP 再配布マッピングを定義できます。
[編集 (Edit)] ボタン	[BGP Redistribution Mapping] ダイアログボックス (9 ページ) が開きます。ここから、選択した BGP 再配布マッピングを編集できます。
[削除 (Delete)] ボタン	選択した BGP 再配布マッピングをテーブルから削除します。

[BGP Redistribution Mapping] ダイアログボックス

[BGP再配布マッピング (BGP Redistribution Mapping)] ダイアログボックスを使用して、BGP 再配布マッピングのプロパティを追加または編集します。

ナビゲーションパス

[\[BGP\] ページ - \[Redistribution\] タブ \(8 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [BGP へのルートの再配布 \(4 ページ\)](#)

フィールドリファレンス

表 4: [BGP Redistribution Mapping] ダイアログボックス

要素	説明
Protocol to Redistribute	<p>再配布されているルーティングプロトコル。</p> <ul style="list-style-type: none"> • [スタティック (Static)] : IP または OSI スタティックルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [EIGRP] : EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに1つのマッピングを定義できます。 • [RIP] : RIP ルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [OSPF] : 別の OSPF プロセスを再配布します。プロセスごとに1つのマッピングを定義できます。表示されるリストからプロセスを選択し、1つ以上の一致基準を選択します。 <ul style="list-style-type: none"> • [Internal] : 特定の AS の内部のルート。 • [External1] : AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1] : AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area (NSSA) ルート。 • [NSAAExternal2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる (NSSA) ルート。 • [Connected] : インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
メトリック (Metric)	再配布されるルートのコストを表す値。有効値の範囲は、0 ~ 4294967295 です。

Cisco IOS ルータにおける EIGRP ルーティング



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

Enhanced Interior Gateway Routing Protocol (EIGRP) は、シスコが開発した、リンクステートプロトコルの機能を統合する拡張距離ベクトル型プロトコルです。EIGRPは、数多くのさまざまなトポロジおよびメディアに適しています。他のルーティングプロトコルとは異なる EIGRP の重要な機能としては、高速コンバージェンスの実現、可変長サブネットマスク、部分的なアップデート、および複数のネットワーク層プロトコルのサポートがあります。

宛先に到達するため、および他のルータにアドバタイズするためにルータが使用するメトリックは、すべてのネイバーから最適にアドバタイズされたメトリックと最適なネイバーへのリンクコストの合計です。

EIGRPはネイバーテーブルを使用して、ルータの各ネイバーに関するアドレスおよびインターフェイス情報を格納します。hello パケットによってホールド時間がアドバタイズされます。これは、ネイバーを到達可能および動作可能と見なすことができる時間です。トポロジテーブルには、ネイバールータでアドバタイズされたすべての宛先が含まれます。アドバタイズされたメトリックがネイバーごとにエントリに記録され、ネイバーによってそのルーティングテーブルに格納されます。

EIGRP を実行しているルータには、代替ルートに迅速に適応できるように、ネイバーすべてのルーティングテーブルが格納されます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP は、ルーティングテーブルの内容全体を送信する代わりに、宛先の状態が変わったときに差分更新を送信します。EIGRP では、情報を必要とするルータだけが更新されます。この機能により、EIGRP パケットに必要な帯域幅が最小限に抑えられます。

EIGRP は、内部ルートと外部ルートの両方をサポートします。内部ルートは、EIGRP 自律システム (AS) 内で発生します。したがって、EIGRP を実行するように設定された直接接続されているネットワークは内部ルートと見なされ、AS 全体にこの情報とともに伝達されます。外部ルートとは、他のルーティングプロトコルによって学習されたルート、またはルーティングテーブルにスタティックルートとして存在するルートです。外部ルートは、生成元の ID によって個別にタグ付けされます。

ここでは、EIGRP ルーティング ポリシーを作成するために実行するタスクについて説明します。

- [EIGRP ルートの定義 \(12 ページ\)](#)
- [EIGRP インターフェイスのプロパティの定義 \(13 ページ\)](#)
- [EIGRP へのルートの再配布 \(15 ページ\)](#)

関連項目

- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)
- [Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

EIGRP ルートの定義

EIGRP ルーティングポリシーを定義するには、各自律システムに番号を割り当てる必要があります。この番号によって、自律システムは他のルータで識別されます。次に、ルートを作成するネットワークを選択する必要があります。さらに、どのインターフェイスが受動かを選択できます。他のルーティングプロトコルとは異なり、EIGRPのパッシブインターフェイスは、ネイバーとの間でルーティング更新を送受信しないため、ネイバー関係が失われます。

EIGRP ルーティングポリシーの設定時に、自動集約を有効にするか決めることもできます。有効にすると、単一のネットワークエントリで多数のサブネットを表すことで、ルーティングテーブルとルーティング情報の交換が大幅に簡素化されます。

関連項目

- [EIGRP インターフェイスのプロパティの定義 \(13 ページ\)](#)
- [EIGRP へのルートの再配布 \(15 ページ\)](#)
- [Cisco IOS ルータにおける EIGRP ルーティング \(10 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [EIGRP]** を選択し、作業領域の **[セットアップ (Setup)]** タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [EIGRP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、**[セットアップ (Setup)]** タブをクリックします。

EIGRP の **[Setup]** タブが表示されます ([\[EIGRP\] ページ : \[セットアップ \(Setup\)\] タブ \(17 ページ\)](#) を参照)。

ステップ 2 EIGRP の **[セットアップ (Setup)]** タブで、テーブルから EIGRP ルートを選択し、**[編集 (Edit)]** をクリックするか、**[追加 (Add)]** をクリックしてルートを作成します。**[EIGRP Setup]** ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 6: \[EIGRP のセットアップ \(EIGRP Setup\)\] ダイアログボックス \(18 ページ\)](#) を参照してください。

ステップ 3 ルートの自律システム番号を入力します。この番号によって、自律システムは他のルータに対して識別されます。

ステップ 4 EIGRP ルートに含めるネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、アドレスをカンマで区切ることができます。**[選択 (Select)]** をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、または新しいネットワーク/ホストオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。

ステップ 5 受動インターフェイスのアドレスを入力します。これは、ネイバーにルーティング更新 (存在する場合) を送信しないインターフェイスです。1 つ以上のインターフェイスの名前またはインターフェイスのロールを入力します。アドレスをカンマで区切ります。**[選択 (Select)]** をクリックして既存のオブジェクトの

リストからインターフェイス名またはロールを選択するか、または新しいインターフェイス ロール オブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#)を参照してください。

ステップ 6 (任意) [自動集約 (Auto-Summary)] をオンにして、ネットワークレベルルートへのサブネットルートの自動集約を有効にします。サマライズによってルーティングテーブルのサイズが削減されるため、ネットワークの複雑さが低減します。

ステップ 7 [OK] をクリックして定義を保存します。EIGRP ルートが、EIGRP の [Setup] タブに表示されるテーブルに表示されます。

EIGRP インターフェイスのプロパティの定義

任意で、選択した EIGRP 自律システムの次の 2 つのインターフェイス プロパティのデフォルト値を変更できます。

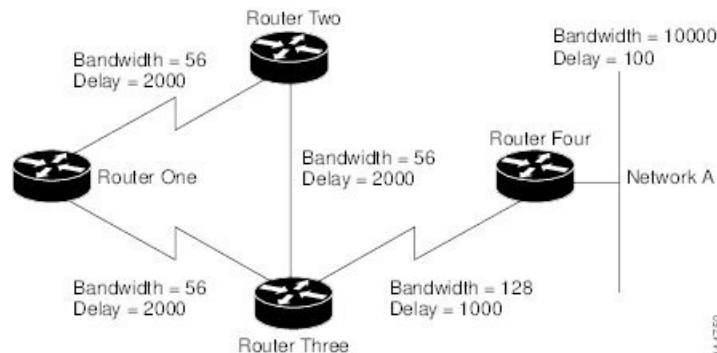
- hello 間隔
- スプリット ホライズン。

hello 間隔によって、hello パケット間の間隔が定義されます。ルーティング デバイスは、これらのパケットを相互に定期的に送信して、直接接続されたネットワーク上の他のルータについて動的に学習します。この情報は、ネイバーを検出したり、ネイバーが到達不能または動作不能になったことを学習したりするために使用されます。デフォルトでは、hello パケットは 5 秒間隔で送信されます。低速 (T1 以下) の NonBroadcast MultiAccess (NBMA; 非ブロードキャスト マルチアクセス) メディアのデフォルトの間隔は、60 秒ごとです。

スプリット ホライズンは、ルート情報がその情報の発生元の方に返送されないようにする機能です。スプリット ホライズンをインターフェイスでイネーブルにした場合 (これがデフォルトです)、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップである宛先に送信されません。これは、ルーティング ループを防止するのに役立ちます。

たとえば、[図 1: EIGRP スプリット ホライズンの例 \(14 ページ\)](#) に示すように、ルータ 1 がルータ 2 および 3 に 1 つのマルチポイント インターフェイスで接続され、ルータ 1 がルータ 2 からネットワーク A について学習した場合、ルータ 1 は、その同じマルチポイント インターフェイスでネットワーク A へのルートをルータ 3 にアドバタイズしません。ルータ 1 では、ルータ 3 はネットワーク A についてルータ 2 から直接学習すると想定します。

図 1: EIGRP スプリット ホライズンの例



スプリットホライズンは、すべてのEIGRPインターフェイスでデフォルトでイネーブルです。通常は、スプリットホライズンによって、複数のルーティングデバイス間の通信が最適化されるためです。ただし、非ブロードキャストネットワーク（フレームリレーやSMDSなど）では、スプリットホライズンをディセーブルにする必要がある場合があります。

EIGRPインターフェイスでスプリットホライズンをディセーブルにする場合は、次の点に注意してください。

- ハブアンドスポークネットワークでは、ハブだけでスプリットホライズンをディセーブルにする必要があります。これは、スポークでスプリットホライズンをディセーブルにすると、ハブルータのEIGRPメモリ消費量が大幅に増加するだけでなく、スポークルータで生成されるトラフィックの量も増加するためです。
- インターフェイスでスプリットホライズン設定を変更すると、そのインターフェイスで到達可能なEIGRPネイバーとの隣接関係はすべてリセットされます。

はじめる前に

- 少なくとも1つのEIGRP自律システムを定義します。[EIGRPルートの定義](#)（12ページ）を参照してください。

関連項目

- [EIGRPルートの定義](#)（12ページ）
- [EIGRPへのルートの再配布](#)（15ページ）
- [Cisco IOSルータにおけるEIGRPルーティング](#)（10ページ）

ステップ1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから[プラットフォーム (Platform)]>[ルーティング (Routing)]>[EIGRP]を選択し、作業領域の[インターフェイス (Interfaces)]タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから[ルータプラットフォーム (Router Platform)]>[ルーティング (Routing)]>[EIGRP]を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイス (Interface)]タブをクリックします。

[EIGRPインターフェイス (EIGRP Interfaces)] タブが表示されます。このタブのフィールドの説明については、[表 7: EIGRP の \[Interfaces\] タブ \(20 ページ\)](#) を参照してください。

- ステップ 2** EIGRPの[インターフェイス (Interfaces)] タブで、テーブルからインターフェイスを選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックしてインターフェイス定義を作成します。[EIGRPインターフェイス (EIGRP Interface)] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 8: \[EIGRP Interface\] ダイアログボックス \(21 ページ\)](#) を参照してください。
- ステップ 3** インターフェイス プロパティを変更する自律システムの AS 番号を選択します。自律システムの定義の詳細については、[EIGRP ルートの定義 \(12 ページ\)](#) を参照してください。
- ステップ 4** 定義するインターフェイスの名前またはインターフェイスロールを入力します。または、[選択 (Select)] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#)を参照してください。
- ステップ 5** (任意) [Hello Interval] フィールドで、選択したインターフェイスで送信される hello パケット間のデフォルトの間隔を変更します。

デフォルトの間隔が 60 秒の低速 (T1 以下) の NBMA メディアを除き、すべてのインターフェイスでデフォルトは 5 秒です。

- ステップ 6** (任意) [スプリットホライズン (Split Horizon)] チェックボックスをオフにして、スプリットホライズン機能をディセーブルにします。この機能をディセーブルにすると、選択したインターフェイスで、ルートの学習元のインターフェイスからそのルートをアドバタイズできます。

(注) 一般に、変更によってルートが正しくアドバタイズされることがアプリケーションにとって必要であることが確実な場合以外は、スプリットホライズンをディセーブルにしないことを推奨します。シリアルインターフェイスでスプリットホライズンをディセーブルにし、そのインターフェイスがパケットスイッチドネットワークに接続されている場合、そのネットワーク上のすべての関連するマルチキャストグループ内のすべてのルータおよびアクセスサーバに対して、スプリットホライズンをディセーブルにする必要があります。

- ステップ 7** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[EIGRPインターフェイス (EIGRP Interface)] タブのテーブルに表示されます。

EIGRP へのルートの再配布

再配布とは、EIGRP などのルーティングプロトコルを使用して、他の方法 (別のルーティングプロトコルなど) で学習されたルート、スタティックルート、または直接接続されたルートをアドバタイズすることです。たとえば、RIP ルーティングプロトコルから EIGRP 自律システム (AS) にルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベースルーティングプロトコルに適用できます。

はじめる前に

- 少なくとも 1 つの EIGRP 自律システムを定義します。[EIGRP ルートの定義 \(12 ページ\)](#) を参照してください。

関連項目

- [EIGRP ルートの定義 \(12 ページ\)](#)
- [EIGRP インターフェイスのプロパティの定義 \(13 ページ\)](#)
- [Cisco IOS ルータにおける EIGRP ルーティング \(10 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)]** > **[ルーティング (Routing)]** > **[EIGRP]** を選択し、作業領域の **[再配布 (Redistribution)]** タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[ルータプラットフォーム (Router Platform)]** > **[ルーティング (Routing)]** > **[EIGRP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、**[再配布 (Redistribution)]** タブをクリックします。

EIGRP の **[Redistribution]** タブが表示されます。このタブのフィールドの説明については、[表 9: EIGRP の \[Redistribution\] タブ \(22 ページ\)](#) を参照してください。

ステップ 2 EIGRP の **[再配布 (Redistribution)]** タブで、**[EIGRP再配布マッピング (EIGRP Redistribution Mappings)]** テーブルから行を選択し、**[編集 (Edit)]** をクリックするか、**[追加 (Add)]** をクリックしてマッピングを作成します。**[EIGRP Redistribution Mapping]** ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 10: \[EIGRP再配布マッピング \(EIGRP Redistribution Mapping\)\] ダイアログボックス \(23 ページ\)](#) を参照してください。

ステップ 3 表示されるリストから既存の EIGRP AS を選択します。

ステップ 4 選択した EIGRP AS にルートを再配布するプロトコルを選択します。

(注) スタティックルート、RIPルート、BGP AS、EIGRP AS、および OSPF プロセスごとに1つのマッピングを作成できます。

ステップ 5 (任意) **[Metrics]** で、メトリックの計算に使用されるフィールドに値を入力して、再配布されるルートのデフォルトのメトリック (コスト) を変更します。メトリックによって、ルートのプライオリティが決まります。

(注) メトリックの入力は任意ですが、値を指定する場合は、5つのパラメータすべての値を入力する必要があります。1つの EIGRP プロセスを別の EIGRP プロセスに再配布する場合は、メトリック値を定義する必要はありません。

ステップ 6 **[OK]** をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、EIGRP の **[再配布 (Redistribution)]** タブの **[再配布マッピング (Redistribution Mapping)]** テーブルに表示されます。

[EIGRP] ルーティングポリシー ページ

Enhanced Interior Gateway Routing Protocol (EIGRP) は、最小のネットワークトラフィックで非常に迅速なコンバージェンス時間を提供するスケーラブルな Interior Gateway Protocol です。

[EIGRP] ルーティング ページの次のタブから、EIGRP ルーティング ポリシーを設定できます。

- [EIGRP] ページ : [セットアップ (Setup)] タブ (17 ページ)
- [EIGRP] ページ : [インターフェイス (Interfaces)] タブ (19 ページ)
- [EIGRP] ページ - [Redistribution] タブ (21 ページ)

詳細については、Cisco IOS ルータにおける EIGRP ルーティング (10 ページ) を参照してください。

ナビゲーションパス

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [EIGRP] を選択します。
- (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [EIGRP] を選択します。[EIGRP] を右クリックしてポリシーを作成するか、または共有ポリシーセクタから既存ポリシーを選択します。

[EIGRP] ページ : [セットアップ (Setup)] タブ

EIGRP の [Setup] タブを使用して、EIGRP ルートを表示、作成、編集、および削除します。

ナビゲーションパス

[EIGRP] ルーティング ポリシー ページ (16 ページ) に移動し、[セットアップ (Setup)] タブをクリックします。

関連項目

- EIGRP ルートの定義 (12 ページ)
- [EIGRP] ページ : [インターフェイス (Interfaces)] タブ (19 ページ)
- [EIGRP] ページ - [Redistribution] タブ (21 ページ)
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールドリファレンス

表 5: EIGRP の [セットアップ (Setup)] タブ

要素	説明
AS 番号 (AS Number)	自律システムを他のルータに対して識別する自律システム番号。

要素	説明
ネットワーク	ルートに含まれるネットワークの名前。
パッシブインターフェイス	ルーティング更新をネイバーと送受信しないインターフェイス。
自動集約 (Auto-Summary)	選択したルートで自動サマライズがアクティブかどうかを指定します。
[追加 (Add)] ボタン	[EIGRPのセットアップ (EIGRP Setup)]ダイアログボックス (18 ページ) が開きます。ここから、EIGRP ルートを作成できます。
[編集 (Edit)] ボタン	[EIGRPのセットアップ (EIGRP Setup)]ダイアログボックス (18 ページ) が開きます。ここから、選択した EIGRP ルートを編集できます。
[削除 (Delete)] ボタン	選択した EIGRP ルートをテーブルから削除します。

[EIGRPのセットアップ (EIGRP Setup)]ダイアログボックス

[EIGRP Setup] ダイアログボックスを使用して、EIGRP ルートを追加または編集します。

ナビゲーションパス

[EIGRP] ページ: [\[セットアップ \(Setup\) \]タブ \(17 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [EIGRP ルートの定義 \(12 ページ\)](#)
- [ポリシー定義中の IP アドレスの指定](#)
- [ネットワーク/ホストオブジェクトについて](#)

フィールドリファレンス

表 6: [\[EIGRPのセットアップ \(EIGRP Setup\) \]ダイアログボックス](#)

要素	説明
AS 番号 (AS Number)	EIGRP ルートの自律システム番号。この番号は、自律システムを他のルータで識別するために使用されます。有効値は 1 ~ 65535 です。

要素	説明
ネットワーク	EIGRP ルートに関連付けられたネットワーク。1つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトをカンマで区切って入力します。[選択 (Select)] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
パッシブ インターフェイス	ルーティング ネイバーに更新を送信しないインターフェイス。1つ以上のインターフェイス名またはロールをカンマで区切って入力します。[選択 (Select)] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイスロールオブジェクトを作成します。 (注) インターフェイスを受動にすると、EIGRPによってルータ間の hello パケットの交換は抑止され、ネイバー関係は失われます。これにより、ルーティング更新のアドバタイズが停止されるだけでなく、着信するルーティング更新も抑止されます。
自動集約 (Auto-Summary)	選択されている場合は、ネットワークレベルルートへのサブネットルートの自動サマライズをイネーブルにします。サマライズによってルーティングテーブルのサイズが削減されるため、ネットワークの複雑さが低減します。 選択解除されている場合、自動サマライズはディセーブルになります。

[EIGRP] ページ : [インターフェイス (Interfaces)] タブ

EIGRP の [Interfaces] タブを使用して、選択した EIGRP 自律システムのインターフェイス プロパティを作成、編集、および削除します。デフォルトの hello 間隔の変更やスプリット ホライズンをディセーブルにすることも含まれます。



- (注) EIGRP の [Interfaces] タブには、[Setup] タブで少なくとも1つの EIGRP 自律システムを定義したあとにだけアクセスできます。[EIGRP] ページ : [セットアップ (Setup)] タブ (17 ページ) を参照してください。

ナビゲーションパス

[EIGRP] ルーティングポリシー ページ (16 ページ) に移動し、[インターフェイス (Interfaces)] タブをクリックします。

関連項目

- EIGRP インターフェイスのプロパティの定義 (13 ページ)

- [\[EIGRP\] ページ : \[セットアップ \(Setup\) \] タブ \(17 ページ\)](#)
- [\[EIGRP\] ページ - \[Redistribution\] タブ \(21 ページ\)](#)
- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールド リファレンス

表 7: EIGRP の [Interfaces] タブ

要素	説明
AS 番号 (AS Number)	インターフェイス プロパティが定義される EIGRP 自律システム番号。
インターフェイス	選択した EIGRP 自律システムに関連する、特に定義された値を持つインターフェイス。
Split Horizon	選択したインターフェイスに対してスプリットホライズン機能がイネーブルかディセーブルかを指定します。
Hello 間隔 (Hello Interval)	ネイバルルータに送信される hello パケット間の定義済みインターバル。
[追加 (Add)] ボタン	[EIGRP Interface] ダイアログボックス (20 ページ) が開きます。ここから、EIGRP インターフェイス定義を作成できます。
[編集 (Edit)] ボタン	[EIGRP Interface] ダイアログボックス (20 ページ) が開きます。ここから、選択した EIGRP インターフェイス定義を編集できます。
[削除 (Delete)] ボタン	選択した EIGRP インターフェイス定義をテーブルから削除します。

[EIGRP Interface] ダイアログボックス

[EIGRP Interface] ダイアログボックスを使用して、選択した EIGRP 自律システムのインターフェイス定義を追加または編集します。

ナビゲーションパス

[\[EIGRP\] ページ : \[インターフェイス \(Interfaces\) \] タブ \(19 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [EIGRP インターフェイスのプロパティの定義 \(13 ページ\)](#)

- [Cisco IOS ルータでの基本的なインターフェイス設定](#)
- [インターフェイス ロール オブジェクトについて](#)

フィールドリファレンス

表 8: [EIGRP Interface] ダイアログボックス

要素	説明
AS 番号 (AS Number)	インターフェイス プロパティを変更する EIGRP 自律システム番号を選択します。EIGRP 自律システムの詳細については、 [EIGRPのセットアップ (EIGRP Setup)] ダイアログボックス (18 ページ) を参照してください。
インターフェイス	設定する EIGRP インターフェイスを指定します。インターフェイスまたはインターフェイスロールの名前を入力します。または、 [選択 (Select)] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、新しいオブジェクトを作成します。
Hello 間隔 (Hello Interval)	ルータからそのネイバーに送信される hello パケット間のデフォルトの間隔。ルータは、hello パケットを相互に送信して、直接接続されたネットワーク上の他のルータについて動的に学習します。有効な値の範囲は、1 ~ 65535 秒です。デフォルトは 5 秒です。
Split Horizon	<p>選択すると、ルーティングループを防止するためにスプリット ホライズン機能が使用されます。</p> <p>選択を解除すると、スプリット ホライズンがディセーブルになります。スプリット ホライズンがディセーブルになると、ルータで、ルートの学習元の同じインターフェイスからそのルートをアドバタイズできます。</p> <p>スプリットホライズンを無効にすると、フレームリレーや SMDS などの非ブロードキャストネットワークを扱う場合に便利です。</p> <p>(注) インターフェイスでスプリット ホライズン設定を変更すると、そのインターフェイスで到達可能な EIGRP ネイバーとの隣接関係はすべてリセットされます。</p>

[EIGRP] ページ - [Redistribution] タブ

EIGRP の [Redistribution] タブを使用して、EIGRP 再配布マッピングを作成、編集、および削除します。

ナビゲーションパス

[\[EIGRP\] ルーティングポリシー ページ \(16 ページ\)](#) に移動し、[\[再配布 \(Redistribution\)\]](#) タブをクリックします。

関連項目

- [EIGRP へのルートの再配布 \(15 ページ\)](#)
- [\[EIGRP\] ページ : \[セットアップ \(Setup\) \] タブ \(17 ページ\)](#)
- [\[EIGRP\] ページ : \[インターフェイス \(Interfaces\) \] タブ \(19 ページ\)](#)
- [テーブルカラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 9: EIGRP の [Redistribution] タブ

要素	説明
EIGRP AS Number	他のルートが再配布されている EIGRP ルートのエリア ID。
プロトコル	再配布されているプロトコル。
[AS/プロセス ID (AS/Process ID)]	再配布されているルートの AS 番号またはプロセス ID。
Bandwidth	ルートメトリックに対して定義された、EIGRP ルートのパスの最小帯域幅。
遅延	ルートメトリックに対して定義された、パスの平均遅延。
信頼性	ルートメトリックに対して定義された、パスの推定信頼性を表す値。
有効帯域幅 (Effective Bandwidth)	ルートメトリックに対して定義された、リンクへの有効負荷を表す値。
[MTU]	ルートメトリックに対して定義された、パスの最小 MTU。
一致 (Match)	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
[追加 (Add)] ボタン	[EIGRP再配布マッピング (EIGRP Redistribution Mapping)] ダイアログボックス (23 ページ) が開きます。ここから、EIGRP 再配布マッピングを定義できます。
[編集 (Edit)] ボタン	[EIGRP再配布マッピング (EIGRP Redistribution Mapping)] ダイアログボックス (23 ページ) が開きます。ここから、選択した EIGRP 再配布マッピングを編集できます。
[削除 (Delete)] ボタン	選択した EIGRP 再配布マッピングをテーブルから削除します。

[EIGRP再配布マッピング (EIGRP Redistribution Mapping)] ダイアログボックス

[EIGRP Redistribution Mapping] ダイアログボックスを使用して、EIGRP 再配布マッピングのプロパティを追加または編集します。

ナビゲーションパス

[EIGRP] ページ - [Redistribution] タブ (21 ページ) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。



- (注) [EIGRP Redistribution] ダイアログボックスにアクセスする前に、少なくとも1つのEIGRP ASを作成する必要があります。[EIGRP] ページ : [セットアップ (Setup)] タブ (17 ページ) を参照してください。

関連項目

- [EIGRP へのルートの再配布 \(15 ページ\)](#)

フィールドリファレンス

表 10: [EIGRP再配布マッピング (EIGRP Redistribution Mapping)] ダイアログボックス

要素	説明
EIGRP AS Numbers	他のルートが再配布されている EIGRP AS。[EIGRP] ページ : [セットアップ (Setup)] タブ (17 ページ) で定義した EIGRP 自律システムのリストから ID 番号を選択する必要があります。
Protocol to Redistribute	再配布されているルーティングプロトコル。 <ul style="list-style-type: none"> • [Static] : スタティック ルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [EIGRP] : EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに1つのマッピングを定義できます。 • [BGP] : BGP 自律システムを再配布します。デバイスごとに1つの BGP マッピングを定義できます。[BGP Setup] タブで [BGP AS] を設定した場合は、AS 番号が表示されます。それ以外の場合は、BGP AS が定義されていないことを示すメッセージが表示されます。[BGP] ページ - [Redistribution] タブ (8 ページ) を参照してください。

要素	説明
Protocol to Redistribute (続き)	<ul style="list-style-type: none"> • [OSPF] : 別の OSPF プロセスを再配布します。プロセスごとに1つのマッピングを定義できます。表示されるリストからプロセスを選択し、1つ以上の一致基準を選択します。 <ul style="list-style-type: none"> • [Internal] : 特定の AS の内部のルート。 • [External1] : AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1] : AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area (NSSA) ルート。 • [NSAAExternal2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる (NSSA) ルート。 • [RIP] : RIP ルートを再配布します。 • [Connected] : インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
メトリック	<p>再配布されたルートのデフォルトのメトリック (コスト)。次のメトリックパラメータがあります。</p> <ul style="list-style-type: none"> • [Bandwidth] : パスの最小帯域幅 (キロビット/秒)。有効値の範囲は 1 ~ 4294967295 です。 • [Delay] : パスの平均遅延 (10 ミリ秒単位)。有効値の範囲は、0 ~ 4294967295 です。 • 信頼性 : リンクの推定信頼性を表す値。有効値の範囲は 0 ~ 255 で、255 は 100% の信頼性を表します。 • 実効帯域幅 : リンクの実効負荷を表す値。有効値の範囲は 1 ~ 255 で、255 は 100% の使用率を表します。 • [MTU of Path] : パスの最大伝送単位。有効な値の範囲は 1 ~ 65535 バイトです。

Cisco IOS ルータにおける OSPF ルーティング



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Open Shortest Path First (OSPF) は、距離ベクトルではなくリンクステートを使用して、1つの自律システム (AS) 内でルーティング情報を配布する Interior Gateway Routing Protocol です。OSPF はルーティングテーブル更新ではなく Link-State Advertisement (LSA; リンクステートアドバタイズメント) を伝播するため、OSPF ネットワークは RIP ネットワークよりも迅速に収束できます。エリアを定義して、エリア内で発生する変更に関連する LSA の数を制限します。

複数の OSPF エリアにインターフェイスを持つルータは、エリア境界ルータ (ABR) と呼ばれます。ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティングプロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ (ASBR) と呼ばれます。どのルータも ABR または ASBR として機能できます。

ここでは、OSPF ルーティングポリシーを作成するために実行するタスクについて説明します。

- [OSPF プロセス設定の定義 \(25 ページ\)](#)
- [OSPF エリア設定の定義 \(26 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

関連項目

- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)
- [Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#)
- [Cisco IOS ルータにおける EIGRP ルーティング \(10 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

OSPF プロセス設定の定義

OSPF プロセスパラメータを設定するには、OSPF プロセスを他のルータに対して識別するプロセス ID 番号を指定し、インターフェイスが受動かどうかを決定します。受動インターフェイスは、ネイバーにルーティング更新を送信しません。

関連項目

- [OSPF エリア設定の定義 \(26 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [OSPF プロセス (OSPF Process)]** を選択し、作業領域の **[セットアップ (Setup)]** タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP][Router Platform] > [Routing] > [RIP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、**[セットアップ (Setup)]** タブをクリックします。

OSPF プロセスの **[Setup]** タブが表示されます。このタブのフィールドの説明については、[表 13 : OSPF プロセスの \[Setup\] タブ \(46 ページ\)](#) を参照してください。

ステップ 2 OSPF プロセスの **[セットアップ (Setup)]** タブで、テーブルから OSPF プロセスを選択し、**[編集 (Edit)]** をクリックするか、**[追加 (Add)]** をクリックしてプロセスを作成します。**[OSPF セットアップ (OSPF Setup)]** ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 14 : \[OSPF Setup\] ダイアログボックス \(46 ページ\)](#) を参照してください。

ステップ 3 表示されるフィールドにプロセス ID 番号を入力します。ここで定義するプロセス ID は、他のデバイスのプロセス ID と一致している必要はありません。

ステップ 4 どのインターフェイスがネイバーにルーティング更新を送信しないかを定義します。

- a) **[パッシブインターフェイス (Passive Interfaces)]** の下にある **[編集 (Edit)]** をクリックして、**[インターフェイスの編集 (Edit Interfaces)]** ダイアログボックスを表示します。このダイアログボックスを使用して、ネイバーにルーティング更新を送信しないインターフェイスを定義します。
- b) 1 つ以上のインターフェイスまたはインターフェイスロールの名前を入力します。または、**[選択 (Select)]** をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。
- c) **[OK]** をクリックして変更を保存し、**[OSPF セットアップ (OSPF Setup)]** ダイアログボックスに戻ります。

ステップ 5 **[OK]** をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

OSPF エリア設定の定義

OSPF エリア設定を設定するには、エリア ID を特定の OSPF プロセスに関連付け、エリアに含まれるネットワークを選択し、エリア内のルータによって使用される認証のタイプを選択します。

定義する各 OSPF プロセスには、少なくとも 1 つの定義されたエリアが含まれている必要があります。複数のエリアを定義する場合は、1 つのエリアがエリア 0 である必要があります。これはバックボーンと呼ばれます。その他のすべてのエリアは、バックボーンに物理的に接続されている必要があります。これによって、他のエリアがルーティング情報をバックボーンに注入し、バックボーンがその他のエリアに配布できるようになります。

少なくとも 1 つの OSPF プロセスを設定してから、そのプロセスの OSPF エリア/ネットワーク設定を定義する必要があります。

関連項目

- [OSPF プロセス設定の定義 \(25 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [OSPF プロセス (OSPF Process)]** を選択し、作業領域の **[エリア (Area)]** タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [OSPF プロセス (OSPF Process)]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、**[エリア (Area)]** タブをクリックします。

[OSPF プロセスエリア (OSPF Process Area)] タブが表示されます。このタブのフィールドの説明については、[表 15: OSPF プロセスの \[Area\] タブ \(48 ページ\)](#) を参照してください。

ステップ 2 **[OSPF プロセスエリア (OSPF Process Area)]** タブで、テーブルから OSPF エリアを選択し、**[編集 (Edit)]** をクリックするか、**[追加 (Add)]** をクリックしてエリアを作成します。**[OSPF Area]** ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 16: \[OSPF Area\] ダイアログボックス \(49 ページ\)](#) を参照してください。

ステップ 3 表示されるリストからプロセス ID を選択します。

ステップ 4 選択した OSPF プロセスに関連付けるエリア ID を入力します。

ステップ 5 OSPF エリアに含めるネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを入力できます。または **[選択 (Select)]** をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。

ステップ 6 OSPF エリアで使用する認証タイプ (MD5、クリアテキスト、またはなし) を選択します。セキュリティが問題となる場合は、MD5 を推奨します。次の点に注意してください。

- 認証タイプは、同じエリア内のすべてのルータおよびアクセスサーバで同じである必要があります。

- エリアに対してクリアテキスト認証を指定すると、認証はタイプ 1（単純なパスワード）に設定されます。ネットワーク上のすべてのルータは、OSPF を使用して相互に通信するために、同じクリアテキストパスワードを使用する必要があります。
- エリア全体で MD5 パスワードを同じにする必要はありませんが、ネイバー間では同じにする必要があります。
- インターフェイス認証（[OSPF インターフェイス設定の定義（31 ページ）](#)）を参照）を使用する場合、エリアで使用する認証タイプが、インターフェイスで使用する認証タイプと一致する必要があります。

ステップ 7 [OK] をクリックして定義を保存します。OSPF エリアが、OSPF の [Area] タブに表示されるテーブルに表示されます。

OSPF へのルートの再配布

再配布とは、OSPF などのルーティングプロトコルを使用して、他の方法（別のルーティングプロトコルなど）で学習されたルート、スタティックルート、または直接接続されたルートをアドバタイズすることです。たとえば、RIP ルーティングプロトコルから OSPF ドメインにルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベースルーティングプロトコルに適用できます。

他のルーティングプロトコルまたはスタティックルートから OSPF へルートを再配布すると、これらのルートは OSPF 外部ルート（タイプ 1 またはタイプ 2）になります。

OSPF へのルートの再配布では、次のことを行います。

- [OSPF 再配布マッピングの定義（28 ページ）](#)
- [OSPF 最大プレフィックス値の定義（30 ページ）](#)

関連項目

- [OSPF プロセス設定の定義（25 ページ）](#)
- [OSPF エリア設定の定義（26 ページ）](#)
- [OSPF インターフェイス設定の定義（31 ページ）](#)
- [Cisco IOS ルータにおける OSPF ルーティング（25 ページ）](#)

OSPF 再配布マッピングの定義

OSPF 再配布マッピングを定義するときは、再配布するプロトコルと、そのプロトコルのルートを再配布する先の OSPF プロセスを選択する必要があります。また、再配布されるルートのプライオリティを決定するメトリック、および作成する外部 OSPF ルートのタイプ（タイプ 1 またはタイプ 2）を手動で定義できます。

同じ OSPF プロセスに複数のマッピングを作成できます。たとえば、RIP ルートと EIGRP ルートの両方を同じ OSPF プロセスに再配布できます。他の OSPF プロセスからルートを再配布することもできます。



- (注) OSPF Not-So-Stubby Area (NSSA) への再配布によって、NSSA エリア内だけで存在可能な、タイプ 7 と呼ばれる特別なタイプのリンクステートアドバタイズメント (LSA) が作成されます。この LSA は、NSSA Autonomous System Border Router (ASBR; 自律システム境界ルータ) によって生成され、NSSA Area Border Router (ABR; エリア境界ルータ) によってタイプ 5 LSA に変換されて、これが OSPF ドメインに伝播されます。

タイプ 1 とタイプ 2 の外部ルート

タイプ 1 とタイプ 2 という 2 つのタイプの OSPF 外部ルートがあります。2 つの違いは、ルートのコスト (メトリック) の計算方法に関係します。タイプ 1 ルートのコストは、そのルートに到達するために使用される外部コストと内部コストの合計です。タイプ 2 ルートのコストは、外部コストだけにに基づきます。デフォルトでは、外部ルートはタイプ 2 として定義されます。ただし、同じ宛先へは、タイプ 1 ルートがタイプ 2 ルートよりも常に優先されます。

はじめる前に

- 少なくとも 1 つの OSPF プロセスを定義します。 [OSPF プロセス設定の定義 \(25 ページ\)](#) を参照してください。

関連項目

- [OSPF 最大プレフィックス値の定義 \(30 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [OSPF プロセス (OSPF Process)] を選択し、作業領域の [再配布 (Redistribution)] タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP][Router Platform] > [Routing] > [RIP] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布 (Redistribution)] タブをクリックします。

[OSPF Process Redistribution] タブが表示されます。このタブのフィールドの説明については、[表 17: OSPF プロセスの \[Redistribution\] タブ \(50 ページ\)](#) を参照してください。

ステップ 2 OSPF プロセスの [再配布 (Redistribution)] タブで、[OSPF 再配布マッピング (OSPF Redistribution Mappings)] テーブルから行を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックしてマッピングを作成します。[OSPF Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 18: \[OSPF Redistribution Mapping\] ダイアログボックス \(52 ページ\)](#) を参照してください。

ステップ3 表示されるリストから既存の OSPF プロセスを選択します。

ステップ4 選択した OSPF プロセスにルートを再配布するプロトコルを選択します。

(注) スタティックルート、RIP ルート、BGP AS、EIGRP AS、および OSPF プロセスごとに1つのマッピングを作成できます。

ステップ5 (任意) 再配布されたルートのデフォルトのメトリック (コスト) を修正します。メトリックによって、ルートのプライオリティが決まります。

ステップ6 作成する外部ルートのメトリック タイプ (タイプ 1 またはタイプ 2) を選択します。デフォルトはタイプ 2 です。

ステップ7 (オプション) [サブネットに制限 (Limit to Subnets)] チェックボックスをオンにして、サブネット化されたルートだけを再配布します。デフォルトでは、このオプションは選択されていません。

ステップ8 [OK] をクリックして定義を保存します。再配布マッピングが、OSPF プロセスの [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

OSPF 最大プレフィックス値の定義

選択した OSPF プロセスに他のプロトコルまたは OSPF プロセスから再配布できるプレフィックス (ルート) の最大数を定義できます。制限を設定すると、再配布されるルートが多すぎてルータがフラッド状態になるのを防止できます。たとえば、最大数を定義しないと、BGP が OSPF に再配布されるときにフラッディングが発生する可能性があります。

最大プレフィックス値を定義する場合、この最大値に達したときに、それ以上ルートが再配布されないようにするか、警告を発行するだけかを決定できます。

再配布制限は、すべての IP 再配布プレフィックスに適用されます。合計されるプレフィックスも含まれます。この制限は、タイプ 7 からタイプ 5 への変換の結果として生成されるデフォルト ルートまたはプレフィックスには適用されません。

はじめる前に

- 少なくとも 1 つの OSPF プロセスを定義します。少なくとも 1 つの OSPF プロセスを定義します。 [OSPF プロセス設定の定義 \(25 ページ\)](#) を参照してください。
- 少なくとも 1 つの OSPF 再配布マッピングを定義します。 [OSPF 再配布マッピングの定義 \(28 ページ\)](#) を参照してください。

関連項目

- [OSPF 再配布マッピングの定義 \(28 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)

ステップ1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから[プラットフォーム (Platform)]>[ルーティング (Routing)]>[OSPFプロセス (OSPF Process)]を選択し、作業領域の[再配布 (Redistribution)]タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから[ルータプラットフォーム (Router Platform)]>[ルーティング (Routing)]>[OSPFプロセス (OSPF Process)]を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布 (Redistribution)]タブをクリックします。

[OSPF Process Redistribution] タブが表示されます。このタブのフィールドの説明については、[表 17: OSPF プロセスの \[Redistribution\] タブ \(50 ページ\)](#) を参照してください。

ステップ 2 OSPF プロセスの [プロセスの再配布 (Process Redistribution)] タブで、[最大プレフィックスマッピング (Max Prefix Mapping)] テーブルから行を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックして定義を作成します。[Max Prefix Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 19: \[OSPF Max Prefix Mapping\] ダイアログボックス \(53 ページ\)](#) を参照してください。

ステップ 3 表示されるリストから既存の OSPF プロセスを選択します。

ステップ 4 [Max Prefix] フィールドで、選択した OSPF プロセスに再配布できるルートの最大数を入力します。

ステップ 5 (任意) デフォルトしきい値のパーセンテージを変更します。再配布されるルートの数がこのしきい値に達すると、警告が発行されます。デフォルトでは、しきい値は定義された最大プレフィックス値の 75% です。

ステップ 6 (任意) 最大プレフィックス値に達したときの動作を選択します。

- [Enforce Maximum Route]: 選択したプロセスにルートがそれ以上再配布されないようにします。
- [Warning Only]: 追加の警告を発行しますが、最大プレフィックス値に達したあともルートの再配布は続行されます。

(注) 最大プレフィックス値を超えたあともルートの再配布を続行すると、フラグディングが発生する可能性があります。

ステップ 7 [OK] をクリックして定義を保存します。最大プレフィックス定義は、OSPF プロセスの [Redistribution] タブの [Maximum Prefix] テーブルに表示されます。

OSPF インターフェイス設定の定義

インターフェイス固有のさまざまな OSPF パラメータを変更できます。ここでは、これらのパラメータを定義する方法について説明します。特定のパラメータについては、次の項を参照してください。

- [インターフェイス コストについて \(33 ページ\)](#)
- [インターフェイス プライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)

- [LSA フラディングのブロック \(35 ページ\)](#)
- [OSPF ネットワーク タイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)

関連項目

- [OSPF プロセス設定の定義 \(25 ページ\)](#)
- [OSPF エリア設定の定義 \(26 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから[プラットフォーム (Platform)]>[ルーティング (Routing)]>[OSPFインターフェイス (OSPF Interface)]を選択します。
- (ポリシービュー) ポリシータイプセクタから[ルータプラットフォーム (Router Platform)]>[ルーティング (Routing)]>[OSPFインターフェイス (OSPF Interface)]を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[OSPF Interface] ページが表示されます。このページのフィールドの説明については、[表 11 : \[OSPF Interface\] ページ \(39 ページ\)](#) を参照してください。

ステップ 2 [OSPFインターフェイス (OSPF Interface)] ページで、テーブルからインターフェイス定義を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックして定義を作成します。[OSPF Interface] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 12 : \[OSPF Interface\] ダイアログボックス \(40 ページ\)](#) を参照してください。

ステップ 3 定義するインターフェイスの名前またはインターフェイスロールを入力します。または、[選択 (Select)] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、[ポリシー定義中のインターフェイスの指定](#)を参照してください。

ステップ 4 インターフェイス認証を定義します。インターフェイスに対して選択する認証タイプは、エリアに対して選択する認証タイプと一致している必要があります ([OSPF エリア設定の定義 \(26 ページ\)](#) を参照)。

OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。詳細については、[OSPF インターフェイス認証について \(37 ページ\)](#) を参照してください。

キー ID 番号は、複数のパスワードに関連付けることができます。これは、パスワードを移行する簡単で安全な方法です。たとえば、あるパスワードを別のパスワードに移行するには、異なるキー ID でパスワードを設定してから、最初のキーを削除します。

ヒント キー ID 番号は、複数のパスワードに関連付けることができます。これは、パスワードを移行する簡単で安全な方法です。たとえば、あるパスワードを別のパスワードに移行するには、異なるキー ID でパスワードを設定してから、最初のキーを削除します。

(注) セキュリティ上の目的から、OSPF パケットにはクリアテキスト認証を使用しないでください。クリアテキスト認証では、各パケットで暗号化されていない認証キーが送信されます。クリアテキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。

- ステップ 5** (任意) [プロパティ (Properties)] で、必要に応じてインターフェイスパラメータを設定します。各パラメータについては、[表 12 : \[OSPF Interface\] ダイアログボックス \(40 ページ\)](#) を参照してください。
- ステップ 6** [OK] をクリックして定義を保存します。定義されたインターフェイスが、[OSPF Interface] ページに表示されます。
- ステップ 7** このプロセスを繰り返して、その他の OSPF インターフェイスのインターフェイス固有のパラメータを定義します。

インターフェイスコストについて

OSPF インターフェイスのコストとは、そのインターフェイスでパケットを送信する場合のコストを表すメトリックのことです。デフォルトでは、このコストは次の式で計算されます。

$10^8 / \text{帯域幅 (ビット/秒)}$

たとえば、ファストイーサネットインターフェイスの帯域幅が 10 Mbps (10^7 と等しい) の場合、そのインターフェイスでパケットを送信するコストは $10^8 / 10^7$ 、または 10 として計算されます。この式によって、インターフェイスの帯域幅とそのコスト間の反比例関係が確立されます。帯域幅が大きくなると、コストは低くなります。

コストは計算される値ですが、選択したインターフェイスのコストを手動で入力できます。

関連項目

- [インターフェイスプライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [LSA フラッドのブロック \(35 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF ネットワークタイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

インターフェイスプライオリティについて

共通セグメントを共有するルータは、Hello プロトコルによって、そのセグメント上でネイバーに選出されます。選出は、ネイバーの hello パケットにリストされていることをルータ自身が確認するとすぐに行われます。隣接関係は、次のステップです。隣接ルータとは、単純な Hello 交換を越えて、データベース交換へと進むルータです。

各マルチアクセス（ポイントツーポイントではない）セグメントで、OSPF は 1 つのルータをそのセグメントの Designated Router（DR; 指定ルータ）として選出します。DR は、情報交換を最小限にするために接続を一元的に管理する場所として機能します。セグメント内の各ルータは、更新を DR に送信し、DR はその情報を他のルータに中継します。DR がダウンしたときのために、別のルータが Backup Designated Router（BDR; バックアップ指定ルータ）として選出されます。

DR および BDR 選出は、Hello プロトコルを通じて実行されます。OSPF プライオリティが最も高いルータが、そのセグメントの DR になります。次に、BDR について同じプロセスが繰り返されます。プライオリティが同じ場合は、Router ID（RID; ルータ ID）が上位のルータが選出されます。デフォルトでは、各インターフェイスのプライオリティは 1 ですが、必要に応じて、選択したインターフェイスに高いプライオリティを割り当てることができます。



(注) プライオリティ設定は、ポイントツーポイントの非ブロードキャストインターフェイスには適用されません。

関連項目

- [インターフェイス コストについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [LSA フラディングのブロック \(35 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF ネットワーク タイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

MTU 不一致検出のディセーブル化

MTU は、特定のインターフェイスで処理できる最大パケット サイズです。あるルータが、ネイバールータ上の MTU 設定よりも大きい DBD パケットを送信した場合、ネイバールータはそのパケットを無視します。多くの場合、MTU の不一致によって 2 台のルータは exstart/exchange 状態になり、OSPF 隣接関係が確立されません。そのため、すべてのネイバールータが同じ MTU 設定を共有し、MTU 不一致検出がイネーブルになっていることが重要です。

ただし、MTU 不一致検出をディセーブルにすることもできます。これは、MTU が異なる以外には有効な設定である 2 台のデバイス間で、不一致検出によって隣接関係が確立されない場合に役立ちます。

関連項目

- [インターフェイス コストについて \(33 ページ\)](#)

- [インターフェイスプライオリティについて \(33 ページ\)](#)
- [LSA フラッディングのブロック \(35 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF ネットワークタイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

LSA フラッディングのブロック

デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。冗長性は必要ですが、過度な冗長性により帯域幅が浪費されることがあります。完全メッシュなどの特定のトポロジでは、過度のリンクおよび CPU 使用率のために、LSA フラッディングによってネットワークが不安定になる可能性があります。そのため、ブロードキャスト、非ブロードキャスト、およびポイントツーポイント ネットワーク上の選択したインターフェイスへの LSA フラッディングをブロックできます。

関連項目

- [インターフェイスコストについて \(33 ページ\)](#)
- [インターフェイスプライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF ネットワークタイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

OSPF タイマー設定について

OSPF では、動作中に一連のタイマーが使用されます。

- [Hello Interval] : インターフェイスが hello パケットを送信する頻度を決定します。hello パケットは、ネイバーの取得に使用され、ルータが機能していることのインジケータの役割を果たします。間隔が短いほど、ネットワーク上のトポロジ変更の検出が速くなります。ただし、間隔が短くなると、インターフェイスで送信されるトラフィックも多くなります。hello 間隔は、特定のネットワーク上のすべてのルータおよびアクセスサーバで同じである必要があります。

- [Transmit Delay] : LSA がリンクでフラッドされる前の遅延を決定します。送信遅延設定は、インターフェイスの送信および伝播遅延を考慮する必要があります。これらの要因は、低速リンクおよびオンデマンドリンクを設定する場合に特に重要です。
- [Retransmit Interval] : 確認応答されなかった DataBase Description (DBD) パケットをネイバーに再送信する前に待機する時間を決定します。再送信間隔設定を低く設定して、過度の再送信を防止する必要があります。



(注) シリアル回線および仮想リンクの場合は、再送信間隔を大きくする必要があります。

- [Dead Interval] : ネイバーがダウンしていると宣言する前にインターフェイスが待機する時間を決定します。この宣言は、この間隔内にネイバーからの hello パケットが届かない場合に行われます。デッド間隔設定は、特定のネットワーク上のすべてのルータおよびアクセスサーバで同じである必要があります。デフォルトでは、この間隔は hello 間隔の 4 倍です。

関連項目

- [インターフェイス コストについて \(33 ページ\)](#)
- [インターフェイス プライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [LSA フラディングのブロック \(35 ページ\)](#)
- [OSPF ネットワーク タイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

OSPF ネットワーク タイプについて

デフォルトのメディアタイプに関係なく、インターフェイスの OSPF ネットワーク タイプをブロードキャストまたは NonBroadcast MultiAccess (NBMA; 非ブロードキャストマルチアクセス) として手動で設定できます。たとえば、マルチキャストアドレッシングをサポートしないルータがネットワークに含まれている場合に、この機能を使用して、ブロードキャストネットワーク (イーサネット、トークンリング、FDDI など) を NBMA として設定できます。また、NBMA ネットワーク (X.25、フレームリレー、SMDS など) をブロードキャストネットワークとして設定できます。このことにより、ネイバーを設定する必要がなくなります。

NBMA ネットワークをブロードキャストまたは非ブロードキャストとして設定するには、すべてのルータからすべてのルータへの仮想回線 (VC) が存在すること (完全にメッシュ化されたネットワーク) が前提となります。各ルータ間に VC が存在しない場合 (コストの制約または部分的にだけメッシュ化されたネットワークの存在による)、OSPF ネットワークタイプをポイントツーマルチポイントとして設定できます。OSPF ポイントツーマルチポイントイン

ターフェイスは、1つ以上のネイバーを持つ番号付きポイントツーポイントインターフェイスとして定義されます。複数のホスト ルートが作成されます。

ポイントツーマルチポイント ネットワーク タイプを使用する場合、直接接続されていない2台のルータ間のルーティングは、両方のルータへの VC を持つ第三のルータを経由します。この機能を使用する場合、ネイバーを設定する必要はありません。OSPF ポイントツーマルチポイント ネットワークには、NBMA およびポイントツーポイント ネットワークと比較して、次の利点があります。

- ポイントツーマルチポイントは、IP サブネットを1つだけ使用し、ネイバー設定または指定ルータ選出が必要ないため、設定が簡単です。
- 完全にメッシュ化されたトポロジが必要ないため、コストが低くなります。
- VC の障害時に接続が維持されるため、信頼性が高まります。



- (注) ポイントツーマルチポイントのブロードキャスト ネットワークでは、任意でネイバーを定義できます。この場合、各ネイバーへのコストを指定する必要があります。ポイントツーマルチポイントの非ブロードキャスト ネットワークでは、ネイバーを識別する必要がありますが、各ネイバーへのコストの指定は任意です。どちらの場合も、**FlexConfig** を使用してネイバーを定義します。詳細については、**FlexConfig ポリシーとポリシー オブジェクトについて**を参照してください。

関連項目

- [インターフェイス コストについて \(33 ページ\)](#)
- [インターフェイス プライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [LSA フラッドのブロック \(35 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)
- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)

OSPF インターフェイス認証について

OSPF インターフェイスのネイバー認証設定を定義するには、インターフェイスを選択し、認証タイプ (MD5 またはクリア テキスト) を選択します。

MD5 認証を使用する場合、ネイバルルータは同じパスワードを共有する必要があります。クリアテキスト認証を使用する場合、OSPF を使用するネットワーク上のすべてのルータは同じパスワードを共有する必要があります。

新しいキーを使用してインターフェイスを設定すると、ルータは、それぞれ異なるキーで認証された複数の同一パケットを送信します。すべてのネイバーが新しいキーを採用したことをルータが検出すると、重複パケットの送信を停止します。



- (注) 攻撃者はOSPF と他のプロトコル (RIP など) との間のルート再配布を利用してルーティング情報を操作できるため、可能なかぎり、すべてのルーティングプロトコルで認証を使用する必要があります。

関連項目

- [インターフェイス コストについて \(33 ページ\)](#)
- [インターフェイス プライオリティについて \(33 ページ\)](#)
- [MTU 不一致検出のディセーブル化 \(34 ページ\)](#)
- [LSA フラディングのブロック \(35 ページ\)](#)
- [OSPF タイマー設定について \(35 ページ\)](#)
- [OSPF ネットワーク タイプについて \(36 ページ\)](#)
- [OSPF インターフェイス認証について \(37 ページ\)](#)

[OSPF Interface] ポリシー ページ

[OSPF Interface] ページを使用して、インターフェイス固有の OSPF 設定を表示、作成、編集、および削除します。詳細については、[OSPF インターフェイス設定の定義 \(31 ページ\)](#) を参照してください。

ナビゲーションパス

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [OSPF インターフェイス (OSPF Interface)] を選択します。
- (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [OSPF インターフェイス (OSPF Interface)] を選択します。[OSPF インターフェイス (OSPF Interface)] を右クリックしてポリシーを作成するか、または共有ポリシーセクタから既存のポリシーを選択します。

関連項目

- [\[OSPF Process\] ポリシー ページ \(44 ページ\)](#)
- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 11 : [OSPF Interface] ページ

要素	説明
インターフェイス	OSPF をイネーブルにするインターフェイスの名前（インターフェイス ロールによって定義）。
認証	選択したインターフェイスでイネーブルにする OSPF ネイバー認証のタイプ。
Key ID	MD5 認証に使用される認証キーの識別番号。
コスト (Cost)	選択したインターフェイスでパケットを送信するコスト（この値が通常計算されるコストと異なる場合）。
プライオリティ	選択したインターフェイスのプライオリティ。
MTU Ignore	選択したインターフェイスで最大伝送単位 (MTU) 検出がディセーブルかどうかを示します。
Database Filter	選択したインターフェイスでリンクステートアドバタイズメント (LSA) フラッドイングがディセーブルかどうかを示します。
Hello 間隔 (Hello Interval)	このインターフェイスで送信される hello パケット間隔 (秒単位)。
送信遅延 (Transmit Delay)	LSA がリンク上にフラッドイングされる前に OSPF が待機する時間 (秒単位)。
再送信間隔 (Retransmit Interval)	選択したインターフェイスでの LSA 再送信間隔 (秒単位)。
dead 間隔 (Dead Interval)	hello パケットがないためネイバルータがデッドであると宣言する前に OSPF が待機する間隔 (秒単位)。
ネットワーク タイプ (Network Type)	選択したインターフェイスに対して設定されるネットワークタイプ (デフォルトのメディアと異なる場合)。
[追加 (Add)] ボタン	[OSPF Interface] ダイアログボックス (40 ページ) が開きます。ここから、OSPF インターフェイスのプロパティを定義できます。
[編集 (Edit)] ボタン	[OSPF Interface] ダイアログボックス (40 ページ) が開きます。ここから、選択した OSPF インターフェイスのプロパティを編集できます。

要素	説明
[削除 (Delete)] ボタン	選択した OSPF インターフェイス定義をテーブルから削除します。

[OSPF Interface] ダイアログボックス

[OSPF Interface] ダイアログボックスを使用して、OSPF インターフェイスのプロパティを追加または編集します。

ナビゲーションパス

[OSPF Interface] ポリシー ページ (38 ページ) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [OSPF インターフェイス設定の定義 \(31 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)
- [Cisco IOS ルータでの基本的なインターフェイス設定](#)
- [インターフェイス ロール オブジェクトについて](#)

フィールド リファレンス

表 12: [OSPF Interface] ダイアログボックス

要素	説明
インターフェイス (Interface)	設定する OSPF インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
認証	<p>[Type] : 選択したインターフェイスで使用される認証タイプ。</p> <ul style="list-style-type: none"> • [MD5] : 認証に MD5 ハッシュアルゴリズムを使用します。これがデフォルトです。 • [Clear Text] : 認証にクリア テキスト パスワードを使用します。 • [None] : 認証を使用しません。 <p>(注) インターフェイスで使用される認証タイプは、エリアに対して定義された認証タイプと一致している必要があります。</p> <p>(注) プレーンテキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。</p> <ul style="list-style-type: none"> • [Key ID] : 認証タイプとして [MD5] を選択した場合にだけ使用できます。 <p>認証キーの識別番号。この番号は、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は、1 ~ 255 です。</p> <ul style="list-style-type: none"> • [Key] : 認証 (MD5 またはクリア テキスト) に使用される共有キー。このキーは、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。 <p>[Confirm] フィールドにこのキーを再入力します。</p> <p>クリア テキストを使用する場合、キーにはキーボードから入力できる任意の連続した文字列を含めることができます (最大 8 バイト)。</p> <p>MD5 を使用する場合、キーに使用できるのは英数字だけです (最大 16 バイト)。</p>
コスト (Cost)	<p>このインターフェイスでパケットを送信するコスト。ここに入力する値は、デフォルトで計算されるコスト (108/帯域幅 (ビット/秒)) よりも優先されます。</p> <p>有効値の範囲は 1 ~ 65535 です。</p>

要素	説明
プライオリティ	<p>インターフェイスのデフォルトのプライオリティ。プライオリティは、どのルータがそのセグメントの Designated Router (DR; 指定ルータ) および Backup Designated Router (BDR; バックアップ指定ルータ) になるかを決定するために使用されます。数字が大きいほど、優先順位は高くなります。</p> <p>デフォルトのプライオリティは 1 です。有効値の範囲は 0 ~ 255 です。</p> <p>(注) インターフェイスが DR または BDR として選出されないようにするには、プライオリティ 0 を割り当てます。ポイントツーポイントネットワークではなくマルチアクセスネットワークへのインターフェイスについてだけ、ルータプライオリティを設定します。</p>
MTU Ignore	<p>選択すると、ネイバルルータ間の MTU 不一致を無視します。</p> <p>選択を解除すると、MTU 不一致検出がイネーブルになります。</p> <p>(注) 通常、このオプションは使用されません。ルータが exstart/exchange 状態になり、OSPF 隣接関係が確立されなくなる可能性があるためです。</p>
Database Filter	<p>選択すると、選択したインターフェイスへのリンクステートアドバタイズメント (LSA) フラッドイングがブロックされます。</p> <p>選択を解除すると、LSA フラッドイングが許可されます。</p> <p>(注) 完全にメッシュ化されたネットワークでは、このオプションをイネーブルにすることを推奨します。このオプションは、ポイントツーマルチポイントネットワークには使用できません。</p>
Hello 間隔 (Hello Interval)	<p>選択したインターフェイスで送信される hello パケット間のデフォルトの間隔 (秒単位)。これらのパケットは、パケットを送信しているルータがまだ動作していることを確認するために、ネイバルルータによって使用されます。</p> <p>有効値の範囲は、1 ~ 65535 秒です。</p> <p>(注) hello 間隔は、ネットワーク内のすべてのルータおよびアクセスサーバで同じである必要があります。</p>
送信遅延 (Transmit Delay)	<p>LSA がリンク上にフラッドイングされる前に OSPF が待機する時間 (秒単位)。</p> <p>デフォルト値は 1 秒です。有効な値の範囲は、1 ~ 65535 秒です。</p> <p>(注) トラフィックを大量に送信する前にキューイングする低速リンクまたはオンデマンドリンクを設定する場合は、この値を定義するときに、これらのリンク遅延を考慮することを推奨します。</p>

要素	説明
再送信間隔 (Retransmit Interval)	選択したインターフェイスでの LSA 再送信間隔 (秒単位)。 デフォルトは 5 秒です。有効な値の範囲は、1 ~ 65535 秒です。 (注) シリアル回線および仮想リンクの場合は、この値を大きくすることを推奨します。
dead 間隔 (Dead Interval)	hello パケットが受信されない場合に、ネイバーがデッドであるとインターフェイスが宣言するまでの間隔 (秒単位)。有効値の範囲は 1 ~ 65535 秒です。 (注) 通常、デッド間隔の値は hello 間隔値の 4 倍です。デッド間隔は、ネットワーク内のすべてのルータおよびアクセスサーバで同じである必要があります。

要素	説明
Configure Network Type	<p>選択すると、インターフェイスによって使用されるデフォルトのメディアとは異なるネットワーク タイプを選択できます。</p> <p>選択を解除すると、ネットワーク タイプはインターフェイスによって使用されるデフォルトのメディアと同じです。</p> <p>NonBroadcast MultiAccess (NBMA; 非ブロードキャスト マルチアクセス) ネットワーク (ATM や フレーム リレー など) の場合、オプションは次のとおりです。</p> <ul style="list-style-type: none"> • [Broadcast] : NBMA ネットワークをブロードキャスト ネットワークとして処理します。このことにより、ネイバーを設定する必要がなくなります。このオプションは、すべてのルータからすべてのルータへの仮想回線がある場合 (完全にメッシュ化されたネットワーク) に使用します。 • [Point-to-Multipoint] : 非ブロードキャスト ネットワークを一連のポイント ツーポイント リンクとして処理します。このオプションは、NBMA またはポイント ツーポイント ネットワークよりも設定が簡単で、コストが小さく、高い信頼性があります。 • [Point-to-Multipoint Non-Broadcast] : ネットワークの既知のネイバーをステティックに保持します。このオプションを選択すると、hello パケットの受信によって動的に学習されたネイバーが失われる問題を回避するのに役立ちます。 <p>(注) NBMA ネットワークの別のオプションは、FlexConfig を使用してネイバーを手動で設定することです。 FlexConfig ポリシーとポリシー オブジェクトについて を参照してください。</p> <p>ブロードキャスト ネットワーク (イーサネット、トークン リング、FDDI など) の場合、次を選択できます。</p> <ul style="list-style-type: none"> • [Non-Broadcast] : ブロードキャスト ネットワークを非ブロードキャスト ネットワークとして処理します。 • [Point-to-Point] : ブロードキャスト ネットワークをポイント ツーポイント ネットワークとして処理します。このオプションを使用して、たとえば、ネットワーク内のすべてのルータがマルチキャスト アドレッシングをサポートしているわけではない場合に、ブロードキャスト ネットワーク (イーサネットなど) を NonBroadcast MultiAccess (NBMA; 非ブロードキャスト マルチアクセス) ネットワークとして設定できます。

[OSPF Process] ポリシー ページ

OSPF は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF はルーティング テーブル更新ではなく Link-State Advertisement (LSA; リ

ンクステートアドバタイズメント) を伝播するため、OSPF ネットワークは迅速に収束できません。

[OSPF Process] ページの次のタブから、OSPF プロセス ポリシーを設定できます。

- [\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#)
- [\[OSPF Process\] ページ - \[Area\] タブ \(47 ページ\)](#)
- [\[OSPF Process\] ページ - \[Redistribution\] タブ \(49 ページ\)](#)

詳細については、[Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#) を参照してください。



-
- (注) [OSPF インターフェイス ポリシーの詳細については、\[OSPF Interface\] ポリシー ページ \(38 ページ\)](#) を参照してください。
-

ナビゲーションパス

- (デバイスビュー) デバイスポリシーセクタから[プラットフォーム (Platform)]>[ルーティング (Routing)]>[OSPFプロセス (OSPF Process)]を選択します。
- (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)]>[ルーティング (Routing)]>[OSPFプロセス (OSPF Process)]を選択します。[OSPFプロセス (OSPF Process)]を右クリックしてポリシーを作成するか、または共有ポリシーセクタから既存のポリシーを選択します。

[OSPF Process] ページ - [Setup] タブ

OSPF プロセスの [Setup] タブを使用して、OSPF プロセスを作成、編集、および削除します。これには、受動のままのインターフェイスの選択も含まれます。これは、ネイバーにルーティング更新を送信しないことを意味します。プロセスは、ルータごとに必要な数だけ作成できます。

ナビゲーションパス

[\[OSPF Process\] ポリシー ページ \(44 ページ\)](#) に移動し、[セットアップ (Setup)] タブをクリックします。

関連項目

- [OSPF プロセス設定の定義 \(25 ページ\)](#)
- [\[OSPF Process\] ページ - \[Area\] タブ \(47 ページ\)](#)
- [\[OSPF Process\] ページ - \[Redistribution\] タブ \(49 ページ\)](#)
- [\[OSPF Interface\] ポリシー ページ \(38 ページ\)](#)

- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールド リファレンス

表 13: OSPF プロセスの [Setup] タブ

要素	説明
プロセス ID (Process ID)	OSPF ルーティングプロセスを他のルータに対して識別するプロセス ID。
パッシブインターフェイス	ルーティング更新を送信しないインターフェイス。
[追加 (Add)] ボタン	[OSPF Setup] ダイアログボックス (46 ページ) が開きます。ここから、OSPF プロセスを定義できます。
[編集 (Edit)] ボタン	[OSPF Setup] ダイアログボックス (46 ページ) が開きます。ここから、選択した OSPF プロセスを編集できます。
[削除 (Delete)] ボタン	選択した OSPF プロセスをテーブルから削除します。

[OSPF Setup] ダイアログボックス

[OSPF Setup] ダイアログボックスを使用して、OSPF プロセスを追加または編集します。

ナビゲーションパス

[\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [OSPF プロセス設定の定義 \(25 ページ\)](#)

フィールド リファレンス

表 14: [OSPF Setup] ダイアログボックス

要素	説明
プロセス ID (Process ID)	OSPF プロセスのプロセス ID 番号。この番号によって、OSPF プロセスは他のルータに対して識別されます。他のデバイス上のプロセス ID と一致している必要はありません。有効値は 1 ~ 65535 です。

要素	説明
パッシブ インターフェイス	<p>ルーティング ネイバーに更新を送信しないインターフェイス。[編集 (Edit)]をクリックして、[Edit Interfaces] ダイアログボックス - OSPF 受動インターフェイス (47 ページ) を表示します。ここから、これらのインターフェイスを定義できます。</p> <p>(注) インターフェイスを受動にすると、OSPF によってネイバー ルータへの hello パケットの送信は抑止されます。ただし、インターフェイスでルーティング更新の受信は続行されます。</p>

[Edit Interfaces] ダイアログボックス - OSPF 受動インターフェイス

Cisco IOS ルータで OSPF ルーティング ポリシーを設定する場合、[Edit Interfaces] ダイアログボックスを使用して、ルーティング ネイバーに更新を送信しないインターフェイスを指定します。複数の名前またはロールを指定する場合は、カンマで区切ります。[選択 (Select)]をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。

ナビゲーションパス

[\[OSPF Setup\] ダイアログボックス \(46 ページ\)](#) に移動してから、[パッシブインターフェイス (Passive Interfaces)] フィールドの [編集 (Edit)] ボタンをクリックします。

関連項目

- [\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#)
- [OSPF プロセス設定の定義 \(25 ページ\)](#)

[OSPF Process] ページ - [Area] タブ

OSPF の [Area] タブを使用して、各 OSPF プロセスに含まれるエリアおよびネットワークを作成、編集、および削除します。これには、各エリアによって使用される認証のタイプの選択が含まれます。

ナビゲーションパス

[\[OSPF Process\] ポリシー ページ \(44 ページ\)](#) に移動し、[エリア (Area)] タブをクリックします。

関連項目

- [OSPF エリア設定の定義 \(26 ページ\)](#)
- [\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#)
- [\[OSPF Process\] ページ - \[Redistribution\] タブ \(49 ページ\)](#)

- [\[OSPF Interface\] ポリシー ページ \(38 ページ\)](#)
- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールド リファレンス

表 15: OSPF プロセスの [Area] タブ

要素	説明
エリア ID (Area ID)	プロセスに関連付けられるエリアの ID 番号。
プロセス ID (Process ID)	OSPF ルーティング プロセスを他のルータに対して識別するプロセス ID。
ネットワーク	エリアに含まれるネットワーク。
認証	エリアによって使用される認証タイプ (MD5、クリアテキスト、またはなし)。
[追加 (Add)] ボタン	[OSPF Area] ダイアログボックス (48 ページ) を開きます。ここから、OSPF エリアを定義できます。
[編集 (Edit)] ボタン	[OSPF Area] ダイアログボックス (48 ページ) が開きます。ここから、選択した OSPF エリアを編集できます。
[削除 (Delete)] ボタン	選択した OSPF エリアをテーブルから削除します。

[OSPF Area] ダイアログボックス

[OSPF Area] ダイアログボックスを使用して、OSPF エリアのプロパティを追加または編集します。OSPF プロセスごとに少なくとも 1 つのエリアを定義する必要がありますが ([\[OSPF Setup\] ダイアログボックス \(46 ページ\)](#) を参照)、定義しない場合でも展開は失敗しません。

ナビゲーションパス

[\[OSPF Process\] ページ - \[Area\] タブ \(47 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [OSPF エリア設定の定義 \(26 ページ\)](#)
- [ポリシー定義中の IP アドレスの指定](#)
- [ネットワーク/ホストオブジェクトについて](#)

フィールドリファレンス

表 16: [OSPF Area] ダイアログボックス

要素	説明
プロセス ID (Process ID)	OSPF エリアに関連付けられるプロセス ID。リストには、 [OSPF Process] ページ - [Setup] タブ (45 ページ) で定義された OSPF プロセスが含まれます。
エリア ID (Area ID)	選択したプロセスに関連付けられるエリア ID 番号。有効値の範囲は、0 ~ 4294967295 です。
ネットワーク	OSPF エリアに追加するネットワーク。1つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
認証	<p>エリアに対して使用される認証のタイプ。</p> <ul style="list-style-type: none"> • [MD5] : (推奨) 認証に MD5 ハッシュ アルゴリズムを使用します。 • [Clear Text] : 認証にクリア テキストを使用します。 • [None] : 認証は使用されません。 <p>(注) 認証タイプは、エリア内のすべてのルータおよびアクセスサーバで同じである必要があります。</p>

[OSPF Process] ページ - [Redistribution] タブ

OSPF プロセスの [Redistribution] タブを使用して、OSPF 再配布マッピングを作成、編集、および削除します。これには、他のプロトコルまたは他の OSPF プロセスから OSPF に再配布できる最大ルート数の定義も含まれます。

ナビゲーションパス

[\[OSPF Process\] ポリシー ページ \(44 ページ\)](#) に移動し、[再配布 (Redistribution)] タブをクリックします。

関連項目

- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#)
- [\[OSPF Process\] ページ - \[Area\] タブ \(47 ページ\)](#)
- [\[OSPF Interface\] ポリシー ページ \(38 ページ\)](#)

- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 17: OSPF プロセスの [Redistribution] タブ

要素	説明
[OSPF Redistribution Mapping] テーブル	
OSPF プロセス ID (OSPF Process ID)	他のルートが再配布されている OSPF ルーティング ドメインの ID。
プロトコル	再配布されているプロトコル。
[AS/プロセス ID (AS/Process ID)]	再配布されているルートの AS 番号またはプロセス ID。
一致 (Match)	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
メトリック (Metric)	再配布されるルートのプライオリティを決定する値。
メトリック タイプ	OSPF ルーティング ドメインにアダプタイズされるデフォルト ルートに関連付けられる外部リンク タイプ。
サブネット	サブネット化されたルートも再配布されるかどうかを示します。
[追加 (Add)] ボタン	[OSPF Redistribution Mapping] ダイアログボックス (51 ページ) が開きます。ここから、OSPF 再配布マッピングを定義できます。
[編集 (Edit)] ボタン	[OSPF Redistribution Mapping] ダイアログボックス (51 ページ) が開きます。ここから、選択した OSPF 再配布マッピングを編集できます。
[削除 (Delete)] ボタン	選択した再配布マッピングをテーブルから削除します。
[OSPF Max Prefix Mapping] テーブル	
OSPF プロセス ID (OSPF Process ID)	最大プレフィックス値が定義された OSPF ルーティング ドメインの ID。
Max Prefix	選択した OSPF プロセスに再配布できるプレフィックス (ルート) の最大数。

要素	説明
[しきい値 (Threshold)]	警告メッセージをトリガーするしきい値として機能する最大プレフィックス値のパーセンテージ。
操作	最大値に達したときに、この OSPF プロセスへの再配布が停止されるか、警告が表示されるだけかを示します。
[追加 (Add)] ボタン	[OSPF Max Prefix Mapping] ダイアログボックス (53 ページ) が開きます。ここから、OSPF プロセスの最大プレフィックス値を定義できます。
[編集 (Edit)] ボタン	[OSPF Max Prefix Mapping] ダイアログボックス (53 ページ) が開きます。ここから、選択した OSPF プロセスに対して定義された最大プレフィックス値を編集できます。
[削除 (Delete)] ボタン	選択した最大プレフィックスマッピングをテーブルから削除します。

[OSPF Redistribution Mapping] ダイアログボックス

[OSPF Redistribution Mapping] ダイアログボックスを使用して、OSPF 再配布マッピングのプロパティを追加または編集します。

ナビゲーションパス

[\[OSPF Process\] ページ - \[Redistribution\] タブ \(49 ページ\)](#) に移動してから、[再配布マッピング (Redistribution Mapping)] テーブルの下にある [追加 (Add)] ボタンまたは [編集 (Edit)] ボタンをクリックします。



- (注) [\[OSPF Redistribution\] ダイアログボックス](#) にアクセスする前に、少なくとも 1 つの OSPF プロセスを作成する必要があります。[\[OSPF Process\] ページ - \[Setup\] タブ \(45 ページ\)](#) を参照してください。

関連項目

- [\[OSPF Max Prefix Mapping\] ダイアログボックス \(53 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)

フィールドリファレンス

表 18 : [OSPF Redistribution Mapping] ダイアログボックス

要素	説明
プロセス ID (Process ID)	他のルートが再配布されている OSPF プロセス。 [OSPF Process] ページ - [Setup] タブ (45 ページ) で定義した OSPF プロセスのリストから、プロセス ID 番号を選択する必要があります。
Protocol to Redistribute	再配布されているルーティングプロトコル。 <ul style="list-style-type: none"> • [Static] : スタティック ルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [EIGRP] : EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに1つのマッピングを定義できます。 • [BGP] : BGP 自律システムを再配布します。デバイスごとに1つの BGP マッピングを定義できます。[BGP Setup] タブで [BGP AS] を設定した場合は、AS 番号が表示されます。それ以外の場合は、BGP AS が定義されていないことを示すメッセージが表示されます。 [BGP] ページ - [Redistribution] タブ (8 ページ) を参照してください。
Protocol to Redistribute (続き)	<ul style="list-style-type: none"> • [OSPF] : 別の OSPF プロセスを再配布します。プロセスごとに1つのマッピングを定義できます。表示されるリストからプロセスを選択し、1つ以上の一致基準を選択します。 <ul style="list-style-type: none"> • [Internal] : 特定の AS の内部のルート。 • [External1] : AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1] : AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area (NSSA) ルート。 • [NSAAExternal2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる (NSSA) ルート。 • [RIP] : RIP ルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [Connected] : インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。

要素	説明
デフォルト メトリック (Default Metric)	再配布されるルートのコストを表す値。
メトリックタイプ	OSPF ルーティングドメインに再配布されているルートに関連付けられる外部リンクタイプ。 <ul style="list-style-type: none"> • [1] : タイプ 1 外部ルート。メトリックは、外部再配布コストと内部 OSPF コストの合計です。 • [2] : タイプ 2 外部ルート。メトリックは、[Metric] フィールドで定義される外部再配布コストと等しくなります。これがデフォルトです。
Limit to Subnets	選択すると、サブネット化されたルートだけが再配布されます。 選択を解除すると、サブネット化されたルートは再配布されません。

[OSPF Max Prefix Mapping] ダイアログボックス

[OSPF Max Prefix Mapping] ダイアログボックスを使用して、OSPF プロセスに再配布できるルートの最大数を追加または編集します。

ナビゲーションパス

[OSPF Process] ページ - [Redistribution] タブ (49 ページ) に移動してから、プレフィックスマッピング テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [OSPF Redistribution Mapping] ダイアログボックス (51 ページ)
- OSPF へのルートの再配布 (28 ページ)

フィールドリファレンス

表 19: [OSPF Max Prefix Mapping] ダイアログボックス

要素	説明
プロセス ID (Process ID)	他のルートが再配布されている OSPF プロセス。リストには、[OSPF Process] ページ - [Setup] タブ (45 ページ) で定義された OSPF プロセスが含まれます。
Max Prefix	選択した OSPF プロセスに再配布できるプレフィックス (ルート) の最大数。再配布されるルートの数を制限すると、過剰な数のルートによってルータがフラッドされるのを防ぐのに役立ちます。

要素	説明
[しきい値 (Threshold)]	警告メッセージをトリガーするしきい値として機能する最大プレフィックス値のパーセンテージ。デフォルトは 75 % です。 (注) この警告は、[Warning-Only] チェックボックスがオンかどうかに関係なくトリガーされます。
When maximum routes reached	再配布ルートの最大数に達したときに実行するアクション。 <ul style="list-style-type: none"> • [Enforce Maximum Route] : 定義された最大プレフィックス値に達した場合、ルートがそれ以上再配布されないようにします。これがデフォルトです。 • [Warning Only] : ルートの最大数に達したときに警告を表示しますが、追加のルートの再配布は抑止しません。

Cisco IOS ルータにおける RIP ルーティング



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

Routing Information Protocol (RIP; ルーティング情報プロトコル) は、小規模な同種のネットワークで使用するために作成された Interior Gateway Protocol (IGP) です。RIP は距離ベクトル型プロトコルであり、定期的な間隔 (アドバタイジングと呼ばれるプロセス) でルーティング更新メッセージを送信します。また、ネットワークトポロジが変更されるたびに更新メッセージを送信します。ルータは、エントリの変更が含まれるルーティングアップデートを受け取ると、新しいルートを反映するようにそのルーティングテーブルを更新します。別のルータから更新を 180 秒以上受信しない場合、ルータは更新のないルータによって提供されるルートを使用不可としてマークします。240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティングテーブルエントリをすべて削除します。ルーティング情報は UDP パケットを使用して交換されます。

RIP は、送信元から宛先へのホップ数 (通過したルータの数) を測定することによってルートの評価します。直接接続されているネットワークのメトリックは 0 です。RIP で許可される最大ホップカウントは 15 です。ホップカウントが 15 を超えるルートは、到達不能と見なされます。

Security Manager では、RFC 1723 に記載されている RIP バージョン 2 だけがサポートされます。RIP 2 ではオリジナルの RIP が改善されており、RIP メッセージでより多くの情報を伝送できます。これにより、単純な認証メカニズム (クリアテキストまたは MD5) を使用してテーブル更新を保護できます。RIP 2 では、サブネットマスクもサポートされています。これは、元のバージョンの RIP では使用できなかった重要な機能です。

ここでは、RIP ルーティングポリシーを作成するために実行するタスクについて説明します。

- [RIP 設定パラメータの定義 \(55 ページ\)](#)
- [RIP インターフェイス認証設定の定義 \(56 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)

関連項目

- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)
- [Cisco IOS ルータにおける EIGRP ルーティング \(10 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

RIP 設定パラメータの定義

RIP 設定パラメータを定義するには、ルートに含めるネットワークを選択し、いずれかのインターフェイスを受動にする必要があるかどうかを決定します。これらのインターフェイスは、ネイバーにルーティング更新を送信しません。また、自動サマライズをイネーブルにすると、ルータが維持するルーティング テーブルのサイズと複雑さを軽減できます。

関連項目

- [RIP インターフェイス認証設定の定義 \(56 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP]** を選択し、作業領域の **[セットアップ (Setup)]** タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、**[セットアップ (Setup)]** タブをクリックします。

RIP の **[Setup]** タブが表示されます ([\[RIP\] ページ - \[Setup\] タブ \(58 ページ\)](#) を参照)。

ステップ 2 インターフェイスで RIP 更新を受信する、直接接続されているネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、アドレスをカンマで区切ることができます。 **[選択 (Select)]** をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいネットワーク/ホストオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#)を参照してください。

ステップ 3 受動インターフェイスのアドレスを入力します。これは、ネイバーにルーティング更新 (存在する場合) を送信しないインターフェイスです。これらのインターフェイスは、引き続き RIP ルーティングブロード

キャストを受信し、それを使用してルーティングテーブルに読み込みます。1つ以上のインターフェイスの名前またはインターフェイスのロールを入力します。アドレスをカンマで区切ります。[選択 (Select)] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイスロールオブジェクトを作成します。詳細については、[ポリシー定義中のインターフェイスの指定](#)を参照してください。

ステップ 4 (任意) [自動集約 (Auto Summary)] チェックボックスをオンにして、ネットワークレベルルートへのサブネットルートの自動集約を有効にします。サマライズによってルーティングテーブルのサイズが削減されるため、ネットワークの複雑さが低減します。

切断されているサブネット間のルーティングを実行する場合は、自動サマライズをディセーブルにします。自動サマライズをオフにすると、サブネットがアドバタイズされます。

RIP インターフェイス認証設定の定義

RIP インターフェイスのネイバー認証設定を定義するには、インターフェイスを選択し、認証タイプ (MD5 またはクリア テキスト) を選択します。

関連項目

- [RIP 設定パラメータの定義 \(55 ページ\)](#)
- [OSPF へのルートの再配布 \(28 ページ\)](#)
- [Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP] を選択し、作業領域の [認証 (Authentication)] タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから **[Router Platform]** > **[Routing]** > **[RIP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[認証 (Authentication)] タブをクリックします。

RIP の [Authentication] タブが表示されます。このタブのフィールドの説明については、[表 21 : RIP の \[Authentication\] タブ \(60 ページ\)](#) を参照してください。

ステップ 2 RIP の [認証 (Authentication)] タブで、テーブルからインターフェイス定義を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックして定義を作成します。[RIP Authentication] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 22 : \[RIP Authentication\] ダイアログボックス \(61 ページ\)](#) を参照してください。

ステップ 3 認証が定義されるインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択 (Select)] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、[ポリシー定義中のインターフェイスの指定](#)を参照してください。

ステップ 4 インターフェイス認証 (MD5 またはクリア テキスト) を定義します。

- (注) RIP パケットでクリア テキスト認証を使用することは推奨しません。これは、暗号化されない認証キーがすべてのパケットで送信されるためです。プレーンテキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたインターフェイスが、RIP の [Authentication] タブに表示されます。

RIP へのルートの再配布

再配布とは、RIP などのルーティング プロトコルを使用して、他の方法（別のルーティング プロトコルなど）で学習されたルート、スタティックルート、または直接接続されたルートをアドバタイズすることです。たとえば、OSPF ルーティング プロトコルから RIP ルートにルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベース ルーティング プロトコルに適用できます。

RIP に再配布する場合、透過的に再配布することによって、ルートの元のメトリックを保持できます。

はじめる前に

- 少なくとも 1 つの RIP ルートを定義します。 [RIP 設定パラメータの定義](#) (55 ページ) を参照してください。

関連項目

- [RIP 設定パラメータの定義](#) (55 ページ)
- [RIP インターフェイス認証設定の定義](#) (56 ページ)
- [Cisco IOS ルータにおける RIP ルーティング](#) (54 ページ)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP] を選択し、作業領域の [再配布 (Redistribution)] タブをクリックします。
- (ポリシービュー) ポリシータイプセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[再配布 (Redistribution)] タブをクリックします。

RIP の [Redistribution] タブが表示されます。このタブのフィールドの説明については、[表 23 : RIP の \[Redistribution\] タブ](#) (62 ページ) を参照してください。

ステップ 2 RIP の [再配布 (Redistribution)] タブで、[RIP再配布マッピング (RIP Redistribution Mappings)] テーブルから行を選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックしてマッピングを作成します。[RIP Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールド

ドの説明については、[表 24 : \[RIP Redistribution Mapping\] ダイアログボックス \(63 ページ\)](#) を参照してください。

ステップ 3 RIP にルート再配布するプロトコルを選択します。

(注) スタティック ルート、BGP AS、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 4 次のいずれかの操作を実行して、再配布されるルートのメトリック（コスト）を定義します。

- [デフォルトメトリック (Default Metric)]チェックボックスをオンにし、再配布されるルートのデフォルトメトリックを入力します。メトリックによって、ルートのプライオリティが決まります。
- [トランスペアレント (Transparent)]チェックボックスをオンにし、RIP に再配布されるルートの元のメトリックを保持します。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、RIP の [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

[RIP] ルーティングポリシー ページ

RIP は、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティングプロトコルです。Security Manager では、RIP バージョン 2 だけがサポートされます。これには、ルーティング更新の交換時のネイバー認証のサポートが含まれています。

[RIP] ルーティング ページの次のタブから、RIP ルーティング ポリシーを設定できます。

- [\[RIP\] ページ - \[Setup\] タブ \(58 ページ\)](#)
- [\[RIP\] ページ - \[Authentication\] タブ \(60 ページ\)](#)
- [\[RIP\] ページ - \[Redistribution\] タブ \(62 ページ\)](#)

詳細については、[Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#) を参照してください。

ナビゲーションパス

- (デバイスビュー) ポリシーセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP]** を選択します。
- (ポリシービュー) ポリシータイプセクタから **[プラットフォーム (Platform)] > [ルーティング (Routing)] > [RIP]** を選択します。[RIP] を右クリックしてポリシーを作成するか、または共有ポリシーセクタから既存のポリシーを選択します。

[RIP] ページ - [Setup] タブ

RIP の [Setup] タブを使用して、RIP ルートを作成、編集、および削除します。

ナビゲーションパス

[RIP] ルーティングポリシー ページ (58 ページ) に移動し、[セットアップ (Setup)] タブをクリックします。

関連項目

- RIP 設定パラメータの定義 (55 ページ)
- [RIP] ページ - [Authentication] タブ (60 ページ)
- [RIP] ページ - [Redistribution] タブ (62 ページ)
- ポリシー定義中の IP アドレスの指定
- ネットワーク/ホストオブジェクトについて

フィールドリファレンス

表 20: RIP の [Setup] タブ

要素	説明
ネットワーク	RIP ルートに関連付けられる直接接続されたネットワーク。1 つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトをカンマで区切って入力します。[選択 (Select)] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
パッシブインターフェイス	ルーティングネイバーに更新を送信しないインターフェイス。1 つ以上のインターフェイス名またはロールをカンマで区切って入力します。[選択 (Select)] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。
自動集約 (Auto-Summary)	<p>選択されている場合は、ネットワークレベルルートへのサブネットルートの自動サマライズをイネーブルにします。サマライズによってルーティング テーブルのサイズが削減されるため、ネットワークの複雑さが低減します。</p> <p>選択解除されている場合、自動サマライズはディセーブルになります。</p> <p>(注) 切断されているサブネット間のルーティングを実行する場合は、自動サマライズをディセーブルにします。この機能をディセーブルにすると、サブネットがアドバタイズされます。</p>

[RIP] ページ - [Authentication] タブ

RIP の [Authentication] タブを使用して、RIP インターフェイスのネイバー認証設定を表示、作成、編集、および削除します。

ナビゲーションパス

[RIP] ルーティングポリシー ページ (58 ページ) に移動し、[認証 (Authentication)] タブをクリックします。

関連項目

- RIP インターフェイス認証設定の定義 (56 ページ)
- [RIP] ページ - [Setup] タブ (58 ページ)
- [RIP] ページ - [Redistribution] タブ (62 ページ)
- [RIP] ルーティングポリシー ページ (58 ページ)
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールドリファレンス

表 21: RIP の [Authentication] タブ

要素	説明
インターフェイス	RIP をイネーブルにするインターフェイスの名前 (インターフェイスロールによって定義)。
認証	選択したインターフェイス ロールでイネーブルにする RIP ネイバー認証のタイプ (クリアテキストまたは MD5)。
Key ID	MD5 認証に使用される認証キーの識別番号。
[追加 (Add)] ボタン	[RIP Authentication] ダイアログボックス (61 ページ) が開きます。ここから、その他の RIP インターフェイスの認証を定義できます。
[編集 (Edit)] ボタン	[RIP Authentication] ダイアログボックス (61 ページ) が開きます。ここから、選択した RIP インターフェイスの認証プロパティを編集できます。
[削除 (Delete)] ボタン	選択した認証定義をテーブルから削除します。

[RIP Authentication] ダイアログボックス

[RIP Authentication] ダイアログボックスを使用して、RIP インターフェイスのネイバー認証プロパティを追加または編集します。

ナビゲーションパス

[RIP] ページ - [Authentication] タブ (60 ページ) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [RIP インターフェイス認証設定の定義 \(56 ページ\)](#)

フィールドリファレンス

表 22: [RIP Authentication] ダイアログボックス

要素	説明
インターフェイス (Interface)	<p>認証プロパティを定義するインターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。</p> <p>(注) 同じインターフェイスに対して異なる認証設定を指定することはできません。</p>
認証	<p>インターフェイスに適用する認証のタイプ。</p> <ul style="list-style-type: none"> • [MD5] : (推奨) 認証に MD5 ハッシュ アルゴリズムを使用します。 • [Clear Text] : 認証にクリア テキストを使用します。 <p>(注) プレーン テキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。</p>
Key ID	<p>認証タイプとして [MD5] を選択した場合にだけ使用できます。</p> <p>認証キーの識別番号。この番号は、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は 0 ~ 2147483647 です。</p>

要素	説明
キー (Key)	<p>認証 (MD5 またはクリア テキスト) に使用される共有キー。このキーは、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。</p> <p>キーには最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースを使用できます。確認フィールドでもう一度キーを入力します。</p>

[RIP] ページ - [Redistribution] タブ

RIP の [Redistribution] タブを使用して、RIP ルーティング ドメインへの再配布を実行するときの再配布設定を表示、作成、編集、および削除します。



(注) RIP の [Redistribution] タブにアクセスする前に、RIP 設定パラメータを定義する必要があります。[RIP] ページ - [Setup] タブ (58 ページ) を参照してください。

ナビゲーションパス

[RIP] ルーティング ポリシー ページ (58 ページ) に移動し、[再配布 (Redistribution)] タブをクリックします。

関連項目

- [RIP へのルートの再配布 \(57 ページ\)](#)
- [\[RIP\] ページ - \[Authentication\] タブ \(60 ページ\)](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 23: RIP の [Redistribution] タブ

要素	説明
プロトコル	再配布されているプロトコル。
[AS/プロセス ID (AS/Process ID)]	再配布されているルートの自律システム (AS) 番号またはプロセス ID。
メトリック (Metric)	再配布されるルートのプライオリティを決定する値。
一致 (Match)	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。

要素	説明
[追加 (Add)] ボタン	[RIP Redistribution Mapping] ダイアログボックス (63 ページ) が開きます。ここから、RIP 再配布マッピングを定義できます。
[編集 (Edit)] ボタン	[RIP Redistribution Mapping] ダイアログボックス (63 ページ) が開きます。ここから、選択したRIP再配布マッピングを編集できます。
[削除 (Delete)] ボタン	選択した再配布マッピングをテーブルから削除します。

[RIP Redistribution Mapping] ダイアログボックス

[RIP Redistribution Mapping] ダイアログボックスを使用して、RIP 再配布マッピングのプロパティを追加または編集します。

ナビゲーションパス

[RIP] ページ - [Redistribution] タブ (62 ページ) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [RIP へのルートの再配布 \(57 ページ\)](#)

フィールドリファレンス

表 24 : [RIP Redistribution Mapping] ダイアログボックス

要素	説明
Protocol to Redistribute	再配布されているルーティングプロトコル。 <ul style="list-style-type: none"> • [Static] : スタティックルートを再配布します。ルートごとに1つのマッピングを定義できます。 • [EIGRP] : EIGRP自律システムを再配布します。表示されるフィールドにAS番号を入力します。ASごとに1つのマッピングを定義できます。 • [BGP] : BGP自律システムを再配布します。デバイスごとに1つのBGPマッピングを定義できます。[BGP Setup] タブで[BGP AS]を設定した場合は、AS番号が表示されます。それ以外の場合は、BGPASが定義されていないことを示すメッセージが表示されます。 [BGP] ページ - [Redistribution] タブ (8 ページ) を参照してください。

要素	説明
Protocol to Redistribute (続き)	<ul style="list-style-type: none"> • [OSPF] : 別の OSPF プロセスを再配布します。プロセスごとに1つのマッピングを定義できます。表示されるリストからプロセスを選択し、1つ以上の一致基準を選択します。 <ul style="list-style-type: none"> • [Internal] : 特定の AS の内部のルート。 • [External1] : AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1] : AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area (NSSA) ルート。 • [NSAAExternal2] : AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる (NSSA) ルート。 • [Connected] : インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
デフォルトメトリック (Default Metric)	再配布されるルートのデフォルト値を設定します。有効値の範囲は 0 ~ 16 です。
Transparent Metric	選択すると、再配布されるルートの元のメトリックが保持されます。選択を解除すると、[Metric] フィールドで指定した値が使用されます。

Cisco IOS ルータにおけるスタティックルーティング



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

ルートを動的に構築できない場合にパケットがルータによって宛先に正しく転送されるように、スタティックルーティングポリシーを設定できます。スタティックルートにはデフォルトでアドミニストレーティブディスタンス 1 (直接接続されたネットワークを意味する) が設定されるため、デフォルトでは、同じホストまたはネットワークに対して検出されたダイナミックルートよりも優先されます。ただし、対応するダイナミックルートよりも優先されないように、大きな値のアドミニストレーティブディスタンスをスタティックルートに定義できます。

たとえば、EIGRP ルートには、デフォルトでアドミニストレーティブ ディスタンス 5 が設定されます。スタティック ルートよりも EIGRP ルートが優先されるようにするには、5 よりも大きいアドミニストレーティブ ディスタンスを指定する必要があります。この機能は、スタティックルートを「フローティング」ルートとして定義する場合に役立ちます。フローティングルートは、優先ルートを使用できない場合にのみルーティングテーブルに挿入されます。



ヒント スタティックルートをバックアップの「フローティング」ルートとして使用する場合は、特定の IP アドレスを入力する代わりに、ネクストホップ IP アドレスに到達できるインターフェイスを指定します。そうしないと、プライマリリンクに障害が発生したときに、「フローティング」ルートはルーティングテーブルに挿入されません。詳細については、Cisco.com の次の URL で『*Specifying a Next Hop IP Address for Static Routes*』を参照してください。http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml [英語]

関連項目

- [スタティック ルートの定義 \(65 ページ\)](#)

スタティック ルートの定義

スタティックルートを定義するには、選択したホストまたはネットワーク宛の packets をルータが転送するホップ ゲートウェイの IP アドレス（および、任意でメトリック）を定義する必要があります。必要な数のスタティック ルートを定義できます。

関連項目

- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)
- [Cisco IOS ルータにおける RIP ルーティング \(54 ページ\)](#)
- [Cisco IOS ルータにおける OSPF ルーティング \(25 ページ\)](#)
- [Cisco IOS ルータにおける EIGRP ルーティング \(10 ページ\)](#)
- [Cisco IOS ルータにおける BGP ルーティング \(1 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [スタティックルーティング (Static Routing)] を選択します。
- (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [スタティックルーティング (Static Routing)] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Static Routing] ページが表示されます。このページのフィールドの説明については、[表 25 : \[Static Routing\] ページ \(67 ページ\)](#) を参照してください。

- ステップ 2** [スタティックルーティング (Static Routing)] ページで、テーブルからスタティックルートを選択し、[編集 (Edit)] をクリックするか、[追加 (Add)] をクリックしてルートを作成します。[Static Routing] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[表 26 : \[Static Routing\] ダイアログボックス \(69 ページ\)](#) を参照してください。
- ステップ 3** (任意) [デフォルトルートとして使用 (Use as Default Route)] チェックボックスをオンにして、このルートを不明なすべてのアウトバウンドパケットのデフォルトルートにします。
- ステップ 4** [プレフィックス (Prefix)] フィールドに、宛先ネットワークのアドレスを入力します。または、[選択 (Select)] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。
- ステップ 5** 転送オプションを選択します。
- パケットをリモートネットワークに転送するルータインターフェイスを定義するには、[転送インターフェイス (Forwarding Interface)] を選択し、インターフェイスまたはインターフェイスロールの名前を入力します。[Select] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成できます。[インターフェイスロールオブジェクトについておよびポリシーのオブジェクトの選択](#) を参照してください。
 - パケットを受信してリモートネットワークに転送するネクストホップルータを指定するには、[転送 IP (Forwarding IP)] を選択し、表示されるフィールドにアドレスを入力します。または、[選択 (Select)] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。詳細については、[ポリシー定義中の IP アドレスの指定](#) を参照してください。
- ステップ 6** (任意) [Distance Metric] フィールドに、このルータのネクストホップアドレスへのホップ数を入力します。このメトリックは、スタティックルートのプライオリティを示します。2つのルーティングエントリで同じネットワークが指定されている場合は、メトリック値の小さい (つまり、コストが低い) ルートに高いプライオリティが与えられ、選択されます。
- 値を指定しない場合、デフォルトは 1 であり、直接接続されたネットワークを意味します。
- ステップ 7** (任意) [永続的なルート (Permanent route)] チェックボックスをオンにして、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、このスタティックルートエントリが削除されないようにします。
- ステップ 8** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。スタティックルートが、[Static Routing] ページのテーブルに表示されます。

[Static Routing] ポリシー ページ

[Static Routing] ページを使用して、スタティックルートを作成、編集、および削除します。詳細については、[スタティックルートの定義 \(65 ページ\)](#) を参照してください。

ナビゲーションパス

- (デバイスビュー) ポリシーセクタから [プラットフォーム (Platform)] > [ルーティング (Routing)] > [スタティックルーティング (Static Routing)] を選択します。
- (ポリシービュー) ポリシータイプセクタから [ルータプラットフォーム (Router Platform)] > [ルーティング (Routing)] > [スタティックルーティング (Static Routing)] を選択します。 [スタティックルーティング (Static Routing)] を右クリックしてポリシーを作成するか、共有ポリシーセクタから既存のポリシーを選択します。

関連項目

- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)
- [テーブル カラムおよびカラム見出しの機能](#)
- [テーブルのフィルタリング](#)

フィールドリファレンス

表 25: [Static Routing] ページ

要素	説明
プレフィックス (Prefix)	スタティック ルートの宛先 IP アドレス。
Prefix Mask	選択した IP アドレスのネット マスク。
Default Route	スタティックルートがこのルータによって転送される不明なパケットのデフォルト ルートかどうかを示します。
Interface or IP Address	このルータのネクスト ホップ アドレスであるゲートウェイ ルータに関連付けられる IP アドレスまたはインターフェイス名。
距離	ゲートウェイ IP から宛先へのホップ数。メトリックによって、このルートのプライオリティが決まります。ホップが少ないほど、コストが低くなるため、ルートに割り当てられるプライオリティは高くなります。 2つのルーティング エントリで同じネットワークが指定されている場合、メトリックの小さい (つまり、プライオリティが高い) エントリが選択されます。
Permanent Route	スタティックルートが永続的なルートとして定義されるかどうかを示します。永続的なルートとは、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、削除されないことを意味します。

要素	説明
[追加 (Add)] ボタン	[Static Routing] ダイアログボックス (68 ページ) が開きます。ここから、スタティック ルートを作成できます。
[編集 (Edit)] ボタン	[Static Routing] ダイアログボックス (68 ページ) が開きます。ここから、選択したスタティック ルートを編集できます。
[削除 (Delete)] ボタン	選択したスタティック ルートをテーブルから削除します。

[Static Routing] ダイアログボックス

[Static Routing] ダイアログボックスを使用して、スタティック ルートを追加または編集します。

ナビゲーションパス

[\[Static Routing\] ポリシー ページ \(66 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

関連項目

- [スタティック ルートの定義 \(65 ページ\)](#)
- [Cisco IOS ルータにおけるスタティック ルーティング \(64 ページ\)](#)

フィールドリファレンス

表 26 : [Static Routing] ダイアログボックス

要素	説明
宛先ネットワーク	<p>このスタティックルートによって定義される宛先ネットワークのアドレス情報。</p> <ul style="list-style-type: none"> • [Use as Default Route] : 選択すると、これをこのルータのデフォルトルートにします。デフォルトルートは、送信元から宛先へのルートが不明な場合、またはルータのルーティングテーブルで多数のルートを保持できない場合に使用されます。すべての不明な送信パケットはデフォルトルートで送信されます。 <p>選択を解除すると、このスタティックルートはデフォルトルートではありません。</p> <ul style="list-style-type: none"> • [Prefix] : 宛先ネットワークの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 <p>プレフィックスは、クラス A、B、または C ネットワークあるいはホスト IP である必要があります。ホスト IP は、不連続マスクが含まれていないかぎり、0 で開始できます。すべてのサブネットアドレスが有効です。</p>
Forwarding (Next Hop)	<p>宛先ネットワークにデータを転送する方式。</p> <ul style="list-style-type: none"> • [Forwarding Interface] : パケットをリモート ネットワークに転送するルータ インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 • [Forwarding IP] : パケットを受信してリモート ネットワークに転送するネクスト ホップルータの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択 (Select)] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Distance Metric	<p>宛先ネットワーク（ゲートウェイ IP）へのホップ数。値を指定しない場合、デフォルトは1です。範囲は1～255です。</p> <p>このメトリック（アドミニストレーティブディスタンスとも呼ばれる）は、指定したホストが存在するネットワークへのホップ数に基づくルートコストの測定値です。このホップカウントには、パケットが通過する必要があるすべてのネットワークが含まれています。宛先ネットワークも含まれます。したがって、直接接続されたネットワークのメトリックはすべて1です。</p> <p>メトリックはコストに基づくため、スタティックルートのプライオリティを識別するために使用されます。2つのルーティングエントリで同じネットワークが指定されている場合は、メトリック値の小さい（つまり、コストが低い）ルートに高いプライオリティが与えられ、選択されます。</p> <p>（注） 特定の状況では、スタティックルートにダイナミックルートよりも低いプライオリティ（大きいディスタンスメトリック）を割り当てると役立つ場合があります。この設定により、スタティックルートはダイナミックルートを使用できない場合のバックアップの「フローティング」ルートとして機能できます。</p>
Permanent route	<p>選択すると、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、このスタティックルートエントリは削除されません。</p> <p>選択を解除すると、このスタティックルートは削除可能です。</p>

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。