CHAPTER 39

# IP ユニキャスト ルーティングの設定

この章では、スイッチで IP Version 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。特に明記しない限り、*スイッチ*という用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。スイッチ スタックは、ネットワーク内のそれ以外のルータに対して、単一のルータとして動作し、認識されます。

スタティック ルーティング、Routing Information Protocol（RIP）などの基本的なルーティング機能は、IP ベース フィーチャ セットおよび IP サービス フィーチャ セットの両方で使用できます。拡張ルーティング機能およびその他のルーティング プロトコルを使用するには、スタンドアロン スイッチやスタック マスターで IP サービス フィーチャ セットをイネーブルにする必要があります。

（注） スイッチまたはスイッチ スタックが IP サービス フィーチャ セットを実行している場合は、IP Version 6（IPv6）ユニキャスト ルーティングをイネーブルにして、IPv4 トラフィックに加えて IPv6 トラフィックを転送するようインターフェイスを設定することもできます。スイッチに IPv6 を設定する手順については、第 40 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

IP ユニキャスト設定情報の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。この章で使用されるコマンドの構文および使用方法の詳細については、次のコマンド リファレンスを参照してください。これらのマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』

この章で説明する内容は、次のとおりです。


- 「IP ルーティングの概要」（P.39-2）
- 「ルーティングを設定する手順」（P.39-5）
- 「IP アドレス指定の設定」（P.39-6）
- 「IP ユニキャスト ルーティングのイネーブル化」（P.39-20）
- 「RIP の設定」（P.39-22）
- 「OSPF の設定」（P.39-28）
- 「EIGRP の設定」（P.39-39）
- 「BGP の設定」（P.39-48）「ISO CLNS ルーティングの設定」（P.39-71）
- 「Multi-VRF CE の設定」（P.39-82）

- 「プロトコル独立機能の設定」（P.39-97）
- 「IP ネットワークのモニタリングおよびメンテナンス」（P.39-114）

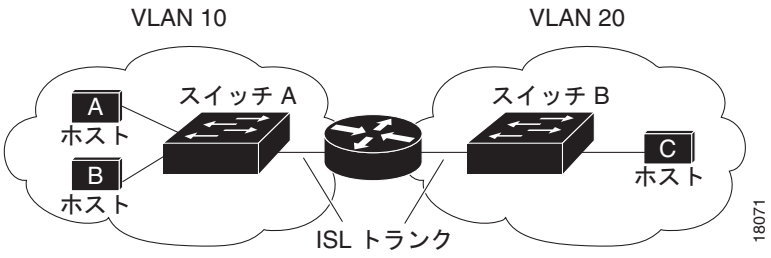
（注）　スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用し、ルーティング テンプレートに Switch Database Management（SDM）機能を設定します。SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」、またはこのリリースのコマンド リファレンスの **sdm prefer** コマンドを参照してください。

# IP ルーティングの概要

一部のネットワーク環境で、VLAN（仮想 LAN）は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャスト ドメインのサイズを制御し、ローカル トラフィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング（VLAN 間ルーティング）するレイヤ 3 デバイス（ルータ）が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 39-1 に基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。

**図 39-1　　ルーティング トポロジの例**




VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ここでは、ルーティングに関する次の内容について説明します。

- 「ルーティング タイプ」（P.39-3）
- 「IP ルーティングおよびスイッチ スタック」（P.39-3）

# ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラミングされているトラフィックのスタティック ルートの使用
- ルーティング プロトコルによるルートの動的な計算

デフォルト ルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しません。そのため、ネットワークの変更によってパケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

ルータは、次のダイナミック ルーティング プロトコルを使用して、トラフィックを転送するのに最適なルートをダイナミックに計算します。

- ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトル プロトコルは 1 つまたは複数のメトリックを使用し、最適なルートを計算します。
- リンクステート プロトコルを使用するルータでは、ルータ間の Link-State Advertisement（LSA; リンクステート アドバタイズメント）の交換に基づき、ネットワーク トポロジに関する複雑なデータベースを保持します。LSA はネットワークのイベントによって起動され、コンバージェンス時間、またはこれらの変更への対応時間を短縮します。リンクステート プロトコルはトポロジの変更にすばやく対応しますが、ディスタンスベクトル プロトコルよりも多くの帯域幅およびリソースを必要とします。

スイッチでサポートされているディスタンスベクトル プロトコルは、Routing Information Protocol（RIP）、最適パスを決定する単一の距離メトリック（コスト）、およびボーダー ゲートウェイ プロトコル（BGP）を使用します。BGP はパス ベクタ メカニズムを追加します。また、Open Shortest Path First（OSPF）リンクステート プロトコル、および従来の Interior Gateway Routing Protocol（IGRP）にリンクステート ルーティング機能の一部を追加して効率化を図った Enhanced IGRP（EIGRP）もサポートされています。

（注）　スイッチまたはスイッチ スタックでは、サポートされるプロトコルは、スイッチまたはスタック マスターで実行されているソフトウェアによって決まります。スイッチまたはスタック マスターが IP ベース フィーチャ セットを実行している場合は、デフォルト ルーティング、スタティック ルーティング、および RIP だけがサポートされます。その他のすべてのルーティング プロトコルには、IP サービス フィーチャ セットが必要です。

# IP ルーティングおよびスイッチ スタック

スタック内のどのスイッチがルーティング ピアに接続されているかに関係なく、ネットワークはスイッチ スタックを単一ルータとして認識します。スイッチ スタックの動作の詳細については、第 7 章「スイッチ スタックの管理」を参照してください。

スタック マスターは、次に示す機能を実行します。

- ルーティング プロトコルを初期化し、設定します。

- ルーティング プロトコル メッセージおよびアップデートを他のルータに送信します。
- ピア ルータから受信したルーティング プロトコル メッセージおよびアップデートを処理します。
- distributed Cisco Express Forwarding（dCEF）データベースを生成および維持し、すべてのスタック メンバーに配信します。このデータベースに基づいて、スタック内のすべてのスイッチにルートがプログラミングされます。
- スタック マスターの MAC アドレスはスタック全体のルータ MAC アドレスとして使用され、すべての外部デバイスはこのアドレスを使用して IP パケットをスタックに送信します。
- ソフトウェア転送またはソフトウェア処理を必要とするすべての IP パケットは、スタック マスターの CPU を通ります。

スタック メンバーは、次に示す機能を実行します。

- ルーティング スタンバイ スイッチとして機能します。スタック マスターに障害が発生し、新規スタック マスターとして選択された場合に、処理を引き継ぐことができます。
- ルートをハードウェアにプログラムします。スタック メンバーによってプログラムされたルートは、dCEF データベースの一部としてスタック マスターがダウンロードしたルートと同じです。

スタック マスターに障害が発生すると、スタックはスタック マスターがダウンしていることを検出し、スタック メンバーの 1 つを新規スタック マスターとして選択します。この期間中に、ハードウェアは一時的な中断を除き、アクティブなプロトコルがない状態でパケットの転送を継続します。

ただし、スイッチ スタックが障害のあとハードウェア ID を維持していても、スタック マスターの再起動前の短い中断の間にルータ ネイバーのルーティング プロトコルがフラップすることがあります。OSPF や EIGRP などのルーティング プロトコルは、ネイバーの移行を認識する必要があります。ルータは、次の 2 つのレベルの Nonstop Forwarding（NSF; ノンストップ フォワーディング）を使用して、切り替えを検出し、ネットワーク トラフィックの転送を続行して、ピア デバイスからルート情報を回復します。

- NFS 認識ルータによる障害の許容。隣接ルータの再起動後、NFS 認識ルータは要求を受けて自身のステート情報とルートの隣接情報を提供します。
- NFS 対応ルータによる NSF のサポート。NSF 対応ルータは、スタック マスターの変更を検出した場合、NFS 認識ネイバーまたは NSF 対応ネイバーからの情報でルーティング情報を再構築します。再起動を待つことはしません。

スイッチ スタックは NSF 対応ルーティングを OSPF および EIGRP に対してサポートします。詳細については、「OSPF NSF 対応」（P.39-31）および「EIGRP NSF 対応」（P.39-43）を参照してください。

新規スタック マスターは、選択されたときに次の機能を実行します。

- ルーティング アップデートの生成、受信、および処理を開始します。
- ルーティング テーブルを構築し、CEF データベースを生成して、スタック メンバーに配信します。
- ルータ MAC アドレスとして自身の MAC アドレスを使用します。新規 MAC アドレスのネットワーク ピアに通知するために、新規ルータ MAC アドレスを使用して余分の ARP 応答を定期的に（5 分間の間、数秒おきに）送信します。

**（注）** 固定 MAC アドレス機能をスタックに設定していて、スタック マスターに変更があった場合、設定された時間スタック MAC アドレスは変更されません。この期間に前のスタック マスターがメンバ スイッチとしてスタックに再加入する場合、スタック MAC アドレスは前のスタック マスターの MAC アドレスのままになります。「永続的 MAC アドレスのイネーブル化」（P.7-23）を参照してください。

- ARP 要求をプロキシ ARP IP アドレスに送信し、ARP 応答を受信して、各プロキシ ARP エントリの到達可能性を判別しようとします。到達可能なプロキシ ARP IP アドレスごとに、新規ルータ MAC アドレスを使用して gratuitous ARP 応答を生成します。このプロセスは、新規スタック マスターが選択されたあと、5 分間繰り返されます。

（注）　スタック マスターが IP サービス フィーチャ セットを実行している場合は、スタックは、Open Shortest Path First（OSPF）、Enhanced IGRP（EIGRP）、およびボーダー ゲートウェイ プロトコル（BGP）を含む、サポートされるすべてのプロトコルを実行できます。スタック マスターで障害が発生し、新しく選択されたスタック マスターが IP ベース フィーチャ セットを実行している場合は、これらのプロトコルはスタックでは実行されなくなります。

注意　スイッチ スタックで複数のスタックに分割すると、ネットワークで望ましくない動作を引き起こす可能性があります。

# ルーティングを設定する手順

スイッチ上で、IP ルーティングはデフォルトでディセーブルとなっているため、ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。IP ルーティング設定情報の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポートです。
- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）：**interface vlan** *vlan_id* グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポートチャネル論理インターフェイス。詳細については、「レイヤ 3 EtherChannel の設定」（P.38-16）を参照してください。

（注）　スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「ネットワーク インターフェイスへの IP アドレスの割り当て」（P.39-7）を参照してください。

スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。ソフトウェアに、設定できるルーテッド ポートおよび SVI の個数制限はありません。ただし、ハードウェアによって制限されるため、設定できるルーテッド ポートおよび SVI の個数と、実装されている機能の組み合わせによっては、CPU 利用率が影響を受けることがあります。システム メモリをルーティング用に最適化するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用します。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチまたはスイッチ スタックで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、第 13 章「VLAN の設定」を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルに設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します（任意）。

# IP アドレス指定の設定

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。ここでは、さまざまな IP アドレス指定機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- 「アドレス指定のデフォルト設定」（P.39-6）
- 「ネットワーク インターフェイスへの IP アドレスの割り当て」（P.39-7）
- 「アドレス解決方法の設定」（P.39-10）
- 「IP ルーティングがディセーブルの場合のルーティング支援機能」（P.39-13）
- 「ブロードキャスト パケットの処理方法の設定」（P.39-15）
- 「IP アドレスのモニタリングおよびメンテナンス」（P.39-19）

## アドレス指定のデフォルト設定

表 39-1 に、アドレス指定のデフォルト設定を示します。

**表 39-1　アドレス指定のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| IP アドレス | 未定義 |
| ARP | ARP キャッシュに永続的なエントリはありません<br>カプセル化：標準イーサネット形式の ARP<br>14400 秒（4 時間） |
| IP ブロードキャスト アドレス | 255.255.255.255（すべて 1） |
| IP クラスレス ルーティング | イネーブル |
| IP デフォルト ゲートウェイ | ディセーブル |
| IP ダイレクト ブロードキャスト | ディセーブル（すべての IP ダイレクト ブロードキャストがドロップされます） |

表 39-1　アドレス指定のデフォルト設定 （続き）

| 機能 | デフォルト設定 |
|---|---|
| IP ドメイン | ドメイン リスト：ドメイン名は未定義<br>ドメイン検索：イネーブル<br>ドメイン名：イネーブル |
| IP 転送プロトコル | ヘルパー アドレスが定義されているか、またはユーザ データグラム プロトコル（UDP）フラッディングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります<br>ローカル ブロードキャスト：ディセーブル<br>スパニングツリー プロトコル（STP）：ディセーブル<br>ターボフラッディング：ディセーブル |
| IP ヘルパー アドレス | ディセーブル |
| IP ホスト | ディセーブル |
| ICMP Router Discovery Protocol（IRDP） | ディセーブル<br>イネーブルの場合のデフォルト：<br>• ブロードキャスト IRDP アドバタイズメント<br>• アドバタイズメント間の最大インターバル：600 秒<br>• アドバタイズメント間の最小インターバル：最大インターバルの 0.75 倍<br>• プリファレンス：0 |
| IP プロキシ ARP | イネーブル |
| IP ルーティング | ディセーブル |
| IP サブネットゼロ | ディセーブル |

# ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166 [Internet Numbers] には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

IP アドレスおよびネットワーク マスクをレイヤ 3 インターフェイスに割り当てるには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **no switchport** | レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **ip address** *ip-address subnet-mask* | IP アドレスおよび IP サブネット マスクを設定します。 |
| ステップ 5 | **no shutdown** | インターフェイスをイネーブルにします。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show interfaces** [*interface-id*]<br>**show ip interface** [*interface-id*]<br>**show running-config interface** [*interface-id*] | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

## サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなってしまいます。

すべてが 1 のサブネット（131.108.255.0）は使用可能です。IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

サブネット ゼロをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip subnet-zero** | インターフェイス アドレスおよびルーティングのアップデート時にサブネット ゼロの使用をイネーブルにします。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

## クラスレス ルーティング

ルーティングを行うよう設定されたスイッチで、クラスレス ルーティングはデフォルトでイネーブルになっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットをルータが受信すると、ルータは最適なスーパーネット ルートにパケットを転送します。スーパーネットは、単一の大規模アドレス空間をシミュレーションするクラス C アドレス空間の連続ブロックであり、クラス B アドレス空間の急速な枯渇を回避するために設計されました。

図 39-2 では、クラスレス ルーティングがイネーブルとなっています。ホストがパケットを 120.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛てパケットを受信したルータは、パケットを廃棄します。

図 39-2　IP クラスレス ルーティングがイネーブルの場合

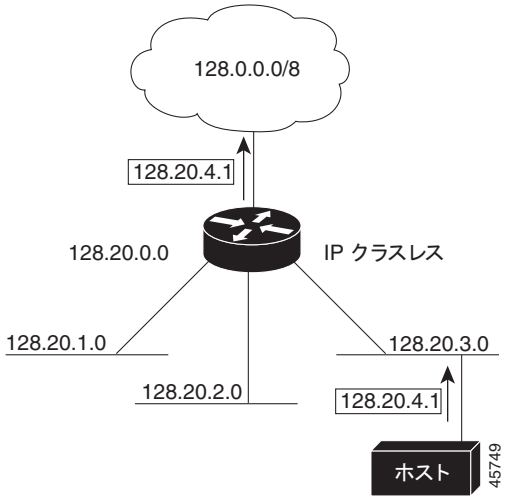
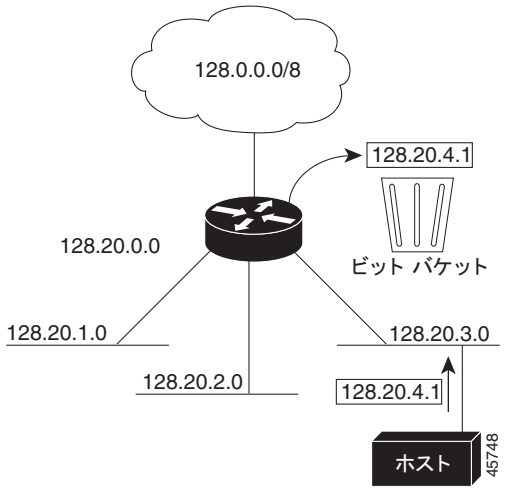



図 39-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ホストがパケットを 120.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 39-3　IP クラスレス ルーティングがディセーブルの場合




認識されないサブネット宛てのパケットが最適なスーパーネット ルートに転送されないようにするには、クラスレス ルーティング動作をディセーブルにします。

クラスレス ルーティングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **no ip classless** | クラスレス ルーティング動作をディセーブルにします。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **show running-config** | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルトに戻して、ネットワークのデフォルト ルートがないネットワークのサブネット宛パケットが、スイッチによって最適なスーパーネット ルートに転送されるようにするには、**ip classless** グローバル コンフィギュレーション コマンドを使用します。

# アドレス解決方法の設定

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレス（MAC アドレス）と、デバイスが属するネットワークを特定するネットワーク アドレスがあります。

（注）　スイッチ スタックでは、スタックの単一の MAC アドレスおよび IP アドレスを使用して、ネットワーク通信を行います。

ローカル アドレス（MAC アドレス）は、パケット ヘッダーのデータ リンク層（レイヤ 2）セクションに格納され、データ リンク（レイヤ 2）デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。イーサネット デバイスと通信するには、ソフトウェアがデバイスの MAC アドレスを判別する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、「*アドレス解決*」と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、「*逆アドレス解決*」と呼びます。

スイッチでは、次のタイプのアドレス解決を使用します。

- アドレス解決プロトコル（ARP）は、IP アドレスを MAC アドレスと関連付けます。ARP は IP アドレスを入力として使用し、関連付けられた MAC アドレスを判別します。次に、IP アドレス /MAC アドレスの関連付けを ARP キャッシュに格納し、すぐに取り出せるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で規定されています。
- プロキシ ARP：ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ（ルータ）が、ARP 要求の送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能（ローカル MAC アドレスでなく IP アドレスを要求する点を除く）を持つ Reverse Address Resolution Protocol（RARP）を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server** *address* インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

アドレス解決を設定するために必要な作業は次のとおりです。

- 「スタティック ARP キャッシュの定義」（P.39-11）

- 「ARP カプセル化の設定」（P.39-12）
- 「プロキシ ARP のイネーブル化」（P.39-12）


## スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間をダイナミックにマッピングできます。ほとんどのホストではダイナミック アドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するために使用される永続的なエントリを、ARP キャッシュに確保できます。指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

IP アドレスと MAC アドレスの間でスタティック マッピングを行うには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **arp** *ip-address hardware-address type* | ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。<br>• **arpa**：ARP カプセル化（イーサネット インターフェイス用）<br>• **snap**：SNAP カプセル化（トークン リングおよび FDDI インターフェイス用）<br>• **sap**：HP の ARP タイプ |
| ステップ 3 | **arp** *ip-address hardware-address type* [*alias*] | （任意）指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。 |
| ステップ 4 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 5 | **arp timeout** *seconds* | （任意）ARP キャッシュ エントリがキャッシュに保持される期間を設定します。指定できる範囲は 0 ～ 2147483 秒です。デフォルト値は 14400 秒（4 時間）です。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show interfaces** [*interface-id*] | すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。 |
| ステップ 8 | **show arp**<br>または<br>**show ip arp** | ARP キャッシュの内容を表示します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ARP キャッシュからエントリを削除するには、**no arp** *ip-address hardware-address type* グローバル コンフィギュレーション コマンドを使用します。ARP キャッシュから非スタティック エントリをすべて削除するには、**clear arp-cache** 特権 EXEC コマンドを使用します。

## ARP カプセル化の設定

IP インターフェイスでは、イーサネット ARP 形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

ARP カプセル化タイプを指定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **arp** {**arpa** \| **snap**} | ARP カプセル化方法を指定します。<br>• **arpa** : ARP<br>• **snap** : SNAP |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show interfaces** [*interface-id*] | すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

## プロキシ ARP のイネーブル化

デフォルトでは、プロキシ ARP が使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

ディセーブルになっているプロキシ ARP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip proxy-arp** | インターフェイスでプロキシ ARP をイネーブルにします。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip interface** [*interface-id*] | 指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

インターフェイスでプロキシ ARP をディセーブルにするには、**no ip proxy-arp** インターフェイス コンフィギュレーション コマンドを使用します。

# IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。


- 「プロキシ ARP」（P.39-13）
- 「デフォルト ゲートウェイ」（P.39-13）
- 「IRDP」（P.39-14）


## プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカル イーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを調べます。最適なルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求を送信したホストはスイッチにパケットを送信し、スイッチはパケットを目的のホストに転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

プロキシ ARP は、デフォルトでイネーブルに設定されています。ディセーブル化されたプロキシ ARP をイネーブルにするには、「プロキシ ARP のイネーブル化」（P.39-12）を参照してください。プロキシ ARP は、他のルータでサポートされているかぎり有効です。

## デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行うか、IP Control Message Protocol（ICMP）リダイレクト メッセージを返信して、ホストが使用する必要があるローカル ルータを識別します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法では、いつデフォルト ルータで障害が発生したか、または使用不可であったかを検出できません。

IP ルーティングがディセーブルの場合にデフォルト ゲートウェイ（ルータ）を定義するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip default-gateway** *ip-address* | デフォルト ゲートウェイ（ルータ）を設定します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show ip redirects** | 設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

この機能をディセーブルにするには、**no ip default-gateway** グローバル コンフィギュレーション コマンドを使用します。

# IRDP

ルータ ディスカバリを使用すると、スイッチは ICMP Router Discovery Protocol（IRDP）を使用し、他のネットワークへのルートを動的に取得します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。スイッチは Routing Information Protocol（RIP）ルーティングの更新を受信し、この情報を使用してルータの場所を推測することもできます。実際のところ、ルーティング デバイスによって送信されたルーティング テーブルは、スイッチにストアされません。どのシステムがデータを送信しているのかが記録されるだけです。IRDP を使用する利点は、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると見なされるまでの期間の両方をルータごとに指定できることです。

検出された各デバイスは、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

インターフェイスで IRDP ルーティングを行う場合は、インターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータは変更可能です。

インターフェイス上で IRDP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip irdp** | インターフェイス上で IRDP 処理をイネーブルにします。 |
| ステップ 4 | **ip irdp multicast** | （任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズを送信します。<br>**（注）** このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。 |
| ステップ 5 | **ip irdp holdtime** *seconds* | （任意）アドバタイズが有効である IRDP 期間を設定します。デフォルト値は **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きな値（9000 秒以下）を指定する必要があります。**maxadvertinterval** 値を変更すると、この値も変更されます。 |
| ステップ 6 | **ip irdp maxadvertinterval** *seconds* | （任意）アドバタイズ間の IRDP の最大インターバルを設定します。デフォルト値は 600 秒です。 |
| ステップ 7 | **ip irdp minadvertinterval** *seconds* | （任意）アドバタイズ間の IRDP の最小インターバルを設定します。デフォルト値は **maxadvertinterval** 値の 0.75 倍です。**maxadvertinterval** を変更すると、この値も新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。 |
| ステップ 8 | **ip irdp preference** *number* | （任意）デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は $-2^{31}$ ～ $2^{31}$ です。デフォルトは 0 です。大きな値を設定すると、ルータのプリファレンス レベルも高くなります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 9 | **ip irdp address** *address* [*number*] | （任意）プロキシアドバタイズを行うために必要な IRDP アドレスとプリファレンスを指定します。 |
| ステップ 10 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 11 | **show ip irdp** | IRDP 値を表示し、設定を確認します。 |
| ステップ 12 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

**maxadvertinterval** 値を変更すると、**holdtime** 値と **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更してから、**holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

IRDP ルーティングをディセーブルにするには、**no ip irdp** インターフェイス コンフィギュレーション コマンドを使用します。

# ブロードキャスト パケットの処理方法の設定

IP インターフェイス アドレスを設定したあとで、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。スイッチでは、次の種類のブロードキャストがサポートされています。

- 特定のネットワークまたは一連のネットワークに送信される指定ブロードキャスト パケット。ダイレクト ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- すべてのネットワークに送信されるフラッディング ブロードキャスト パケット

（注）　**storm-control** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャスト トラフィックを制限することもできます。詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。

ルータはローカル ケーブル長を制限して、ブロードキャスト ストームを防ぎます。ブリッジ（インテリジェントなブリッジを含む）はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームを伝播します。ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。IP 実装機能ではほとんどの場合、ブロードキャスト アドレスを設定できます。スイッチをはじめ、多数の実装機能では、ブロードキャスト メッセージを転送するためのアドレス方式が複数サポートされています。

これらの方式をイネーブルにするには、次に示す作業を実行します。

- 「ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化」（P.39-16）
- 「UDP ブロードキャスト パケットおよびプロトコルの転送」（P.39-17）
- 「IP ブロードキャスト アドレスの確立」（P.39-18）
- 「IP ブロードキャストのフラッディング」（P.39-18）

## ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクト ブロードキャストがドロップされるため、転送されることはありません。IP ダイレクト ブロードキャストがドロップされると、ルータが DoS 攻撃（サービス拒絶攻撃）にさらされる危険が少なくなります。

ブロードキャストが物理（MAC レイヤ）ブロードキャストになる場合、インターフェイスでは IP 指定ブロードキャストの転送をイネーブルにできます。**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス コントロール リスト（ACL）を指定できます。ACL を指定した場合は、ACL で許可されている IP パケットだけを、指定ブロードキャストから物理ブロードキャストに変換できます。アクセス リストの詳細については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。

インターフェイス上で IP ダイレクト ブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 3 | **ip directed-broadcast** [*access-list-number*] | インターフェイス上で、ダイレクト ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御する ACL を含めることができます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが変換可能になります。<br>（注）　**ip directed-broadcast** インターフェイス コンフィギュレーション コマンドは VPN Routing/Forwarding（VRF; VPN ルーティング/転送）インターフェイスで設定でき、こうすると VRF 認識になります。ダイレクト ブロードキャスト トラフィックが VRF 内でだけルーティングされます。 |
| ステップ 4 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 5 | **ip forward-protocol** {**udp** [*port*] \| **nd** \| **sdns**} | ブロードキャスト パケットを転送するときに、ルータによって使用されるプロトコルおよびポートを指定します。<br>• **udp**：UDP データグラムを転送します。<br>*port*：（任意）転送される UDP サービスを制御する宛先ポートです。<br>• **nd**：ネットワーク ディスク データグラムを転送します。<br>• **sdns**：Secure Data Network Service（SDNS）データグラムを転送します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ip interface** [*interface-id*]<br>または<br>**show running-config** | 指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

指定ブロードキャストから物理ブロードキャストへの変換をディセーブルにするには、**no ip directed-broadcast** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

## UDP ブロードキャスト パケットおよびプロトコルの転送

ユーザ データグラム プロトコル（UDP）は IP のホスト間レイヤ プロトコルです。UDP は、2 つのエンド システム間のコネクションレスのセッションを提供しますが、受信されたデータグラムの確認応答は行いません。ネットワーク ホストは UDP ブロードキャストを使用し、アドレス、設定、および名前に関する情報を検索します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、UDP ブロードキャストは転送されないことがあります。ただし、特定のブロードキャスト クラスをヘルパー アドレスに転送するように、ルータのインターフェイスを設定できます。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk Protocol（NDP）も指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と NDP の両方の転送がイネーブルになっています。『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP フォワーディング エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol（DHCP）情報を伝達します。

インターフェイスで UDP ブロードキャスト パケットの転送をイネーブルにし、宛先アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip helper-address** *address* | 転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。 |
| ステップ 4 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 5 | **ip forward-protocol** {**udp** [*port*] \| **nd** \| **sdns**} | ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ip interface** [*interface-id*]<br>または<br>**show running-config** | 指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

特定アドレスへのブロードキャスト パケットの転送をディセーブルにするには、**no ip helper-address** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

## IP ブロードキャスト アドレスの確立

（デフォルトの）IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレスです（255.255.255.255）。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

インターフェイス上で IP ブロードキャスト アドレスを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 3 | **ip broadcast-address** *ip-address* | デフォルト値と異なるブロードキャスト アドレス（128.1.255.255 など）を入力します。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip interface** [*interface-id*] | 指定されたインターフェイスまたはすべてのインターフェイスのブロードキャスト アドレスを確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルトの IP ブロードキャスト アドレスに戻すには、**no ip broadcast-address** インターフェイス コンフィギュレーション コマンドを使用します。

## IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IP ヘルパー アドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットを、フラッディングできます。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります （これらの条件は、IP ヘルパー アドレスを使用する場合に転送するパケットについての条件と同じであることに注意してください）。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。
- パケットは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、ドメイン ネーム システム（DNS）、Time、NetBIOS、Network Disk、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの存続可能時間（TTL）値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスを設定します。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内に伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされた UDP データグラムがインターフェイスで送信される（場合によっては宛先アドレスが変更される）と、データグラムは通常の IP 出力ルーチンによって処理されます。このため、出力インターフェイスに ACL がある場合、データグラムはその影響を受けます。

ブリッジング スパニングツリー データベースを使用し、UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip forward-protocol spanning-tree** | ブリッジング スパニングツリー データベースを使用し、UDP データグラムをフラッディングします。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

IP ブロードキャストのフラッディングをディセーブルにするには、**no ip forward-protocol spanning-tree** グローバル コンフィギュレーション コマンドを使用します。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニングツリーベースの UDP フラッディングを約 4 ～ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

スパニングツリーベースのフラッディングを高速化するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip forward-protocol turbo-flood** | スパニングツリー データベースを使用し、UDP データグラムのフラッディングを高速化します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

この機能をディセーブルにするには、**no ip forward-protocol turbo-flood** グローバル コンフィギュレーション コマンドを使用します。

# IP アドレスのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になっている場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を削除できます。表 39-2 に、内容をクリアするために使用するコマンドを示します。

表 39-2　キャッシュ、テーブル、データベースをクリアするコマンド

| コマンド | 目的 |
|---|---|
| **clear arp-cache** | IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。 |
| **clear host** {*name* \| *}} | ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。 |
| **clear ip route** {*network* [*mask*] \|*} | IP ルーティング テーブルから 1 つまたは複数のルートを削除します。 |

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティング パスなど、特定の統計情報を表示できます。表 39-3 に、IP を消去および表示するために使用する特権 EXEC コマンドを示します。

表 39-3　キャッシュ、テーブル、データベースを表示するコマンド

| コマンド | 目的 |
|---|---|
| **show arp** | ARP テーブルのエントリを表示します。 |
| **show hosts** | デフォルトのドメイン名、検索サービスの方式、ネーム サーバ ホスト、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。 |
| **show ip aliases** | TCP ポートにマッピングされた IP アドレスを表示します（エイリアス）。 |
| **show ip arp** | IP ARP キャッシュを表示します。 |
| **show ip interface** [*interface-id*] | インターフェイスの IP ステータスを表示します。 |
| **show ip irdp** | IRDP 値を表示します。 |
| **show ip masks** *address* | ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。 |
| **show ip redirects** | デフォルト ゲートウェイのアドレスを表示します。 |
| **show ip route** [*address* [*mask*]] \| [*protocol*] | ルーティング テーブルの現在のステートを表示します。 |
| **show ip route summary** | ルーティング テーブルの現在のステートをサマリー形式で表示します。 |

# IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

IP ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip routing** | IP ルーティングをイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **router** *ip_routing_protocol* | IP ルーティング プロトコルを指定します。このステップでは、他のコマンドを実行することもできます。たとえば、**network**（RIP）ルータ コンフィギュレーション コマンドを使用し、ルーティングするネットワークを指定できます。具体的なプロトコルの詳細については、この章の後半および『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。<br>**（注）** IP ベース フィーチャ セットは、ルーティング プロトコルとして RIP だけをサポートします。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング プロトコルとして RIP を使用し、IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

ここで、選択したルーティング プロトコルのパラメータを設定できます。具体的な手順は次のとおりです。

- 「RIP の設定」（P.39-22）
- 「OSPF の設定」（P.39-28）
- 「EIGRP の設定」（P.39-39）
- 「BGP の設定」（P.39-48）
- 「uRPF の設定」（P.39-97）
- 「プロトコル独立機能の設定」（P.39-97）（任意）

# RIP の設定

Routing Information Protocol（RIP）は、小規模な同種ネットワーク間で使用するための Interior Gateway Protocol（IGP）です。RIP は、ブロードキャスト UDP データ パケットを使用してルーティング情報を交換するディスタンスベクトル ルーティング プロトコルです。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

（注）　RIP は、IP ベース フィーチャ セットによってサポートされる唯一のルーティング プロトコルです。その他のルーティング プロトコルでは、スイッチまたはスタック マスターが IP サービス フィーチャ セットを実行している必要があります。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート（アドバタイズメント）を送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマークされます。240 秒が経過してもアップデートが届かない場合、そのルータに関するすべてのルーティング テーブル エントリはルータによって削除されます。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由されるルータ数です。ホップ カウントの範囲は 0 ～ 15 です。直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達できません。範囲が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルト ネットワークが RIP によって取得された場合、またはルータが最終ゲートウェイで、RIP がデフォルト メトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しないと、RIP アップデート中にアドバタイズされません。

ここでは、次の設定について説明します。

- 「RIP のデフォルト設定」（P.39-23）
- 「基本的な RIP パラメータの設定」（P.39-24）
- 「RIP 認証の設定」（P.39-25）
- 「サマリー アドレスおよびスプリット ホライズンの設定」（P.39-26）

# RIP のデフォルト設定

表 39-4 に、RIP のデフォルト設定を示します。

**表 39-4　RIP のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| 自動サマリー | イネーブル |
| デフォルト情報送信元 | ディセーブル |
| デフォルト メトリック | 自動メトリック変換（組み込み） |
| IP RIP 認証キーチェーン | 認証なし<br>認証モード：クリア テキスト |
| IP RIP 受信バージョン | **version** ルータ コンフィギュレーション コマンドに準拠 |
| IP RIP 送信バージョン | **version** ルータ コンフィギュレーション コマンドに準拠 |
| IP RIP の起動 | **version** ルータ コンフィギュレーション コマンドに準拠 |
| IP スプリット ホライズン | メディアにより異なる |
| ネイバー | 未定義 |
| ネットワーク | 指定なし |
| オフセット リスト | ディセーブル |
| 出力遅延 | 0 ミリ秒 |
| タイマー基準 | • 更新：30 秒<br>• 無効：180 秒<br>• ホールドダウン：180 秒<br>• フラッシュ：240 秒 |
| アップデート送信元の検証 | イネーブル |
| バージョン | RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。 |

# 基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。RIP コンフィギュレーション コマンドは、ネットワーク番号を設定するまでスイッチでは無視されます。

RIP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip routing** | IP ルーティングをイネーブルにします。（IP ルーティングがディセーブルになっている場合だけ、必須です）。 |
| ステップ 3 | **router rip** | RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **network** *network number* | ネットワークを RIP ルーティング プロセスに関連付けます。複数の **network** コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。<br>**（注）** RIP コマンドを有効にするためにネットワーク番号を設定する必要があります。 |
| ステップ 5 | **neighbor** *ip-address* | （任意）ルーティング情報を交換する隣接ルータを定義します。このステップを使用すると、RIP（通常はブロードキャスト プロトコル）からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。 |
| ステップ 6 | **offset list** [*access-list number* \| *name*] {**in** \| **out**} *offset* [*type number*] | （任意）オフセット リストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。 |
| ステップ 7 | **timers basic** *update invalid holddown flush* | （任意）ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ～ 4294967295 秒です。<br>• *update*：ルーティング アップデートの送信間隔。デフォルトは 30 秒です。<br>• *invalid*：ルートが無効と宣言された後の時間。デフォルト値は 180 秒です。<br>• *holddown*：ルートがルーティング テーブルから削除されるまでの時間。デフォルト値は 180 秒です。<br>• *flush*：ルーティング アップデートが延期される時間。デフォルトは 240 秒です。 |
| ステップ 8 | **version** {**1** \| **2**} | （任意）RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトでは、スイッチはバージョン 1 とバージョン 2 を受信しますが、送信するのはバージョン 1 だけです。<br>インターフェイス コマンド **ip rip {send \| receive} version 1 \| 2 \| 1 2**} を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 9 | **no auto summary** | （任意）自動サマライズをディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィックスがサマライズされます。サマライズをディセーブルにし（RIP バージョン 2 だけ）、クラスフル ネットワーク境界にサブネットおよびホスト ルーティング情報をアドバタイズします。 |
| ステップ 10 | **no validate-update-source** | （任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の環境では、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。 |
| ステップ 11 | **output-delay** *delay* | （任意）送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなる RIP アップデートのパケットには、パケット間遅延時間は追加されません。パケットを低速なデバイスに送信する場合は、8 ～ 50 ミリ秒の範囲でパケット間遅延を追加できます。 |
| ステップ 12 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show ip protocols** | 設定を確認します。 |
| ステップ 14 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

RIP ルーティング プロセスをオフにするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと現在のステートを表示するには、**show ip protocols** 特権 EXEC コマンドを使用します。RIP データベースのサマリー アドレス エントリを表示するには、**show ip rip database** 特権 EXEC コマンドを使用します。

# RIP 認証の設定

RIP バージョン 1 では、認証がサポートされていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キー チェーンによって指定されます。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。「認証キーの管理」（P.39-112）に記載されている作業も実行してください。

スイッチは、RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という認証モードをサポートします。デフォルトはプレーン テキストです。

インターフェイスに RIP 認証を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 3 | **ip rip authentication key-chain** *name-of-chain* | RIP 認証をイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **ip rip authentication mode** [**text** \| **md5**} | プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config interface** [*interface-id*] | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を禁止するには、**no ip rip authentication key-chain** インターフェイス コンフィギュレーション コマンドを使用します。

# サマリー アドレスおよびスプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

**（注）** ルートを適切にアドバタイズするために、アプリケーションでスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。

サマライズされたローカル IP アドレスをアドバタイズし、インターフェイスのスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip address** *ip-address subnet-mask* | IP アドレスおよび IP サブネットを設定します。 |
| ステップ 4 | **ip summary-address rip** *ip address ip-network mask* | サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。 |
| ステップ 5 | **no ip split horizon** | 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ます。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ip interface** *interface-id* | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

IP サマライズをディセーブルにするには、**no ip summary-address rip** ルータ コンフィギュレーション コマンドを使用します。

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイスのギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

（注）　スプリット ホライズンがイネーブルである場合、（**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される）自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

# スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

（注）　ルートを適切にアドバタイズするために、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

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には、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 3 | **ip address** *ip-address subnet-mask* | IP アドレスおよび IP サブネットを設定します。 |
| ステップ 4 | **no ip split-horizon** | 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ます。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip interface** *interface-id* | 入力内容を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

スプリット ホライズン メカニズムをイネーブルにするには、**ip split-horizon** インターフェイス コンフィギュレーション コマンドを使用します。

# OSPF の設定

ここでは、OSPF の設定方法について簡単に説明します。OSPF コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「OSPF Commands」の章を参照してください。

**（注）** OSPF では、各メディアがブロードキャスト ネットワーク、非ブロードキャスト ネットワーク、ポイントツーポイント ネットワークに分類されます。スイッチでは、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）およびポイントツーポイント ネットワーク（ポイントツーポイント リンクとして設定されたイーサネット インターフェイス）がサポートされます。

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。

シスコの実装は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。ドメイン内レベルで、OSPF は EIGRP および RIP によって取得したルートを取り込むことができます。OSPF ルートを RIP に伝達することもできます。
- エリア内の隣接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータのデッド インターバルと hello インターバル、認証キーなどがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された *Area Border Router*（ABR; エリア境界ルータ）、および *Autonomous System Boundary Router*（ASBR; 自律システム境界ルータ）間で調整する必要があります。最小設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

ここでは、次の設定について説明します。

- 「OSPF のデフォルト設定」（P.39-29）
- 「基本的な OSPF パラメータの設定」（P.39-32）
- 「OSPF インターフェイスの設定」（P.39-33）
- 「OSPF エリア パラメータの設定」（P.39-34）
- 「その他の OSPF パラメータの設定」（P.39-35）
- 「LSA グループ ペーシングの変更」（P.39-37）
- 「ループバック インターフェイスの設定」（P.39-38）
- 「OSPF のモニタリング」（P.39-39）

# OSPF のデフォルト設定

表 39-5 に、OSPF のデフォルト設定を示します。

**表 39-5　OSPF のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| インターフェイス パラメータ | コスト：デフォルト コストは未定義<br>再送信インターバル：5 秒<br>送信遅延：1 秒。<br>プライオリティ：1<br>hello インターバル：10 秒<br>デッド インターバル：hello インターバルの 4 倍<br>認証なし<br>パスワードの指定なし<br>MD5 認証はディセーブル |
| エリア | 認証タイプ：0（認証なし）<br>デフォルト コスト：1<br>範囲：ディセーブル<br>スタブ：スタブ エリアは未定義<br>NSSA：NSSA エリアは未定義 |
| 自動コスト | 100 Mb/s |
| デフォルト情報送信元 | ディセーブル イネーブルの場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルトはタイプ 2 です。 |
| デフォルト メトリック | 各ルーティング プロトコルに適切な、組み込みの自動メトリック変換 |
| 距離 OSPF | dist1（エリア内のすべてのルート）：110<br>dist2（エリア間のすべてのルート）：110<br>dist3（他のルーティング ドメインからのルート）：110 |
| OSPF データベース フィルタ | ディセーブル すべての発信 LSA がインターフェイスにフラッディングされます。 |
| IP OSPF 名検索 | ディセーブル |
| 隣接関係変更ログ | イネーブル |
| ネイバー | 指定なし |
| ネイバー データベース フィルタ | ディセーブル すべての発信 LSA はネイバーにフラッディングされます。 |
| ネットワーク エリア | ディセーブル |
| NSF[1] 認識 | イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。 |
| NSF 対応 | ディセーブル<br>**（注）**　スイッチ スタックは OSPF NSF 対応ルーティングを IPv4 に対してサポートします。 |

表 39-5　OSPF のデフォルト設定（続き）

| 機能 | デフォルト設定 |
|---|---|
| ルータ ID | OSPF ルーティング プロセスは未定義 |
| サマリー アドレス | ディセーブル |
| タイマー LSA グループのペーシング | 240 秒 |
| タイマー Shortest Path First（SPF） | spf delay：5 秒<br>spf-holdtime：10 秒 |
| 仮想リンク | エリア ID またはルータ ID は未定義<br>hello インターバル：10 秒<br>再送信インターバル：5 秒<br>送信遅延：1 秒<br>デッド インターバル：40 秒<br>認証キー：キーは未定義<br>メッセージ ダイジェスト キー（MD5）：キーは未定義 |

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）。
2. OSPF NSF 認識は、IP サービス フィーチャ セットを実行しているスイッチでは IPv4 に対してイネーブルになっています。

## ルーテッド アクセスの OSPF

Cisco IOS Release 12.2(55)SE で、IP Base イメージは OSPF for Routed Access をサポートしています。ルート制限のない複数の OSPFv2 および OSPFv3 インスタンスが必要な場合は、IP サービス イメージが必要です。また、マルチ VRF CE 機能をイネーブルにするためにも、IP サービス イメージが必要です。

OSPF for Routed Access は、特にレイヤ 3 のルーティング機能をワイヤリング クローゼットに拡張するために作成されました。

（注）　OSPF for Routed Access は、動的に学習された合わせて 200 のルートを持つ OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つだけサポートします。IP ベース イメージは、ルーテッド アクセス用に OSPF を提供します。

ただし、これらの制限はこのリリースでは適用されません。

構内環境内の標準的なトポロジ（ハブおよびスポーク）では、すべての非ローカル トラフィックをディストリビューション レイヤに転送するディストリビューション スイッチ（ハブ）にワイヤリング クローゼット（スポーク）が接続されているため、ワイヤリング クローゼット スイッチで完全なルーティング スイッチ テーブルを保持する必要はありません。OSPF for Routed Access をワイヤリング クローゼットで使用する場合、エリア間ルートおよび外部ルートに到達するためのデフォルト ルートがディストリビューション スイッチによってワイヤリング クローゼット スイッチに送信される、ベスト プラクティスの設計（OSPF スタブまたは完全スタブ エリア構成）を使用する必要があります。

詳細については、EIGRP または OSPF を使用するルーテッド アクセス レイヤの「ハイ アベイラビリティ キャンパス ネットワーク設計」について Google 検索を実行します。

# OSPF NSF

スイッチまたはスイッチ スタックは、次の 2 つのレベルの NSF をサポートします。

- 「OSPF NSF 認識」（P.39-31）
- 「OSPF NSF 対応」（P.39-31）

## OSPF NSF 認識

IP サービス フィーチャ セットでは、IPv4 の OSPF NSF 認識がサポートされます。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ ルート プロセッサがバックアップ ルート プロセッサによって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ ルート プロセッサを手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「OSPF Nonstop Forwarding (NSF) Awareness」の項を参照してください。

## OSPF NSF 対応

Cisco IOS Release 12.2(58)SE 以降のスイッチでは、先行リリースでサポートされていた OSPFv2 NSF Cisco フォーマットに加えて、OSPFv2 NSF IETF フォーマットもサポートされます。この機能の詳細については、『*NSF—OSPF (RFC 3623 OSPF Graceful Restart)*』を参照してください。

IP サービス フィーチャ セットでは、コンバージェンスを改善し、スタック マスターの変更後のトラフィック損失を削減するために、IPv4 の OSPF NSF 対応ルーティングもサポートされます。スタック マスターの変更が OSPF NSF 対応スタックで発生した場合は、新しいスタック マスターは、リンクステート データベースを OSPF ネイバーと再同期するために、2 つの作業を行う必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な OSPF ネイバーを解放します。
- ネットワークのリンクステート データベースの内容を再取得する。

スタック マスターの変更後に、新しいマスターが、OSPF NSF 信号を NSF 認識ネイバー デバイスに送信します。デバイスはこの信号を、スタックとのネイバー関係をリセットしない指示として認識します。NSF 対応スタック マスターは、ネットワーク上の他のルータから信号を受け取ると、自身のネイバー リストの再構築を開始します。

NSF 対応スタック マスターはネイバー関係を再確立すると、自身のデータベースを NSF 認識ネイバーと再同期化し、OSPF ネイバー間でルーティング情報を交換します。新しいスタック マスターはこのルーティング情報を使用して、新しい情報を基に古いルートの削除、Routing Information Database（RIB; ルーティング情報ベース）の更新、Forwarding Information Base（FIB; 転送情報ベース）のアップデートを行います。これで OSPF プロトコルは完全に収束します。

（注）　OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。NSF 対応ルータは、ネットワーク セグメントで非 NSF 認識ネイバーを検出すると、そのセグメントの NSF 機能をディセーブルにします。すべてのデバイスが NSF 認識または NSF 対応デバイスとなっているその他のネットワーク セグメントでは、NSF 対応機能が継続して提供されます。

OSPF NSF ルーティングをイネーブルにするには、**nsf** OSPF ルーティング コンフィギュレーション コマンドを使用します。OSPF NSF ルーティングがイネーブルになっていることを確認するには、**show ip ospf** 特権 EXEC コマンドを使用します。

（注）　NSF は、ホットスタンバイ ルータ プロトコル（HSRP）用に設定されたインターフェイス上ではサポートされません。

# 基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに関連付ける IP アドレスの範囲を指定して、この範囲に関連付けるエリア ID を割り当てる必要があります。Cisco IOS Release 12.2(58)SE 以降、Cisco OSPFv2 NSF フォーマットと IETF OSPFv2 NSF フォーマットのいずれかを設定できます。

OSPF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router ospf** *process-id* | OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられる内部の識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。 |
| ステップ 3 | **nsf cisco** [**enforce global**] | （任意）OSPF での Cisco NSF 動作をイネーブルにします。**enforce global** キーワードを指定すると、非 NSF 認識のネイバー ネットワーキング デバイスが検出されたときに NSF 再起動がキャンセルされます。 |
| | または | |
| | **nsf ietf** [**restart-interval** *seconds*] | （任意）OSPF での IETF NSF 動作をイネーブルにします。**restart-interval** キーワードでは、グレースフル リスタート間隔の長さを秒単位で指定します。指定できる範囲は 1 ～ 1800 です。デフォルトは 120 です。 |
| ステップ 4 | **network** *address wildcard-mask* **area** *area-id* | OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。ワイルドカードマスクを使用して単一のコマンドを使用し、特定の OSPF エリアに関連付ける複数のインターフェイスを定義できます。エリア ID には 10 進数または IP アドレスを指定できます。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip protocols** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

OSPF ルーティング プロセスを終了するには、**no router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。

次に、OSPF ルーティング プロセスを設定し、プロセス ID 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

# OSPF インターフェイスの設定

**ip ospf** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ（hello インターバル、デッド インターバル、認証キーなど）については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。

OSPF インターフェイス パラメータを変更にするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip ospf** *cost* | （任意）インターフェイスでパケットを送信するコストを指定します。 |
| ステップ 4 | **ip ospf retransmit-interval** *seconds* | （任意）リンクステート アドバタイズメント送信間隔を秒数で指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。 |
| ステップ 5 | **ip ospf transmit-delay** *seconds* | （任意）リンク ステート アップデート パケットを送信するまでの予測待機時間を秒数で設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 1 秒です。 |
| ステップ 6 | **ip ospf priority** *number* | （任意）ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。 |
| ステップ 7 | **ip ospf hello-interval** *seconds* | （任意）OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 10 秒です。 |
| ステップ 8 | **ip ospf dead-interval** *seconds* | （任意）最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。 |
| ステップ 9 | **ip ospf authentication-key** *key* | （任意）隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列（最大 8 バイト長）を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。 |
| ステップ 10 | **ip ospf message digest-key** *keyid* **md5** *key* | （任意）MDS 認証をイネーブルにします。<br>• *keyid* : 1 ～ 255 の ID<br>• *key* : 最大 16 バイトの英数字パスワード |
| ステップ 11 | **ip ospf database-filter all out** | （任意）インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトでは、OSPF は、LSA が着信する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に新しい LSA をフラッディングします。 |
| ステップ 12 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 13 | **show ip ospf interface** [*interface-name*] | OSPF に関連するインターフェイス情報を表示します。 |
| ステップ 14 | **show ip ospf neighbor detail** | ネイバー スイッチの NSF 認証ステータスを表示します。出力には、次のいずれかが表示されます。<br>• *Options is 0x52*<br>*LLS Options is 0x1 (LR)*<br>これらの行の両方が表示される場合、ネイバー スイッチは NSF 認識です。<br>• *Options is 0x42*：ネイバー スイッチが NSF 認識でないことを示します。 |
| ステップ 15 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

# OSPF エリア パラメータの設定

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。*スタブ エリア*に外部ルートに関する情報は送信されません が、代わりに、Autonomous System（AS; 自律システム）外の宛先に対するスタブ エリアへのデフォルトの外部ルートが、エリア境界ルータ（ABR）によって生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の自律システム外部ルートを取り込むことができます。

ルートのサマライズは、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。

（注）　OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

エリア パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router ospf** *process-id* | OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **area** *area-id* **authentication** | （任意）特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。ID には 10 進数または IP アドレスのいずれかを指定できます。 |
| ステップ 4 | **area** *area-id* **authentication message-digest** | （任意）エリアに関して MD5 認証をイネーブルにします。 |
| ステップ 5 | **area** *area-id* **stub** [**no-summary**] | （任意）エリアをスタブ エリアとして定義します。**no-summary** キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブ エリアに送信できなくなります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**] | （任意）エリアを NSSA として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。<br>• **no-redistribution**：ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA でなく通常のエリアに取り込む場合に選択します。<br>• **default-information-originate**：タイプ 7 LSA を NSSA に取り込むことができるようにするには、ABR を選択します。<br>• **no-redistribution**：サマリー LSA を NSSA に送信しない場合に選択します。 |
| ステップ 7 | **area** *area-id* **range** *address mask* | （任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show ip ospf** [*process-id*] | 設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。 |
| | **show ip ospf** [*process-id* [*area-id*]] **database** | 特定のルータの OSPF データベースに関連する情報のリストを表示します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

# その他の OSPF パラメータの設定

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート サマライズ：他のプロトコルからのルートを再配信すると（「ルート マップによるルーティング情報の再配信」（P.39-102）を参照）、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワーク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に ASBR になります。ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用されるドメイン ネーム サーバ（DNS）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅（*bw*）は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。

- アドミニストレーティブ ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ～ 255 の整数を指定でき、値が大きいほど信頼性は低下します。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって取得した別のルーティング ドメインからのルート（外部）の 3 つの異なるアドミニストレーティブ ディスタンスが使用されます。どのアドミニストレーティブ ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。両方のデバイスは受信側インターフェイス宛ての hello パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。
- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

上記の OSPF パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router ospf** *process-id* | OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **summary-address** *address mask* | （任意）1 つのサマリー ルートだけがアドバタイズされるように、再配信されたルートのアドレスおよび IP サブネット マスクを指定します。 |
| ステップ 4 | **area** *area-id* **virtual-link** router-id [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**trans**] [[**authentication-key** *key*] \| **message-digest-key** *keyid* **md5** *key*]] | （任意）仮想リンクを確立し、パラメータを設定します。パラメータ定義については「OSPF インターフェイスの設定」（P.39-33）、仮想リンクのデフォルト設定については表 39-5（P.39-29）を参照してください。 |
| ステップ 5 | **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*] | （任意）強制的に OSPF ルーティング ドメインにデフォルト ルートを生成するように ASBR を設定します。パラメータはすべて任意です。 |
| ステップ 6 | **ip ospf name-lookup** | （任意）DNS 名検索を設定します。デフォルトはディセーブルです。 |
| ステップ 7 | **ip auto-cost reference-bandwidth** *ref-bw* | （任意）単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。 |
| ステップ 8 | **distance ospf** {[**inter-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]} | （任意）OSPF の距離の値を変更します。指定できる範囲は 1 ～ 255 です。各タイプのルートのデフォルト距離は 110 です。 |
| ステップ 9 | **passive-interface** *type number* | （任意）指定されたインターフェイス経由の hello パケットの送信を抑制します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 10 | **timers throttle spf** *spf-delay spf-holdtime spf-wait* | （任意）ルート計算タイマーを設定します。<br>• *spf-delay*：SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。<br>• *spf-holdtime*：最初と 2 番めの SPF 計算の間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。<br>• *spf-wait*：SPF 計算の最大待機時間（ミリ秒）。指定できる範囲は 1 ～ 600000 ミリ秒です。 |
| ステップ 11 | **ospf log-adj-changes** | （任意）ネイバー ステートが変更されたとき、Syslog メッセージを送信します。 |
| ステップ 12 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show ip ospf** [*process-id* [*area-id*]] **database** | 特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「OSPF のモニタリング」（P.39-39）を参照してください。 |
| ステップ 14 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# LSA グループ ペーシングの変更

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用できるようになります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ同期インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。たとえば、データベース内に約 10,000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを長くし、10 ～ 20 分に設定してください。

OSPF LSA ペーシングを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router ospf** *process-id* | OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **timers lsa-group-pacing** *seconds* | LSA のグループ ペーシングを変更します。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-config** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

# ループバック インターフェイスの設定

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信する必要があります。ループバック インターフェイスが IP アドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

ループバック インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface loopback 0** | ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip address** *address mask* | このインターフェイスに IP アドレスを割り当てます。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip interface** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

# OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

表 39-6 に、統計情報を表示するために使用する特権 EXEC コマンドの一部を示します。**show ip ospf database** 特権 EXEC コマンドのオプションおよび表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

**表 39-6　IP OSPF 統計情報の表示コマンド**

| コマンド | 目的 |
|---|---|
| **show ip ospf** [*process-id*] | OSPF ルーティング プロセスに関する一般的な情報を表示します。 |
| **show ip ospf** [*process-id*] **database** [**router**] [*link-state-id*]<br>**show ip ospf** [*process-id*] **database** [**router**] [**self-originate**]<br>**show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]]<br>**show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*]<br>**show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*]<br>**show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*]<br>**show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*]<br>**show ip ospf** [*process-id area-id*] **database** [**database-summary**] | OSPF データベースに関連する情報を表示します。 |
| **show ip ospf border-routes** | 内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。 |
| **show ip ospf interface** [*interface-name*] | OSPF に関連するインターフェイス情報を表示します。 |
| **show ip ospf neighbor** [*interface-name*] [*neighbor-id*] **detail** | OSPF インターフェイス ネイバー情報を表示します。 |
| **show ip ospf virtual-links** | OSPF に関連する仮想リンク情報を表示します。 |

# EIGRP の設定

**（注）** スイッチで IP ベース イメージが稼働している場合は、*complete* EIGRP ルーティングを設定できます。ただし、IP ベース イメージでは EIGRP *スタブ ルーティング*だけがサポートされるため、設定は実装されません。

**eigrp stub** ルータ コンフィギュレーション コマンドの入力後に、**eigrp stub connected summary** コマンドだけが有効になります。CLI ヘルプには、**receive-only** キーワードと **static** キーワードが表示されることがあり、これらのキーワードを入力できますが、IP ベース イメージが稼働しているスイッチの動作は常に、**connected** キーワードと **summary** キーワードが設定されている場合と同じです。

Enhanced IGRP（EIGRP）は IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンス技術には、拡散更新アルゴリズム（DUAL）と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階で操作にループが発生しなくなります。トポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算に含まれません。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート層のホップ カウンタだけです。IP パケットが 15 台のルータを経由し、宛先方向のネクストホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステートが変更された場合、ルーティング テーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：完全更新パケットを受信ごとに処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しないネイバー探索メカニズム：このメカニズムを使用し隣接ルータに関する情報を取得します。
- Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）
- 任意のルート集約
- 大規模ネットワークの場合のスケーラビリティ

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- *ネイバー探索および回復*：直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。ルータは、ネイバーが到達不能または動作不能になったことも検出する必要があります。ネイバー探索および回復：サイズの小さい hello パケットを定期的に送信することにより実現します。hello パケットが受信されている限り、Cisco IOS ソフトウェアは、ネイバーが有効に機能していると判別します。このように判別された場合、隣接ルータはルーティング情報を交換できます。
- *信頼できるトランスポート プロトコル*：EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率を高めるため、信頼性は必要な場合にだけ確保されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーに個別に hello パケットを確実に送信する必要はありません。したがって、EIGRP はパケットへの確認応答が不要であることを知らせる、レシーバ宛の情報をパケットに格納し、単一のマルチキャスト hello を送信します。他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）を要求します。信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチキャスト パケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。
- *DUAL 有限状態マシン*：すべてのルート計算に関する決定プロセスを統合し、すべてのネイバーによってアドバタイズされたすべてのルートをトラッキングします。DUAL は距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、この結果、新しい後継ルータが決定されます。ルートの再計算に要する時間によって、コンバージェンス時間が変わります。再計算はプロセッサに負

荷がかかるため、必要でない場合は、再計算しないようにしてください。トポロジが変更されると、DUAL は適切な後継ルータの有無を調べます。適切な後継ルータが存在する場合は、それらを探して使用し、不要な再計算を回避します。

- *プロトコル依存モジュール*：ネットワーク層プロトコル特有の作業を行います。たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。また、EIGRP パケットを解析したり、DUAL に受信した新しい情報を通知したりします。EIGRP はルーティング決定に DUAL を使用しますが、結果は IP ルーティング テーブルに格納されます。EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

ここでは、次の設定について説明します。

- 「EIGRP のデフォルト設定」（P.39-41）
- 「基本的な EIGRP パラメータの設定」（P.39-44）
- 「EIGRP インターフェイスの設定」（P.39-45）
- 「EIGRP ルート認証の設定」（P.39-45）
- 「EIGRP スタブ ルーティング」（P.39-47）
- 「EIGRP のモニタリングおよびメンテナンス」（P.39-48）

（注）　EIGRP をイネーブルにするには、スイッチまたはスタック マスターは IP サービス フィーチャ セットを実行している必要があります。

# EIGRP のデフォルト設定

表 39-7 に、EIGRP のデフォルト設定を示します。

**表 39-7　EIGRP のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| 自動サマリー | ディセーブル クラスフル ネットワーク境界を通過するとき、この境界にサブプレフィックスはサマライズされません。 |
| デフォルト情報 | 再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。 |
| デフォルト メトリック | デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。<br>• 帯域幅：0 以上の kb/s<br>• 遅延（10 マイクロ秒）：0 または 39.1 ナノ秒の倍数である任意の正の数値<br>• 信頼性：0 ～ 255 の任意の数値（255 の場合は信頼性が 100%）<br>• 負荷：0 ～ 255 の数値で表される有効帯域幅（255 の場合は 100% の負荷）<br>• MTU：バイトで表されたルートの MTU サイズ （0 または任意の正の整数） |
| ディスタンス | 内部距離：90<br>外部距離：170 |

表 39-7　EIGRP のデフォルト設定 （続き）

| 機能 | デフォルト設定 |
|---|---|
| EIGRP の隣接関係変更ログ | ディセーブル 隣接関係の変更はロギングされません。 |
| IP 認証キーチェーン | 認証なし |
| IP 認証モード | 認証なし |
| IP 帯域幅比率 | 50% |
| IP hello 間隔 | 低速 Nonbroadcast Multiaccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒 |
| IP ホールドタイム | 低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒 |
| IP スプリットホライズン | イネーブル |
| IP サマリー アドレス | サマリー集約アドレスは未定義 |
| メトリック重み | tos：0、k1 および k3：1、k2、k4、および k5：0 |
| ネットワーク | 指定なし |
| NSF[1] 認識 | イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。 |
| NSF 対応 | ディセーブル<br>**（注）** スイッチは EIGRP NSF 対応ルーティングを IPv4 に対してサポートします。 |
| オフセットリスト | ディセーブル |
| ルータ EIGRP | ディセーブル |
| メトリック設定 | ルート マップにはメトリック設定なし |
| トラフィック共有 | メトリックの比率に応じて配分 |
| 差異 | 1（等コスト ロード バランシング） |

1. NSF = Nonstop Forwarding
2. EIGRP NSF 認識は、IP サービス フィーチャ セットを実行するスイッチ上で IPv4 対してイネーブルになっています。

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。

ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の*両方*が設定された移行ルータを指定する必要があります。この場合は、この次の項に記載されているステップ 1 ～ 3 を実行してください（「スプリット ホライズンの設定」（P.39-27）も参照）。ルートを自動的に再配信するには、ルートに同じ自律システム番号を使用する必要があります。

## EIGRP NSF

スイッチ スタックは、次の 2 つのレベルの EIGRP NFS をサポートします。

- 「EIGRP NSF 認識」（P.39-43）
- 「EIGRP NSF 対応」（P.39-43）

## EIGRP NSF 認識

IP サービス フィーチャ セットでは、IPv4 の EIGRP NSF 認識がサポートされます。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ ルート プロセッサがバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ ルート プロセッサを手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「EIGRP Nonstop Forwarding (NSF) Awareness」の項を参照してください。

## EIGRP NSF 対応

Cisco IOS Release 12.2(58)SE 以降、スイッチはスタック マスター変更後にコンバージェンスを高速化し、トラフィックの損失を防ぐために EIGRP Cisco NSF ルーティングをサポートします。この NSF 機能の詳細については、次のサイトにある『*High Availability Configuration Guide, Cisco IOS XE Release 3S*』の「Configuring Nonstop Forwarding」の章を参照してください。
http://www.cisco.com/en/US/docs/ios/ios_xe/ha/configuration/guide/ha-nonstp_fwdg_xe.html#wp1085061

IP サービス フィーチャ セットでは、コンバージェンスを改善し、スタック マスターの変更後のトラフィック損失を削減するために、IPv4 の EIGRP NSF 対応ルーティングもサポートされます。EIGRP NSF 対応スタック マスターを再起動したとき、または新しいスタック マスターを起動して NSF を再起動したときには、スイッチにネイバーはなく、トポロジ テーブルは空です。スイッチは、スイッチ スタックに送信されるトラフィックを中断することなく、インターフェイスの起動、ネイバーの再取得、およびトポロジ テーブルとルーティング テーブルの再作成を行う必要があります。EIGRP ピア ルータは、新しいスタック マスターから取得したルートを維持し、NSF 再起動プロセスによってトラフィックの転送を続行します。

ネイバーによる隣接関係のリセットを防止するには、新しいスタック マスターは、EIGRP パケット ヘッダーで新規の再起動ビットを使用します。ネイバーは、これを受信すると、ピア リストにあるスタックを同期化し、スタックとの隣接関係を維持します。次にネイバーは、NSF を認識しており、新規のスタック マスターを支援することを示すために再起動ビットを設定し、トポロジ テーブルをスタック マスターに送信します。

スタックのピア ネイバーの少なくとも 1 つが NFS 認識デバイスであれば、スタック マスターはアップデート情報を受信してデータベースを再構築します。それぞれの NSF 認識ネイバーは、最後のアップデート パケットで End-of-Table（EOT）マーカーを送信して、テーブルの内容の最後をマーキングします。スタック マスターは、EOT マーカーを受信して、アップデートの送信を開始すると、コンバージェンスを認識します。スタック マスターがネイバーからすべての EOT マーカーを受信した場合、または NSF コンバージ タイマーが期限切れになった場合、EIGRP は RIB にコンバージェンスを通知し、すべての NSF 認識ピアにトポロジ テーブルをフラッディングします。

**（注）** NSF は、ホットスタンバイ ルータ プロトコル（HSRP）用に設定されたインターフェイス上ではサポートされません。

EIGRP NSF ルーティングをイネーブルにするには、**nsf** EIGRP ルーティング コンフィギュレーション コマンドを使用します。NSF がイネーブルになっていることを確認するには、**show ip protocols** 特権 EXEC コマンドを使用します。**nsf** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

# 基本的な EIGRP パラメータの設定

EIGRP を設定するには、特権 EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外のステップはオプションです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router eigrp** *autonomous-system* | EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。自律システム番号によって、他の EIGRP ルータへのルートを特定し、ルーティング情報をタグ付けします。 |
| ステップ 3 | **nsf** | （任意）EIGRP NSF をイネーブルにします。スタック マスターおよびそのすべてのピア上でこのコマンドを入力します。 |
| ステップ 4 | **network** *network-number* | ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。 |
| ステップ 5 | **eigrp log-neighbor-changes** | （任意）EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニタします。 |
| ステップ 6 | **metric weights** *tos k1 k2 k3 k4 k5* | （任意）EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。<br>⚠ **注意** メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。 |
| ステップ 7 | **offset list** [*access-list number* \| *name*] {**in** \| **out**} *offset* [*type number*] | （任意）オフセット リストをルーティング メトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増やします。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。 |
| ステップ 8 | **auto-summary** | （任意）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。 |
| ステップ 9 | **ip summary-address eigrp** *autonomous-system-number address mask* | （任意）サマリー集約を設定します。 |
| ステップ 10 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 11 | **show ip protocols** | 入力内容を確認します。 |
| ステップ 12 | **show ip protocols** | 設定を確認します。<br>NSF 認識の場合、出力に次のように表示されます。<br>`*** IP Routing is NSF aware ***`<br>`EIGRP NSF enabled` |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

EIGRP インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip bandwidth-percent eigrp** *percent* | （任意）インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。 |
| ステップ 4 | **ip summary-address eigrp** *autonomous-system-number address mask* | （任意）指定されたインターフェイスのサマリー集約アドレスを設定します（auto-summary がイネーブルの場合は、通常設定する必要はありません）。 |
| ステップ 5 | **ip hello-interval eigrp** *autonomous-system-number seconds* | （任意）EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。 |
| ステップ 6 | **ip hold-time eigrp** *autonomous-system-number seconds* | （任意）EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。指定できる範囲は 1 ～ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。<br>⚠ **注意** ホールド タイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。 |
| ステップ 7 | **no ip split-horizon eigrp** *autonomous-system-number* | （任意）スプリット ホライズンをディセーブルにし、ルータが、情報元インターフェイスからルート情報をアドバタイズできるようにします。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show ip eigrp interface** | EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

# EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **ip authentication mode eigrp** *autonomous-system* **md5** | IP EIGRP パケットの MD5 認証をイネーブルにします。 |
| ステップ 4 | **ip authentication key-chain eigrp** *autonomous-system key-chain* | IP EIGRP パケットの認証をイネーブルにします。 |
| ステップ 5 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **key chain** *name-of-chain* | キー チェーンを識別し、キーチェーン 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 で設定した名前を指定します。 |
| ステップ 7 | **key** *number* | キーチェーン コンフィギュレーション モードで、キー番号を識別します。 |
| ステップ 8 | **key-string** *text* | キーチェーン コンフィギュレーション モードで、キーストリングを識別します。 |
| ステップ 9 | **accept-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*} | （任意）キーを受信する期間を指定します。<br>*start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、*無制限*です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。 |
| ステップ 10 | **send-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*} | （任意）キーを送信する期間を指定します。<br>*start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、*無制限*です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show key chain** | 認証キー情報を表示します。 |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

# EIGRP スタブ ルーティング

（注）　IP ベース フィーチャ セットに含まれる EIGRP スタブ ルーティング機能では、ルーティング テーブルからの接続ルートまたはサマリー ルートをネットワーク内のほかのルータにアドバタイズすることだけを行います。スイッチは アクセス レイヤで EIGRP スタブ ルーティングを使用することにより、ほかのタイプのルーティング アドバタイズメントの必要性を排除しています。拡張機能および完全な EIGRP ルーティングを使用するには、スイッチで IP サービス フィーチャ セットを稼働させる必要があります。
IP ベース フィーチャ セットが稼働するスイッチ上で、Multi-VRF-CE と EIGRP スタブ ルーティングを同時に設定しようとすると、設定は許可されません。

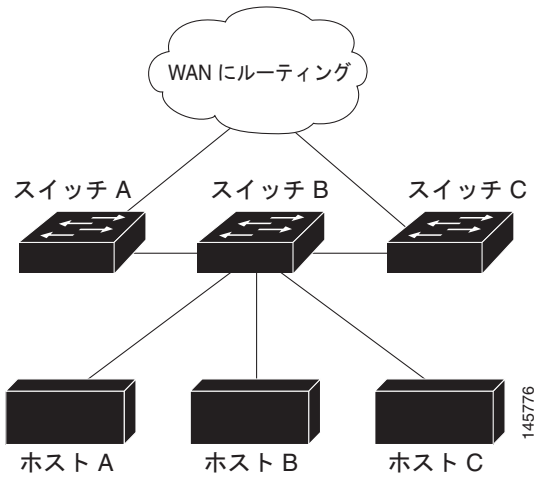
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートだけが EIGRP スタブ ルーティングを設定しているスイッチを通過します。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用しているときは、EIGRP を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、配布ルータに依存して適切なアップデートをすべてのピアに送信します。

図 39-4 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

**図 39-4　　EIGRP スタブ ルータ設定**




EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2*』の「Configuring EIGRP Stub Routing」の項を参照してください。

# EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。さらに、各種 EIGRP ルーティング統計情報を表示することもできます。表 39-8 に、ネイバー削除および統計情報表示用の特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

**表 39-8　IP EIGRP の clear および show コマンド**

| コマンド | 目的 |
|---|---|
| **clear ip eigrp neighbors** [*if-address* \| *interface*] | ネイバー テーブルからネイバーを削除します。 |
| **show ip eigrp interface** [*interface*] [*as number*] | EIGRP に設定されているインターフェイスに関する情報を表示します。 |
| **show ip eigrp neighbors** [*type-number*] | EIGRP によって検出されたネイバーを表示します。 |
| **show ip eigrp topology** [*autonomous-system-number*] \| [[*ip-address*] *mask*]] | 指定されたプロセスの EIGRP トポロジ テーブルを表示します。 |
| **show ip eigrp traffic** [*autonomous-system-number*] | すべてまたは特定の EIGRP プロセスの送受信パケット数を表示します。 |

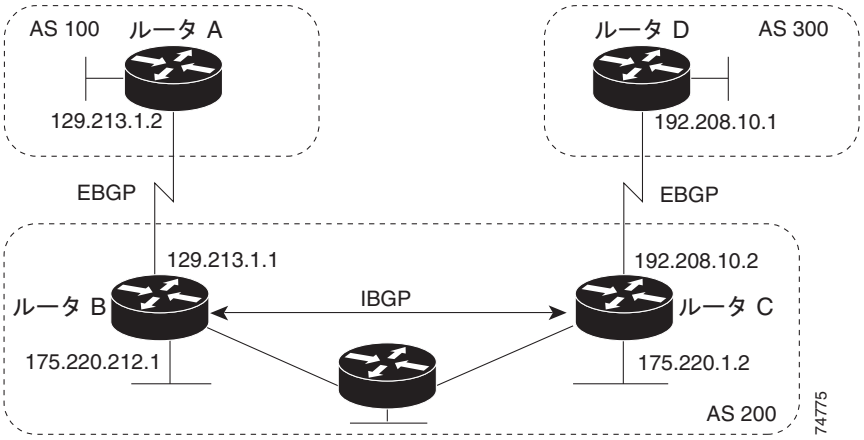
# BGP の設定

ボーダー ゲートウェイ プロトコル（BGP）は、自律システム間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムのための Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）です。自律システムは、同じ管理下で動作している複数のルータで構成され、RIP や OSPF などの内部ゲートウェイ プロトコル（IGP）を境界内で実行し、外部ゲートウェイ プロトコル（EGP）を使用して相互接続しています。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」の章を参照してください。

BGP コマンドとキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocols」を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B「Cisco IOS Release 15.0(2)SE でサポートされていないコマンド」を参照してください。

同じ自律システムに属し、BGP アップデートを交換するルータは、*Internal BGP*（IBGP）を実行します。異なる自律システムに属し、BGP アップデートを交換するルータは、*External BGP*（EBGP）を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、ルーティング アップデートが自律システム間で交換される（EBGP）か、自律システム内で交換される（IBGP）かという点で異なります。図 39-5 に、EBGP と IBGP の両方が稼働するネットワークを示します。

図 39-5　EBGP、IBGP、および複数の AS




外部自律システムと情報を交換する前に、BGP は、ルータ間で Internal BGP ピアリングを定義し、IGRP や OSPF などの自律システム内で稼働する IGP に BGP ルーティング情報を再配信して、自律システム内のネットワークに到達できることを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP *スピーカー*と呼ばれます。BGP はトランスポート プロトコルとして TCP を使用します（特にポート 179）。相互に TCP 接続された 2 つの BGP スピーカーを、*ピア*または*ネイバー*と呼びます。図 39-5 では、ルータ A と B、ルータ B と C、およびルータ C と D がそれぞれ BGP ピアです。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の自律システム番号です。BGP はこの情報を使用し、ループのない AS マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP によって 2 つのネイバーが相互に到達できる限り、IBGP ピアを直接接続する必要はありません。
- 自律システム内のすべての BGP スピーカーは、ピア関係を確立する必要があります。つまり、自律システム内の BGP スピーカーは、論理的な完全メッシュを保持している必要があります。ただし、BGP4 は、論理的な完全メッシュに関する要求を軽減する技術（*連合*および*ルート リフレクタ*）を提供します。
- 自律システム AS 200 は AS 100 および AS 300 の*中継自律システム*です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送します。

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

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

Cisco IOS が稼働しているルータまたはスイッチが IBGP ルートを選択または使用するのは、ネクストホップ ルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP は*属性*値に基づいてパスを選択します。BGP 属性の詳細については、「BGP 判断属性の設定」（P.39-57）を参照してください。

BGP バージョン 4 では Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）がサポートされているため、集約ルートを作成して*スーパーネット*を構築し、ルーティング テーブルのサイズを削減できます。CIDR は、BGP 内部のネットワーク クラスをなくし、IP プレフィックスのアドバタイズメントをサポートします。

ここでは、次の設定について説明します。

- 「BGP のデフォルト設定」（P.39-50）
- 「BGP ルーティングのイネーブル化」（P.39-53）
- 「ルーティング ポリシー変更の管理」（P.39-56）
- 「BGP 判断属性の設定」（P.39-57）
- 「ルート マップによる BGP フィルタリングの設定」（P.39-59）
- 「ネイバーによる BGP フィルタリングの設定」（P.39-60）
- 「BGP フィルタリング用のプレフィックス リストの設定」（P.39-61）
- 「BGP コミュニティ フィルタリングの設定」（P.39-63）
- 「BGP ネイバーおよびピア グループの設定」（P.39-65）
- 「集約アドレスの設定」（P.39-67）
- 「ルーティング ドメイン連合の設定」（P.39-67）
- 「BGP ルート リフレクタの設定」（P.39-68）
- 「ルート ダンプニングの設定」（P.39-69）
- 「BGP のモニタリングおよびメンテナンス」（P.39-70）

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Routing Protocols」で「Configuring BGP」の章を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B「Cisco IOS Release 15.0(2)SE でサポートされていないコマンド」を参照してください。

# BGP のデフォルト設定

表 39-9 に、BGP のデフォルト設定を示します。すべての特性のデフォルトについては、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の特定のコマンドを参照してください。

**表 39-9　BGP のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| 集約アドレス | ディセーブル：未定義 |
| 自律システム パス アクセス リスト | 未定義 |
| 自動サマリー | イネーブル |
| 最適パス | • ルータはルートを選択する場合に *AS パス*を考慮し、外部 BGP ピアからの類似ルートは比較されない<br>• ルータ ID の比較：ディセーブル |

表 39-9　BGP のデフォルト設定 （続き）

| 機能 | デフォルト設定 |
|---|---|
| BGP コミュニティ リスト | • 番号：未定義。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。<br>• フォーマット：Cisco IOS デフォルト フォーマット（32 ビット番号）。 |
| BGP 連合 ID/ ピア | • ID：未設定<br>• ピア：識別なし |
| BGP 高速外部フォールオーバー | イネーブル |
| BGP ローカル初期設定 | 100。指定できる範囲は 0 ～ 4294967295 です（大きな値を推奨）。 |
| BGP ネットワーク | 指定なし。バックドア ルートのアドバタイズなし |
| BGP ルート ダンプニング | デフォルトでは、ディセーブルです。イネーブルの場合は、次のようになります。<br>• 半減期は 15 分<br>• 再使用は 750（10 秒増分）<br>• 抑制は 2000（10 秒増分）<br>• 最大抑制時間は半減期の 4 倍（60 分） |
| BGP ルータ ID | ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス |
| デフォルトの情報送信元（プロトコルまたはネットワーク再配信） | ディセーブル |
| デフォルト メトリック | 自動メトリック変換（組み込み） |
| ディスタンス | • 外部ルート アドミニストレーティブ ディスタンス：20（有効値は 1 ～ 255）<br>• 内部ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255）<br>• ローカル ルート アドミニストレーティブ ディスタンス：200（有効値は 1 ～ 255） |
| ディストリビュート リスト | • 入力（アップデート中に受信されたネットワークをフィルタリング）：ディセーブル<br>• 出力（アップデート中のネットワークのアドバタイズを抑制）：ディセーブル |
| 内部ルート再配信 | ディセーブル |
| IP プレフィックス リスト | 未定義 |
| Multi-Exit Discriminator（MED） | • 常に比較：ディセーブル。異なる AS 内のネイバーからのパスに対して、MED を比較しません。<br>• 最適パスの比較：ディセーブル。<br>• 最悪パスである MED の除外：ディセーブル<br>• 決定的な MED 比較：ディセーブル |

表 39-9　BGP のデフォルト設定 （続き）

| 機能 | デフォルト設定 |
|---|---|
| ネイバー | • アドバタイズメント インターバル：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒<br>• ロギング変更：イネーブル<br>• 条件付きアドバタイズ：ディセーブル<br>• デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし<br>• 説明：なし<br>• ディストリビュート リスト：未定義<br>• 外部 BGP マルチホップ：直接接続されたネイバーだけを許可<br>• フィルタ リスト：使用しない<br>• 受信したプレフィックスの最大数：制限なし<br>• ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル<br>• パスワード：ディセーブル<br>• ピア グループ：定義なし、割り当てメンバなし<br>• プレフィックス リスト：指定なし<br>• リモート自律システム（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし<br>• プライベート自律システム番号の削除：ディセーブル<br>• ルート マップ：ピアへの適用なし<br>• コミュニティ属性送信：ネイバーへの送信なし<br>• シャットダウンまたはソフト再設定：ディセーブル<br>• タイマー：60 秒、ホールドタイム：180 秒<br>• アップデート送信元：最適ローカル アドレス<br>• バージョン：BGP バージョン 4<br>• 重み：BGP ピアによって学習されたルート：0、ローカル ルータから取得されたルート：32768 |
| NSF[1] 認識 | ディセーブル[2] レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。 |
| ルート リフレクタ | 未設定 |
| 同期化（BGP および IGP） | イネーブル |
| テーブル マップ アップデート | ディセーブル |
| タイマー | キープアライブ：60 秒、ホールドタイム：180 秒 |

1. NSF = Nonstop Forwarding（ノンストップ フォワーディング）。
2. NSF 認識は、グレースフル リスタートをイネーブルにすることにより、IP サービス フィーチャ セットがあるスイッチでは IPv4 に対してイネーブルにできます。

## NSF 認識

BGP NSF 認識機能は、IP サービス フィーチャ セットでは IPv4 に対してサポートされています。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。隣接ルータが NSF 対応であり、この機能がイネーブルになっている場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ ルート プロセッサがバックアップ ルート プロセッサによって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ ルート プロセッサを手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能の詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*』の「BGP Nonstop Forwarding (NSF) Awareness」の項を参照してください。

# BGP ルーティングのイネーブル化

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

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

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

自律システムが別の自律システムからさらに別の自律システムにトラフィックを渡す場合は、アドバタイズメント対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを取得した場合、自律システムは一部のルータがルーティングできなかったトラフィックを受信することがあります。そのため、IGP が自律システム間に情報を伝播し、BGP が IGP と*同期化*されるまで、BGP は待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。自律システムが特定の自律システムから別の自律システムにトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼働している場合は、同期化をディセーブルにし、ネットワークによって IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束できるようにします。

**（注）** BGP をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

BGP ルーティングをイネーブルにして BGP ルーティング プロセスを確立し、ネイバーを指定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip routing** | IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合にだけ必須）。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **router bgp** *autonomous-system* | BGP ルーティング プロセスをイネーブルにして自律システム番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる自律システム番号は 1 ～ 65535 です。64512 ～ 65535 は、プライベート自律システム番号として指定されています。 |
| ステップ 4 | **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*] | この自律システムに対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。 |
| ステップ 5 | **neighbor** {*ip-address* \| *peer-group-name*} **remote-as** *number* | BGP ネイバー テーブルにエントリを追加し、IP アドレスによって識別されるネイバーが、指定された自律システムに属することを指定します。<br>通常 EBGP ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。<br>IBGP の場合、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。 |
| ステップ 6 | **neighbor** {*ip-address* \| *peer-group-name*} **remove-private-as** | （任意）発信ルーティング アップデート内の自律システム パスからプライベート自律システム番号を削除します。 |
| ステップ 7 | **no synchronization** | （任意）BGP と IGP の同期化をディセーブルにします。 |
| ステップ 8 | **no auto-summary** | （任意）自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに追加されます。 |
| ステップ 9 | **bgp fast-external-fallover** | （任意）外部ネイバー間のリンクが切断された場合、BGP セッションを自動的にリセットします。デフォルトで、セッションは即座にリセットされません。 |
| ステップ 10 | **bgp graceful-restart** | （任意）NSF 認識をスイッチでイネーブルにします。NSF 認識はデフォルトではディセーブルです。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show ip bgp network** *network-number*<br>または<br>**show ip bgp neighbor** | 設定を確認します。<br>ネイバーで NSF 認識（グレースフル リスタート）がイネーブルになっていることを確認します。<br>スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。<br>`Graceful Restart Capability: advertised and received`<br>スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。<br>`Graceful Restart Capability: advertised` |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

BGP 自律システムを削除するには、**no router bgp** *autonomous-system* グローバル コンフィギュレーション コマンドを使用します。BGP テーブルからネットワークを削除するには、**no network** *network-number* ルータ コンフィギュレーション コマンドを使用します。ネイバーを削除するには、**no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number* ルータ コンフィギュレーション コマンドを使用します。ネイバーにアップデート内のプライベート自律システム番号を含めるには、**no neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** ルータ コンフィギュレーション コマンドを使用します。同期化を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 39-5 に示されたルータ上で BGP を設定する例を示します。

ルータ A：

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C：

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D：

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼働していることを確認するには、**show ip bgp neighbors** 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors
BGP neighbor is 129.213.1.1, remote AS 200, external link
 BGP version 4, remote router ID 175.220.212.1
 BGP state = established, table version = 3, up for 0:10:59
 Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
 Minimum time between advertisement runs is 30 seconds
 Received 2828 messages, 0 notifications, 0 in queue
 Sent 2826 messages, 0 notifications, 0 in queue
 Connections established 11; dropped 10
```

*BGP state = established* 以外の情報が出力された場合、ピアは稼働していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。継続的にテーブル バージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B「Cisco IOS Release 15.0(2)SE でサポートされていないコマンド」を参照してください。

# ルーティング ポリシー変更の管理

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

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

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

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

表 39-10 に、ハード リセットとソフト リセットの利点および欠点を示します。

**表 39-10　ハード リセットとソフト リセットの利点および欠点**

| リセット タイプ | 利点 | 欠点 |
|---|---|---|
| ハード リセット | メモリ オーバーヘッドが発生しません。 | ネイバーから提供された BGP、IP、および FIB テーブルのプレフィックスが失われます。推奨しません。 |
| 発信ソフト リセット | ルーティング テーブル アップデートが設定、保管されません。 | インバウンド ルーティング テーブル アップデートがリセットされません。 |
| ダイナミック インバウンド ソフト リセット | BGP セッションおよびキャッシュがクリアされません。<br>ルーティング テーブル アップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。 | 両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります（Cisco IOS Release 12.1 以降）。 |

BGP ピアがルート リフレッシュ機能をサポートするかどうかを判別して、BGP セッションをリセットするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **show ip bgp neighbors** | ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。<br>*Received route refresh capability from peer* |
| ステップ 2 | **clear ip bgp** {***** \| *address* \| *peer-group-name*} | 指定された接続上でルーティング テーブルをリセットします。<br>• すべての接続をリセットするには、アスタリスク（*）を入力します。<br>• 特定の接続をリセットするには、IP *アドレス*を入力します。<br>• ピア グループをリセットする場合は、ピア グループ名を入力します。 |
| ステップ 3 | **clear ip bgp** {***** \| *address* \| *peer-group-name*} **soft out** | （任意）指定された接続上でインバウンド ルーティング テーブルをリセットするには、アウトバウンド ソフト リセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。<br>• すべての接続をリセットするには、アスタリスク（*）を入力します。<br>• 特定の接続をリセットするには、IP *アドレス*を入力します。<br>• ピア グループをリセットする場合は、ピア グループ名を入力します。 |
| ステップ 4 | **show ip bgp**<br>**show ip bgp neighbors** | ルーティング テーブル情報と BGP ネイバー情報を調べて、リセットされたことを確認します。 |

# BGP 判断属性の設定

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

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

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

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。BGP のネクスト ホップの属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクスト ホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 最大ウェイトのパスを推奨します（シスコ独自のパラメータ）。ウェイト属性はルータにローカルであるため、ルーティング アップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。最大の重みのルートを推奨します。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。

3. ローカル プリファレンス値が最大のルートを推奨します。ローカル初期設定はルーティング アップデートに含まれ、同じ自律システム内のルータ間で交換されます。ローカル初期設定属性のデフォルト値は 100 です。ローカル プリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼働する BGP から送信されたルートを推奨します。
5. 自律システム パスが最短のルートを推奨します。
6. 送信元タイプが最小のルートを推奨します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートでネイバー自律システムが同じである場合は、Multi Exit Discriminator（MED）メトリック属性が最小のルートを推奨します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部（IBGP）パスより、外部（EBGP）パスを推奨します。
9. 最も近い IGP ネイバー（最小の IGP メトリック）を通って到達できるルートを推奨します。ルータは、自律システム内の最短の内部パス（BGP のネクスト ホップへの最短パス）を使用し、宛先に到達するためです。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。
    - 最適ルートと目的のルートがともに外部ルートである
    - 最適ルートと目的のルートの両方が、同じネイバー AS からのルートである
    - maximum-paths がイネーブルである
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック（仮想）アドレスですが、実装に依存することがあります。

同じ判断属性を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルーティング プロセスをイネーブルにして自律システム番号を割り当て、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **bgp best-path as-path ignore** | （任意）ルートの選択中に自律システム パス長を無視するようにルータを設定します。 |
| ステップ 4 | **neighbor** {*ip-address* \| *peer-group-name*} **next-hop-self** | （任意）ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。 |
| ステップ 5 | **neighbor** {*ip-address* \| *peer-group-name*} **weight** *weight* | （任意）ネイバー接続に重みを割り当てます。値は 0 ～ 65535 です。最大ウェイトのルートを推奨します。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **default-metric** *number* | （任意）推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルートも、この値に設定されます。指定できる範囲は 1 ～ 4294967295 です。最小値を推奨します。 |
| ステップ 7 | **bgp bestpath med missing-as-worst** | （任意）MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。 |
| ステップ 8 | **bgp always-compare med** | （任意）異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ自律システム内のパス間だけで比較されます。 |
| ステップ 9 | **bgp bestpath med confed** | （任意）連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。 |
| ステップ 10 | **bgp deterministic med** | （任意）同じ自律システム内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。 |
| ステップ 11 | **bgp default local-preference** *value* | （任意）デフォルトのローカル初期設定値を変更します。指定できる範囲は 0 ～ 4294967295 で、デフォルト値は 100 です。最大のローカル初期設置値を推奨します。 |
| ステップ 12 | **maximum-paths** *number* | （任意）IP ルーティング テーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティング テーブルに追加されます。指定できる範囲は 1 ～ 16 です。複数の値を指定すると、パス間のロード バランシングが可能になります。（スイッチ ソフトウェアでは、最大である 32 個の等コスト ルートを使用できますが、1 つのルートにつき 16 個を超えるパスがスイッチ ハードウェアで使用されることはありません）。 |
| ステップ 13 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 14 | **show ip bgp**<br>**show ip bgp neighbors** | ルーティング テーブル情報と BGP ネイバー情報を調べて、リセットされたことを確認します。 |
| ステップ 15 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト ステートに戻すには、このコマンドの **no** 形式を使用します。

# ルート マップによる BGP フィルタリングの設定

ルート マップは、BGP 内で、ルーティング情報を制御および変更したり、ルーティング ドメイン間でルートを再配信する条件を定義したりできます。ルート マップの詳細については、「ルート マップによるルーティング情報の再配信」（P.39-102）を参照してください。各ルート マップには、ルート マップを識別する名前（マップ タグ）およびオプションのシーケンス番号が付いています。

ルート マップを使用してネクストホップ処理をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **route-map** *map-tag* [[**permit** \| **deny**] \| *sequence-number*]] | ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **set ip next-hop** *ip-address* [*...ip-address*] [**peer-address**] | （任意）ネクストホップ処理をディセーブルにするようにルート マップを設定します。<br>• 着信ルート マップの場合は、一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクストホップを上書きします。<br>• BGP ピアのアウトバウンド ルート マップの場合は、ネクストホップをローカル ルータのピア アドレスに設定して、ネクストホップ計算をディセーブルにします。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show route-map** [*map-name*] | 設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ルート マップを削除するには、**no route-map** *map-tag* コマンドを使用します。ネクストホップ処理を再びイネーブルにするには、**no set ip next-hop** *ip-address* コマンドを使用します。

# ネイバーによる BGP フィルタリングの設定

BGP アドバタイズメントをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの自律システム パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」（P.39-111）を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。ルート マップは、着信アップデートまたは発信アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。着信および発信の両方のアップデートで、自律システム パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。自律システム パスのマッチングには **match as-path access-list** ルート マップ コマンド、コミュニティに基づくマッチングには **match community-list** ルート マップ コマンド、ネットワークに基づくマッチングには **ip access-list** グローバル コンフィギュレーション コマンドが必要です。

ネイバー単位のルート マップを適用するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルーティング プロセスをイネーブルにして自律システム番号を割り当て、ルータ コンフィギュレーション モードを開始します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **neighbor** {*ip-address* \| *peer-group name*} **distribute-list** {*access-list-number* \| *name*} {**in** \| **out**} | （任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。<br>**（注）** **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定するということはできません。 |
| ステップ 4 | **neighbor** {*ip-address* \| *peer-group name*} **route-map** *map-tag* {**in** \| **out**} | （任意）ルート マップを適用し、着信または発信ルートをフィルタリングします。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip bgp neighbors** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ネイバーからアクセス リストを削除するには、**no neighbor distribute-list** コマンドを使用します。ネイバーからルート マップを削除するには、**no neighbor route-map** *map-tag* ルータ コンフィギュレーション コマンドを使用します。

BGP 自律システム パスに基づいて着信および発信の両方のアップデートでアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現を使用するアクセス リストです。（正規表現の作成方法については、『*Cisco IOS Dial Technologies Command Reference, Release 12.2*』の付録「Regular Expressions」を参照してください）。この方法を使用するには、自律システム パスのアクセス リストを定義し、特定のネイバーに対して送受信されるアップデートに適用します。

BGP 自律システム パス フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip as-path access-list** *access-list-number* {**permit** \| **deny**} *as-regular-expressions* | BGP 関連アクセス リストを定義します。 |
| ステップ 3 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **neighbor** {*ip-address* \| *peer-group name*} **filter-list** {*access-list-number* \| *name*} {**in** \| **out** \| **weight** *weight*} | アクセス リストに基づいて、BGP フィルタを確立します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip bgp neighbors** [**paths** *regular-expression*] | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# BGP フィルタリング用のプレフィックス リストの設定

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

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

- 空のプレフィックス リストはすべてのプレフィックスを許可します。
- プレフィックスがプレフィックス リスト内のどのエントリとも一致しない場合は、暗黙の拒否が使用されます。
- プレフィックスと一致するエントリがプレフィックス リスト内に複数存在する場合は、プレフィックス リスト エントリのシーケンス番号によって、シーケンス番号が最小であるエントリが識別されます。

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

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

コマンド内でプレフィックス リストを使用する場合は、あらかじめプレフィックス リストを設定しておく必要があります。プレフィックス リストを作成したり、プレフィックス リストにエントリを追加するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip prefix-list** *list-name* [**seq** *seq-value*] **deny** \| **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*] | 一致条件のために、アクセスを拒否（**deny**）または許可（**permit**）するプレフィックス リストを作成します。シーケンス番号を指定することもできます。少なくとも 1 つの **permit** コマンドまたは **deny** コマンドを入力する必要があります。<br>• *network*/*len* は、ネットワーク番号およびネットワーク マスクの長さ（ビット単位）です。<br>• （任意）**ge** および **le** の値は、照合するプレフィックス長の範囲を指定します。指定された *ge-value* および *le-value* は、次の条件を満たす必要があります。*len* < *ge-value* < *le-value* < 32 |
| ステップ 3 | **ip prefix-list** *list-name* **seq** *seq-value* **deny** \| **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*] | （任意）プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip prefix list** [**detail** \| **summary**] *name* [*network*/*len*] [**seq** *seq-num*] [**longer**] [**first-match**] | プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示して、設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

プレフィックス リストまたはそのエントリをすべて削除するには、**no ip prefix-list** *list-name* グローバル コンフィギュレーション コマンドを使用します。プレフィックス リストから特定のエントリを削除する場合は、**no ip prefix-list seq** *seq-value* グローバル コンフィギュレーション コマンドを使用します。シーケンス番号の自動生成をディセーブルにするには **no ip prefix-list sequence number** コマンドを、自動生成を再びイネーブルにするには **ip prefix-list sequence number** コマンドを使用します。プレフィックス リスト エントリのヒット数テーブルをクリアするには、**clear ip prefix-list** 特権 EXEC コマンドを使用します。

# BGP コミュニティ フィルタリングの設定

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

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

- **internet**：このルートをインターネット コミュニティにアドバタイズします。すべてのルータが所属します。
- **no-export**：EBGP ピアにこのルートをアドバタイズしません。
- **no-advertise**：どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as**：ローカルな AS 外部のピアにこのルートをアドバタイズしません。

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

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

コミュニティに基づいて COMMUNITIES 属性および match 句を設定するには、「ルート マップによるルーティング情報の再配信」（P.39-102）に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

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

コミュニティ リストを作成、適用するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip community-list** *community-list-number* {**permit** \| **deny**} *community-number* | コミュニティ リストを作成し、番号を割り当てます。<br>• *community-list-number* は 1 ～ 99 の整数です。この値は、コミュニティの許可または拒否グループを 1 つまたは複数識別します。<br>• *community-number* は、**set community** ルートマップ コンフィギュレーション コマンドで設定される番号です。 |
| ステップ 3 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **neighbor** {*ip-address* \| *peer-group name*} **send-community** | COMMUNITIES 属性をこの IP アドレスのネイバーに送信することを指定します。 |
| ステップ 5 | **set comm-list** *list-num* **delete** | （任意）ルート マップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **ip bgp-community new-format** | （任意）AA:NN の形式で、BGP コミュニティを表示、解析します。<br>BGP コミュニティは、2 つの部分からなる 2 バイト長フォーマットで表示されます。シスコのデフォルトのコミュニティ フォーマットは NNAA です。BGP に関する最新の RFC では、コミュニティの形式は AA:NN です。最初の部分は自律システム番号で、その次の部分は 2 バイトの数値です。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show ip bgp community** | 設定を確認します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# BGP ネイバーおよびピア グループの設定

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

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

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

BGP ピアを設定するには、特権 EXEC モードで次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **neighbor** *peer-group-name* **peer-group** | BGP ピア グループを作成します。 |
| ステップ 4 | **neighbor** *ip-address* **peer-group** *peer-group-name* | BGP ネイバーをピア グループのメンバにします。 |
| ステップ 5 | **neighbor** {*ip-address* \| *peer-group-name*} **remote-as** *number* | BGP ネイバーを指定します。**remote-as** *number* を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ～ 65535 です。 |
| ステップ 6 | **neighbor** {*ip-address* \| *peer-group-name*} **description** *text* | （任意）ネイバーに記述子を関連付けます。 |
| ステップ 7 | **neighbor** {*ip-address* \| *peer-group-name*} **default-originate** [**route-map** *map-name*] | （任意）BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。 |
| ステップ 8 | **neighbor** {*ip-address* \| *peer-group-name*} **send-community** | （任意）COMMUNITIES 属性をこの IP アドレスのネイバーに送信することを指定します。 |
| ステップ 9 | **neighbor** {*ip-address* \| *peer-group-name*} **update-source** *interface* | （任意）IBGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。 |
| ステップ 10 | **neighbor** {*ip-address* \| *peer-group-name*} **ebgp-multihop** | （任意）ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート（0.0.0.0）の場合、マルチホップ セッションは確立されません。 |
| ステップ 11 | **neighbor** {*ip-address* \| *peer-group-name*} **local-as** *number* | （任意）ローカル自律システムとして使用する自律システム番号を指定します。指定できる範囲は 1 ～ 65535 です。 |
| ステップ 12 | **neighbor** {*ip-address* \| *peer-group-name*} **advertisement-interval** *seconds* | （任意）BGP ルーティング アップデートを送信する最小インターバルを設定します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 13 | **neighbor** {*ip-address* \| *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] | （任意）ネイバーから受信できるプレフィックス数を制御します。指定できる範囲は 1 ～ 4294967295 です。*threshold*（任意）は、警告メッセージが生成される基準となる最大値（%）です。デフォルトは 75% です。 |
| ステップ 14 | **neighbor** {*ip-address* \| *peer-group-name*} **next-hop-self** | （任意）ネイバー宛ての BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。 |
| ステップ 15 | **neighbor** {*ip-address* \| *peer-group-name*} **password** *string* | （任意）TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。 |
| ステップ 16 | **neighbor** {*ip-address* \| *peer-group-name*} **route-map** *map-name* {**in** \| **out**} | （任意）着信または発信ルートにルート マップを適用します。 |
| ステップ 17 | **neighbor** {*ip-address* \| *peer-group-name*} **send-community** | （任意）COMMUNITIES 属性をこの IP アドレスのネイバーに送信することを指定します。 |
| ステップ 18 | **neighbor** {*ip-address* \| *peer-group-name*} **timers** *keepalive holdtime* | （任意）ネイバーまたはピア グループ用のタイマーを設定します。<br>• *keepalive* インターバルは、キープアライブ メッセージがピアに送信される間隔です。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 60 秒です。<br>• *holdtime* は、キープアライブ メッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲は 1 ～ 4294967295 秒です。デフォルト値は 180 秒です。 |
| ステップ 19 | **neighbor** {*ip-address* \| *peer-group-name*} **weight** *weight* | （任意）ネイバーからのすべてのルートに関する重みを指定します。 |
| ステップ 20 | **neighbor** {*ip-address* \| *peer-group-name*} **distribute-list** {*access-list-number* \| *name*} {**in** \| **out**} | （任意）アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 |
| ステップ 21 | **neighbor** {*ip-address* \| *peer-group-name*} **filter-list** *access-list-number* {**in** \| **out** \| **weight** *weight*} | （任意）BGP フィルタを確立します。 |
| ステップ 22 | **neighbor** {*ip-address* \| *peer-group-name*} **version** *value* | （任意）ネイバーと通信するときに使用する BGP バージョンを指定します。 |
| ステップ 23 | **neighbor** {*ip-address* \| *peer-group-name*} **soft-reconfiguration inbound** | （任意）受信したアップデートを保管するようにソフトウェアを設定します。 |
| ステップ 24 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 25 | **show ip bgp neighbors** | 設定を確認します。 |
| ステップ 26 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

既存の BGP ネイバーまたはネイバー ピア グループをディセーブルにするには、**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。ディセーブル化されている既存のネイバーまたはネイバー ピア グループをイネーブルにするには、**no neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。

# 集約アドレスの設定

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

ルーティング テーブル内に集約アドレスを作成するには、特権 EXEC モードで次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aggregate-address** *address mask* | BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは自律システムからのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。 |
| ステップ 4 | **aggregate-address** *address mask* **as-set** | （任意）自律システム設定パス情報を生成します。このコマンドは、この前のコマンドと同じ規則に従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。 |
| ステップ 5 | **aggregate-address** *address-mask* **summary-only** | （任意）サマリー アドレスだけをアドバタイズします。 |
| ステップ 6 | **aggregate-address** *address mask* **suppress-map** *map-name* | （任意）選択された、より具体的なルートを抑制します。 |
| ステップ 7 | **aggregate-address** *address mask* **advertise-map** *map-name* | （任意）ルート マップによって指定された設定に基づいて、集約を生成します。 |
| ステップ 8 | **aggregate-address** *address mask* **attribute-map** *map-name* | （任意）ルート マップで指定された属性を持つ集約を生成します。 |
| ステップ 9 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show ip bgp neighbors** [**advertised-routes**] | 設定を確認します。 |
| ステップ 11 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

集約エントリを削除するには、**no aggregate-address** *address mask* ルータ コンフィギュレーション コマンドを使用します。オプションをデフォルト値に戻すには、キーワードを指定してコマンドを使用します。

# ルーティング ドメイン連合の設定

IBGP メッシュを削減するには、自律システムを複数のサブ自律システムに分割して、単一の自律システムとして表示される単一の*連合*にグループ化します。各 AS は内部で完全にメッシュ化されていて、同じ連合内の他の AS との間には数本の接続があります。異なる AS 内にあるピアでは EBGP セッショ

ンが使用されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。特に、ネクストホップ、MED、およびローカル初期設定情報が維持されるため、すべての AS で単一の IGP を使用できます。

BGP 連合を設定するには、自律システム グループの自律システム番号として機能する連合 ID を指定する必要があります。

BGP 連合を設定するには、特権 EXEC モードで次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **bgp confederation identifier** *autonomous-system* | BGP 連合 ID を設定します。 |
| ステップ 4 | **bgp confederation peers** *autonomous-system* [*autonomous-system autonomous-system ...*] | 連合に属する自律システム、および特殊な EBGP ピアとして処理する自律システムを指定します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip bgp neighbor**<br>**show ip bgp network** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# BGP ルート リフレクタの設定

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

ルート リフレクタを使用する場合は、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。Internal BGP ピアを*ルート リフレクタ*に設定すると、その IBGP ピアは IBGP によって取得されたルートを一連の IBGP ネイバーに送信します。ルート リフレクタの内部ピアは、*クライアント ピア*と*非クライアント ピア*（自律システム内の他のすべてのルータ）に分けられます。ルート リフレクタは、これらの 2 つのグループ間でルートを反映させます。ルート リフレクタおよびそのクライアント ピアは、*クラスタ*を形成します。非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

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

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、クラスタはルート リフレクタのルータ ID で識別されます。冗長性を高めて、シングル ポイントでの障害を回避するには、クラスタに複数のルート リフレクタを設定できます。この場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じ

クラスタ ID（4 バイト）を設定する必要があります。クラスタを処理するすべてのルート リフレクタは完全メッシュ構造にし、一連の同一なクライアント ピアおよび非クライアント ピアを設定する必要があります。

ルート リフレクタおよびクライアントを設定するには、特権 EXEC モードで次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **neighbor** {*ip-address* \| *peer-group-name*} **route-reflector-client** | ローカル ルータを BGP ルート リフレクタに、指定されたネイバーをクライアントに設定します。 |
| ステップ 4 | **bgp cluster-id** *cluster-id* | （任意）クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。 |
| ステップ 5 | **no bgp client-to-client reflection** | （任意）クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルート リフレクタはルートをクライアントに反映させる必要がありません。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ip bgp** | 設定を確認します。送信元の ID およびクラスタリスト属性を表示します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# ルート ダンプニングの設定

ルート フラップ ダンピング化は、インターネットワーク内でフラッピング ルートの伝播を最小化するための BGP 機能です。ルートのフラッピングが行われるのは、ルートが使用可能、使用不可能、使用可能、使用不可能のように、状態が継続的に変化する場合です。ルート ダンプニングがイネーブルの場合は、フラッピングしているルートに *penalty* 値が割り当てられます。ルートの累積ペナルティが設定済みの制限値に達すると、ルートが稼働している場合でも、BGP はルートのアドバタイズメントを抑制します。*再使用限度*は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが自律システムの外部にあるルートよりも大きくなることはありません。

BGP ルート ダンプニングを設定するには、EXEC モードで次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router bgp** *autonomous-system* | BGP ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **bgp dampening** | BGP ルート ダンプニングをイネーブルにします。 |
| ステップ 4 | **bgp dampening** *half-life reuse suppress max-suppress* [**route-map** *map*] | （任意）ルート ダンプニング係数のデフォルト値を変更します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **show ip bgp flap-statistics** [{**regexp** *regexp*} \| {**filter-list** *list*} \| {*address mask* [**longer-prefix**]}] | （任意）フラッピングしているすべてのパスのフラップをモニタします。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。 |
| ステップ 7 | **show ip bgp dampened-paths** | （任意）抑制されるまでの時間を含めて、減衰されたルートを表示します。 |
| ステップ 8 | **clear ip bgp flap-statistics** [{**regexp** *regexp*} \| {**filter-list** *list*} \| {*address mask* [**longer-prefix**]} | （任意）BGP フラップ統計情報を消去して、ルートがダンピング化される可能性を小さくします。 |
| ステップ 9 | **clear ip bgp dampening** | （任意）ルート ダンプニング情報を消去して、ルートの抑制を解除します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

フラップ ダンプニングをディセーブルにするには、キーワードを指定しないで **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。ダンプニング係数をデフォルト値に戻すには、値を指定して **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。

# BGP のモニタリングおよびメンテナンス

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

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。この情報を使用して、リソースの利用率の判別や、ネットワーク問題の解決を行うことができます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

表 39-8 に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。表示フィールドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

**表 39-11　IP BGP の clear および show コマンド**

| コマンド | 目的 |
|---|---|
| **clear ip bgp** *address* | 特定の BGP 接続をリセットします。 |
| **clear ip bgp *** | すべての BGP 接続をリセットします。 |
| **clear ip bgp peer-group** *tag* | BGP ピア グループのすべてのメンバを削除します。 |
| **show ip bgp** *prefix* | プレフィックスがアドバタイズされるピア グループ、またはピア グループに含まれないピアを表示します。ネクスト ホップやローカル プレフィックスなどのプレフィックス属性も表示されます。 |
| **show ip bgp cidr-only** | サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。 |
| **show ip bgp community** [*community-number*] [**exact**] | 指定されたコミュニティに属するルートを表示します。 |
| **show ip bgp community-list** *community-list-number* [**exact-match**] | コミュニティ リストで許可されたルートを表示します。 |
| **show ip bgp filter-list** *access-list-number* | 指定された自律システム パス アクセス リストによって照合されたルートを表示します。 |
| **show ip bgp inconsistent-as** | 送信元の AS と矛盾するルートを表示します。 |

表 39-11　IP BGP の clear および show コマンド（続き）

| コマンド | 目的 |
|---|---|
| **show ip bgp regexp** *regular-expression* | コマンドラインに入力された指定の正規表現と一致する自律システム パスを持つルートを表示します。 |
| **show ip bgp** | BGP ルーティング テーブルの内容を表示します。 |
| **show ip bgp neighbors** [*address*] | 各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。 |
| **show ip bgp neighbors** [*address*] [**advertised-routes** \| **dampened-routes** \| **flap-statistics** \| **paths** *regular-expression* \| **received-routes** \| **routes**] | 特定の BGP ネイバーから取得されたルートを表示します。 |
| **show ip bgp paths** | データベース内のすべての BGP パスを表示します。 |
| **show ip bgp peer-group** [*tag*] [**summary**] | BGP ピア グループに関する情報を表示します。 |
| **show ip bgp summary** | すべての BGP 接続のステータスを表示します。 |

また、**bgp log-neighbor changes** ルータ コンフィギュレーション コマンドを使用し、BGP ネイバーをリセット、起動、またはダウンさせるときに生成されるメッセージのロギングをイネーブルにすることもできます。

# ISO CLNS ルーティングの設定

International Organization for Standardization（ISO; 国際標準化機構）Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）プロトコルとは、Open System Interconnection（OSI; オープン システム インターコネクション）モデルのネットワーク層の標準の 1 つです。ISO ネットワーク アーキテクチャ内のアドレスは、Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスおよび Network Entity Titles（NETs）と呼ばれます。OSI ネットワークの各ノードには、1 つ以上の NETs が含まれます。さらに、各ノードには、多数の NSAP アドレスが含まれます。

スイッチ上で、**clns routing** グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをイネーブルにすると、スイッチはルーティング関連の機能を果たさず、転送の決定だけを行います。ダイナミック ルーティングには、ルーティング プロトコルもイネーブルにする必要があります。スイッチは、Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティング プロトコルをサポートします。このプロトコルは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づいています。

動的にルーティングを行う場合は、IS-IS を使用します。このルーティング プロトコルは、*エリア*の概念をサポートします。1 つのエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータは適切なエリアに到達する方法を認識しています。IS-IS は、*ステーション ルーティング*（1 つのエリア内）および*エリア ルーティング*（エリア間）という 2 つのレベルのルーティングをサポートします。

ISO IGRP と IS-IS NSAP アドレス方式の主な違いは、エリア アドレスの定義にあります。両方ともレベル 1 ルーティング（1 つのエリア内）にはシステム ID を使用します。ただし、エリア ルーティングに関してアドレスが指定される方法が異なります。ISO IGRP NSAP アドレスには、*ドメイン*、*エリア*、および*システム ID* という 3 つの異なるフィールドが含まれます。IS-IS アドレスには、単一の連続的*エリア*フィールド（ドメイン フィールドおよびエリア フィールドから成る）と*システム ID* という 2 つのフィールドが含まれます。

（注）　ISO CLNS の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.2*』を参照してください。この章で使用されるコマンドの構文および使用方法の詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*』を参照するか、IOS コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

# IS-IS ダイナミック ルーティングの設定

IS-IS は、ISO ダイナミック ルーティング プロトコルの 1 つです（ISO 105890 で説明されている）。その他のルーティング プロトコルとは異なり、IS-IS をイネーブルするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することで、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロトコルを指定できます。その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのルータが含まれる単一のエリアとして構築されます。ネットワークの規模が大きくなるに従って、このネットワークは、すべてのエリアに属する、接続されたすべてのレベル 2 ルータのセットから構成されるバックボーン エリア内に再編成され、その後、このネットワークはローカル エリアに接続されます。1 つのローカル エリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を認識しており、バックボーン ルータは他のエリアに到達する方法を認識しています。

ルータは、ローカル エリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します（ステーション ルーティング）。ルータは、レベル 1 のエリア間でルーティングを実行するために、レベル 2 の隣接関係を確立します（エリア ルーティング）。

1 つの Cisco ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。一般に、ルーティング プロセスごとに 1 つのエリアに対応します。デフォルトでは、ルーティング プロセスの最初のインスタンスが、レベル 1 および レベル 2 両方のルーティングを実行するように設定されます。追加のルーティング インスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個の レベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。ルータ インスタンスにレベル 2 ルーティングが必要でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 の機能を削除します。別のルータ インスタンスをレベル 2 ルータとして設定する場合にも **is-type** コマンドを使用します。

（注）　IS-IS の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Routing Protocols」の章を参照してください。ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Release 12.2*』を参照してください。

ここでは、IS-IS ルーティングの設定方法を簡単に説明します。内容は次のとおりです。

- 「IS-IS のデフォルト設定」（P.39-73）
- 「IS-IS ルーティングのイネーブル化」（P.39-74）
- 「IS-IS グローバル パラメータの設定」（P.39-76）

- 「IS-IS インターフェイス パラメータの設定」（P.39-78）

## IS-IS のデフォルト設定

表 39-12 に、IS-IS のデフォルト設定を示します。

**表 39-12　IS-IS のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| リンクステート PDU（LSP）エラーを無視 | イネーブル |
| IS-IS タイプ | 従来型の IS-IS：ルータは、レベル 1（ステーション）とレベル 2（エリア）両方のルータとして機能します。<br>マルチエリア IS-IS：IS-IS ルーティング プロセスの最初のインスタンスが レベル 1-2 ルータです。残りのインスタンスは、レベル 1 ルータです。 |
| デフォルト情報送信元 | ディセーブル |
| IS-IS 隣接関係のステート変更を記録 | ディセーブル |
| LSP 生成スロットリング タイマー | 連続で生成した 2 つの間の最大インターバル：5 秒<br>初期 LSP 生成遅延：50 ミリ秒<br>1 番目と 2 番目の LSP 生成間のホールド タイム：5000 ミリ秒 |
| LSP 最大ライフ タイム（リフレッシュなし） | LSP パケットが削除されるまで 1200 秒（20 分） |
| LSP リフレッシュ インターバル | LSP リフレッシュを 900 秒（15 分）ごとに送信 |
| 最大 LSP パケット サイズ | 1497 バイト |
| NSF 認識[1] | イネーブル[2]。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。 |
| Partial Route Computation（PRC; 部分ルート計算）スロットリング タイマー | 最大 PRC 待機インターバル：5 秒<br>トポロジの変更後の初期 PRC 計算遅延：2000 ミリ秒<br>1 番目と 2 番目の PRC 計算間のホールド タイム：5000 ミリ秒 |
| パーティション回避 | ディセーブル |
| Password | エリアまたはドメインのパスワードが定義されておらず、認証はディセーブルになっています。 |
| 過負荷ビットの設定 | ディセーブル イネーブルの際に引数が入力されない場合、過負荷ビットが直ちに設定され、**no set-overload-bit** コマンドが入力されるまで設定されたままになります。 |
| Shortest Path First（SPF）スロットリング タイマー | 連続した SFP 間の最大インターバル：10 秒<br>トポロジの変更後の初期 SFP 計算：5500 ミリ秒<br>1 番目と 2 番目の SFP 計算間のホールド タイム：5500 ミリ秒 |
| サマリー アドレス | ディセーブル |

1. NSF = Nonstop Forwarding
2. IS-IS NSF 認識は、Cisco IOS Release 12.2（25）SEG 以降を実行するスイッチ上で IPv4 に対してイネーブルになっています。

## NSF 認識

Cisco IOS Release 12.2（25）SEG からは、IPv4 向けに統合 IS-IS NSF 認識機能がサポートされます。この機能により、NSF を認識する顧客宅内装置（CPE）ルータが、NFS 対応ルータによるパケットのノンストップ転送を実現します。ローカル ルータでは、必ずしも NSF を実行している必要はありませんが、このルータが NSF を認識していると、スイッチオーバー プロセス時にルーティング データベースの整合性と精度、および隣接 NSF 対応ルータ上のリンクステート データベースが保持されます。

この機能は、自動的にイネーブルにされ、設定は必要ありません。この機能の詳細については、『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

## IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティング プロセスに名前と NET を指定します。その後、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

IS-IS をイネーブルにし、IS-IS ルーティング プロセスの各インターフェイスに エリアを指定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **clns routing** | スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。 |
| ステップ 3 | **router isis** [*area tag*] | 指定したルーティング プロセスに対して IS-IS ルーティング プロセスをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。<br>（任意）*area tag* 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。複数の IS-IS エリアを設定する場合は、値を入力する必要があります。<br>最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。後のインスタンスは、自動的にレベル 1 になります。**is-type** グローバル コンフィギュレーション コマンドを使用してルーティングのレベルを変更できます。 |
| ステップ 4 | **net** *network-entity-title* | ルーティング プロセスに NET を設定します。マルチエリア IS-IS を設定する場合、各ルーティング プロセスに NET を指定します。NET およびアドレスに対して名前を指定できます。 |
| ステップ 5 | **is-type** {**level-1** \| **level-1-2** \| **level-2-only**} | （任意）ルータは、レベル 1（ステーション）ルータ、マルチエリア ルーティング用のレベル 2（エリア）ルータ、または両方（デフォルト）として設定できます。<br>• **level-1**：ステーション ルータとしてだけ機能<br>• **level-1-2**：ステーションおよびエリア ルータの両方として機能<br>• **level 2**：エリア ルータだけとして機能 |
| ステップ 6 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 7 | **interface** *interface-id* | IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 8 | **ip router isis** [*area tag*] | インターフェイス上の ISO CLNS に対して IS-IS ルーティング プロセスを設定し、ルーティング プロセスにエリア デジグネータを接続します。 |
| ステップ 9 | **clns router isis** [*area tag*] | インターフェイス上で ISO CLNS をイネーブルにします。 |
| ステップ 10 | **ip address** *ip-address-mask* | インターフェイスの IP アドレスを定義します。インターフェイスのいずれかが IS-IS ルーティングに設定されている場合は、イネーブルになっているエリアに含まれるすべてのインターフェイスで IP アドレスが必要です。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show isis** [*area tag*] **database detail** | 入力内容を確認します。 |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

IS-IS ルーティングをディセーブルにするには、**no router isis** *area-tag* ルータ コンフィギュレーション コマンドを使用します。

次に、従来型の IS-IS を IP ルーティング プロトコルとして実行するために 3 つのルータを設定する方法を示します。従来型の IS-IS では、すべてのルータはレベル 1 およびレベル 2 のルータとして機能します（デフォルト）。

**ルータ A**

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

**ルータ B**

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

**ルータ C**

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
```

```
Switch(config-router)# exit
```

## IS-IS グローバル パラメータの設定

設定可能ないくつかのオプションの IS-IS グローバル パラメータを次に示します。

- ルート マップによって制御されるデフォルト ルートを設定することで、デフォルト ルートを IS-IS ルーティング ドメイン内に強制的に設定できます。ルート マップで設定可能な、その他のフィルタリング オプションも指定できます。
- 内部チェックサム エラーとともに受信された IS-IS LSP を無視したり、破損した LSP を消去するようにルータを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。
- サマリー アドレスを使用して、ルーティング テーブル内に表示される集約アドレスを作成できます（経路集約）。他のルーティング プロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバルおよび LSP がリフレッシュなしでルータ データベース内にとどまることができる最大時間を設定できます。
- LSP 生成に対するスロットリング タイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、スイッチがログ メッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の 最大伝送単位（MTU）サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。
- パーティション回避ルータ コンフィギュレーション コマンドは、レベル 1-2 境界ルータ、隣接レベル 1 ルータ、およびエンド ホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぎます。

IS-IS パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **clns routing** | スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。 |
| ステップ 3 | **router isis** | IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **default-information originate** [**route-map** *map-name*] | （任意）デフォルト ルートを IS-IS ルーティング ドメイン内に強制的に設定します。**route-map** *map-name* を入力すると、ルート マップが満たされると、ルーティング プロセスがデフォルト ルートを生成します。 |
| ステップ 5 | **ignore-lsp-errors** | （任意）LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにルータを設定します。このコマンドは、デフォルトでイネーブルになっています（破損した LSP はドロップされます）。破損した LSP を消去するには、**no ignore-lsp-errors** ルータ コンフィギュレーション コマンドを入力します。 |
| ステップ 6 | **area-password** *password* | （任意）レベル 1（ステーション ルータ レベル）LSP に挿入されるエリア認証パスワードを設定します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 7 | **domain-password** *password* | （任意）レベル 2（エリア ルータ レベル）LSP に挿入されるルーティング ドメイン認証パスワードを設定します。 |
| ステップ 8 | **summary-address** *address mask* [**level-1** \| **level-1-2** \| **level-2**] | （任意）所定のレベルのアドレスのサマリーを作成します。 |
| ステップ 9 | **set-overload-bit** [**on-startup** {*seconds* \| **wait-for-bgp**}] | （任意）ルータに問題がある場合に、他のルータが Shortest Path First（SPF; 最短パス優先）計算でこのルータを無視するように過負荷ビット（hippity ビット）を設定ます。<br>• （任意）**on-startup**：起動時だけ過負荷ビットを設定します。**on-startup** が指定されない場合、過負荷ビットが即座に設定され、**no set-overload-bit** コマンドを入力するまで設定されたままになります。**on-startup** が指定された場合、秒数または **wait-for-bgp** を入力する必要があります。<br>• *seconds*：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、この秒数の間設定されたままになります。指定できる範囲は 5 ～ 86400 秒です。<br>• **wait-for-bgp**：**on-startup** キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、BGP が収束するまで設定されたままになります。BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。 |
| ステップ 10 | **lsp-refresh-interval** *seconds* | （任意）LSP リフレッシュ インターバル（秒）を設定します。範囲は 1 ～ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒（15 分）ごとに送信します。 |
| ステップ 11 | **max-lsp-lifetime** *seconds* | （任意）LSP パケットがリフレッシュされずにルータ データベース内に存続する最大時間を設定します。範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定されたタイム インターバルのあと、LSP パケットは削除されます。 |
| ステップ 12 | **lsp-gen-interval** [**level-1** \| **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] | （任意）IS-IS 生成スロットリング タイマーを設定します。<br>• *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒）。指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。<br>• *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒）。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。<br>• *lsp-second-wait*：最初と 2 番めの LSP 生成間（ミリ秒）のホールドタイム。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 |
| ステップ 13 | **spf-interval** [**level-1** \| **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] | （任意）IS-IS SPF スロットリング タイマーを設定します。<br>• *spf-max-wait*：連続する SFP 間（秒）の最大インターバル。指定できる範囲は 1 ～ 120 で、デフォルトは 10 です。<br>• *spf-initial-wait*：トポロジ変更後の最初の SFP 計算（ミリ秒）。指定できる範囲は 1 ～ 10000 で、デフォルトは 5500 です。<br>• *spf-second-wait*：最初と 2 番めの SFP 計算間（ミリ秒）のホールドタイム。指定できる範囲は 1 ～ 10000 で、デフォルトは 5500 です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 14 | **prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] | （任意）IS-IS PRC スロットリング タイマーを設定します。<br>• *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒）。指定できる範囲は 1 ～ 120 秒です。デフォルト値は 5 秒です。<br>• *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒）。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 2000 ミリ秒です。<br>• *prc-second-wait*：最初と 2 番めの PRC 計算間（ミリ秒）のホールド タイム。指定できる範囲は 1 ～ 10,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 |
| ステップ 15 | **log-adjacency-changes** [**all**] | （任意）IS-IS 隣接ステート変更をログするようルータを設定します。End System-to-Intermediate System PDU および Link State Packet（LSP; リンクステート パケット）など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに含めるには、**all** を入力します。 |
| ステップ 16 | **lsp-mtu** *size* | （任意）最大 LSP パケット サイズ（バイト）を指定します。指定できる範囲は 128 ～ 4352 バイトです。デフォルト値は 1497 バイトです。<br>**（注）** ネットワーク内の任意のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。 |
| ステップ 17 | **partition avoidance** | （任意）境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアドバタイズしないようにします。 |
| ステップ 18 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 19 | **show clns** | 入力内容を確認します。 |
| ステップ 20 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト ルート生成をディセーブルにするには、**no default-information originate** ルータ コンフィギュレーション コマンドを使用します。**no area-password** または **no domain-password** ルータ コンフィギュレーション コマンドを使用して、パスワードをディセーブルにします。LSP MTU 設定をディセーブルにするには、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレス指定、LSP リフレッシュ インターバル、LSP ライフタイム、LSP タイマー、SPF タイマー、および PRC タイマーをデフォルト状態に戻すには、コマンドの **no** 形式を使用します。**no partition avoidance** ルータ コンフィギュレーション コマンドを使用して、出力形式をディセーブルにします。

## IS-IS インターフェイス パラメータの設定

任意で、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数およびタイム インターバルなど）をデフォルトから変更する場合、複数のルータおよびインターフェイス上でもこれを変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック：Quality of Service（QoS）ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- hello インターバル（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数：インターフェイス上で使用されて、IS-IS hello パケットで送信されるホールド タイムを決定します。ホールド タイムは、ネイバーがダウンしていると宣言するまでに、別の

hello パケットを待機する時間を決定します。これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。hello パケットが頻繁に損失され、IS-IS 隣接で不要に障害が発生する場合は、hello 乗数を変更します。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、hello プロトコルの信頼性を高めることができます。

- その他のタイム インターバル：
  - Complete Sequence Number PDU（CSNP）インターバル CSNP は、指定ルータにより送信され、データベースの同期を維持します。
  - 再送信インターバル これは、ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
  - IS-IS LSP 再送信スロットル インターバル これは、IS-IS LSP がポイントツーポイント リンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、*同じ* LSP が連続する再送信間隔である再送信インターバルとは異なります。
- 指定ルータの選択プライオリティ：マルチアクセス ネットワークで必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証

IS-IS インターフェイス パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、**no switchport** コマンドを入力し、インターフェイスをレイヤ 3 モードにします。 |
| ステップ 3 | **isis metric** *default-metric* [**level-1** \| **level-2**] | （任意）指定したインターフェイスにメトリック（またはコスト）を設定します。指定できる範囲は 0 ～ 63 です。デフォルトは 10 です。レベルが入力されない場合は、レベル 1 およびレベル 2 ルータの両方にデフォルト値が適用されます。 |
| ステップ 4 | **isis hello-interval** {*seconds* \| **minimal**} [**level-1** \| **level-2**] | （任意）スイッチが hello パケットを送信する間隔を指定します。デフォルトでは、hello インターバル *seconds* の 3 倍の値が、送信される hello パケットの *holdtime* としてアドバタイズされます。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。<br>• **minimal**：ホールド タイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。<br>• *seconds*：指定できる範囲は、1 ～ 65,535 秒です。デフォルトは 10 秒です。 |
| ステップ 5 | **isis hello-multiplier** *multiplier* [**level-1** \| **level-2**] | （任意）ルータが隣接装置のダウンを宣言するまでに、ネイバーが損失する IS-IS hello パケット数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。 |
| ステップ 6 | **isis csnp-interval** *seconds* [**level-1** \| **level-2**] | （任意）インターフェイスに IS-IS CSNP を設定します。指定できる範囲は 0 ～ 65535 です。デフォルトは 10 秒です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 7 | **isis retransmit-interval** *seconds* | （任意）ポイントツーポイント リンクの IS-IS LSP の再送信間隔（秒）を設定します。指定する値は、ネットワーク上の任意の 2 つのルータ間の予測ラウンドトリップ遅延よりも大きい整数である必要があります。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 秒です。 |
| ステップ 8 | **isis retransmit-throttle-interval** *milliseconds* | （任意）IS-IS LSP 再送信スロットル インターバルを設定します。これは、IS-IS LSP がポイントツーポイント リンク上で再送信される最大レート（パケット間のミリ秒数）です。指定できる範囲は 0 ～ 65535 です。デフォルト値は、**isis lsp-interval** コマンドにより決定します。 |
| ステップ 9 | **isis priority** *value* [**level-1** \| **level-2**] | （任意）指定ルータ選択で使用するプライオリティを設定します。指定できる範囲は 0 ～ 127 です。デフォルト値は 64 です。 |
| ステップ 10 | **isis circuit-type** {**level-1** \| **level-1-2** \| **level-2-only**} | （任意）指定されたインターフェイス上のネイバーで必要な隣接タイプを設定します（インターフェイスの回線タイプを指定します）。<br>• **level-1**：このノードとネイバーの両方に共通のエリア アドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。<br>• **level-1-2**：ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。これはデフォルトです。<br>• **level 2**：レベル 2 隣接関係が確立されます。隣接ルータがレベル 1 ルータである場合、隣接関係は確立されません。 |
| ステップ 11 | **isis password** *password* [**level-1** \| **level-2**] | （任意）インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。 |
| ステップ 12 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show clns interface** *interface-id* | 入力内容を確認します。 |
| ステップ 14 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト設定に戻るには、コマンドの **no** 形式を使用します。

# ISO IGRP と IS-IS のモニタリングおよびメンテナンス

CLNS キャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

表 39-13 に、ISO CLNS および IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『*Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*』を参照するか、Cisco IOS コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

**表 39-13　ISO CLNS と IS-IS の clear および show コマンド**

| コマンド | 目的 |
|---|---|
| **clear clns cache** | CLNS ルーティング キャッシュを消去して、再初期化します。 |
| **clear clns es-neighbors** | 隣接データベースから End System（ES）ネイバー情報を削除します。 |
| **clear clns is-neighbors** | 隣接データベースから Intermediate System（IS）ネイバー情報を削除します。 |
| **clear clns neighbors** | 隣接データベースから CLNS ネイバー情報を削除します。 |
| **clear clns route** | ダイナミックに取得された CLNS ルーティング情報を削除します。 |
| **show clns** | CLNS ネットワークについての情報を表示します。 |
| **show clns cache** | CLNS ルーティング キャッシュのエントリを表示します。 |
| **show clns es-neighbors** | 関連するエリアを含む、ES ネイバー エントリを表示します。 |
| **show clns filter-expr** | フィルタ式を表示します。 |
| **show clns filter-set** | フィルタ セットを表示します。 |
| **show clns interface** [*interface-id*] | 各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。 |
| **show clns neighbor** | IS-IS ネイバーについての情報を表示します。 |
| **show clns protocol** | このルータの IS-IS または ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。 |
| **show clns route** | このルータが認識している CLNS パケットのルーティング方法について、その宛先をすべて表示します。 |
| **show clns traffic** | このルータが認識している CLNS パケットの情報を表示します。 |
| **show ip route isis** | ISIS IP ルーティング テーブルの現在のステートを表示します。 |
| **show isis database** | IS-IS リンクステート データベースを表示します。 |
| **show isis routes** | IS-IS レベル 1 ルーティング テーブルを表示します。 |
| **show isis spf-log** | IS-IS の SPF 計算履歴を表示します。 |
| **show isis topology** | すべてのエリア内の接続されたルータすべてのリストを表示します。 |
| **show route-map** | 設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |
| **trace clns** *destination* | ネットワークのパケットが指定された宛先までに経由するパスを検出します。 |
| **which-route** {*nsap-address* \| *clns-name*} | 指定された CLNS 宛先が検出されたルーティング テーブルを表示します。 |

# Multi-VRF CE の設定

バーチャル プライベート ネットワーク（VPN）を使用すると、お客様は ISP バックボーン ネットワーク上で帯域幅を安全に共有できます。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つ以上のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VPN ルーティング/転送（VRF）テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

スイッチでは、スイッチが IP サービス フィーチャ セットを実行している場合は、カスタマー エッジ（CE）デバイスで複数の VPN ルーティング/転送（マルチ VRF）インスタンス（マルチ VRF CE）がサポートされます。サービス プロバイダーは、マルチ VRF CE を使用して、重複する IP アドレスで複数の VPN をサポートできます。

（注）　スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。MPLS VRF の詳細については、『*Cisco IOS Switching Services Configuration Guide, Release 12.2*』を参照してください。

ここでは、次の情報について説明します。


- 「Multi-VRF CE の概要」（P.39-82）
- 「Multi-VRF CE のデフォルト設定」（P.39-84）
- 「マルチ VRF CE の設定時の注意事項」（P.39-84）
- 「VRF の設定」（P.39-85）
- 「VRF 認識サービスの設定」（P.39-86）
- 「マルチキャスト VRF の設定」（P.39-90）
- 「VPN ルーティング セッションの設定」（P.39-91）
- 「BGP PE/CE ルーティング セッションの設定」（P.39-92）
- 「Multi-VRF CE の設定例」（P.39-92）
- 「Multi-VRF CE ステータスの表示」（P.39-96）


## Multi-VRF CE の概要

マルチ VRF CE は、サービス プロバイダーが、VPN 間で IP アドレスが重複する複数の VPN をサポートできるようにする機能です。マルチ VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つ以上のレイヤ 3 インターフェイスを各 VRF に関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN スイッチ仮想インターフェイス（SVI）のように論理的なもののいずれかにできますが、一度に複数の VRF に属すことはできません。

（注）　Multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

Multi-VRF CE には、次のデバイスが含まれます。

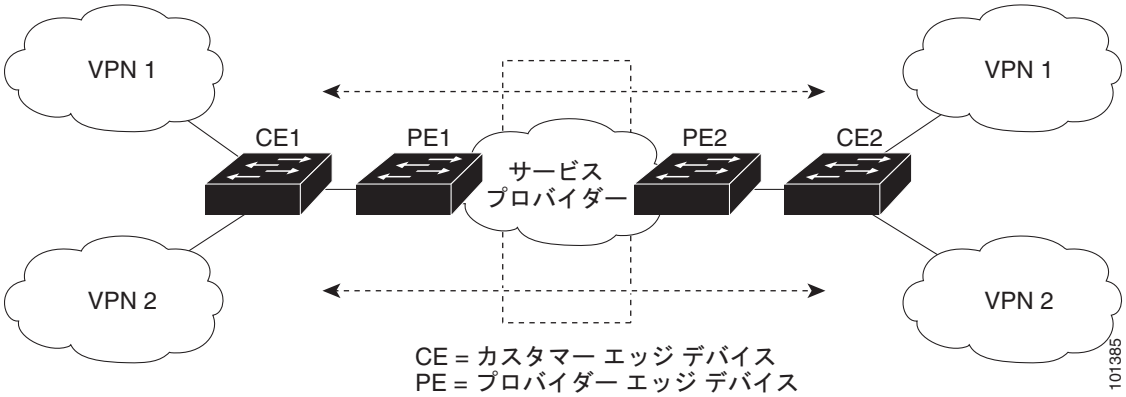
- カスタマー エッジ（CE）デバイスは、1 つ以上のプロバイダー エッジ（PE）ルータへのデータ リンクを介して、サービス プロバイダー ネットワークにアクセスできるようにします。CE デバイスは、サイトのローカル ルートをルータにアドバタイズし、リモート VPN ルートをそこから取得します。スイッチを CE に設定することができます。

- プロバイダー エッジ（PE）ルータは CE デバイスとルーティング情報を交換する際に、スタティック ルーティング、または BGP、RIPv2、OSPF、または EIGRP などのルーティング プロトコルを使用します。直接接続している VPN の VPN ルートを維持するには、PE だけが必要です。PE は、すべてのサービス プロバイダーの VPN ルートだけを維持する必要があります。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- プロバイダー ルータまたはコア ルータは、CE デバイスに接続されていない、サービス プロバイダー ネットワーク内の任意のルータです。

Multi-VRF CE では、複数のお客様が 1 つの CE を共有でき、CE と PE の間で 1 つの物理リンクだけが使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。マルチ VRF CE は、制限付きの PE 機能を CE デバイスに拡張します。次に、別々の VRF テーブルを維持し、VPN のプライバシおよびセキュリティを支店に拡張できます。

図 39-6 に、スイッチを複数の仮想 CE として使用した例を示します。このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。この場合、スイッチにはマルチ VRF CE のサポートが必要です。Multi-VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

**図 39-6　　複数の仮想 CE として機能するスイッチ**




CE スイッチは、VRF にレイヤ 3 インターフェイスを追加するコマンドを受信すると、マルチ VRF CE 関連データ構造内の VLAN ID と Policy Label（PL; ポリシー ラベル）間にマッピングを設定して、この VLAN ID および PL を VLAN データベースに追加します。

マルチ VRF CE が設定されている場合、レイヤ 3 転送テーブルは事実上 2 つの部分に分割されます。

- Multi-VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID は異なるポリシー ラベルにマッピングされ、処理中に VRF を区別するために使用されます。レイヤ 3 設定機能では、取得した新しい VPN ルートごとに、入力ポートの VLAN ID を使用してポリシー ラベルを取得し、マルチ VRF CE ルーティング セクションにポリシー ラベルおよび新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポート内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

Multi-VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力 PL 番号に基づいてルーティング テーブルを検索します。ルートが見つかると、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかると、パケットを正しい隣接デバイスに転送します。
- CE は、出力 PE からパケットを受信すると、入力 PL を使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、PE は VPN 内のパケットを転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が望ましいルーティング プロトコルです。マルチ VRF CE ネットワークには、次の主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバのリスト。VPN コミュニティ メンバごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバ間で、全トラフィックを伝送します。

# Multi-VRF CE のデフォルト設定

表 39-14 に、マルチ VRF CE のデフォルト設定を示します。

**表 39-14　Multi-VRF CE のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| VRF | ディセーブル VRF は定義されていません。 |
| マップ | インポート マップ、エクスポート マップ、ルート マップは定義されていません。 |
| VRF 最大ルート数 | ファスト イーサネット スイッチ：8000<br>ギガビット イーサネット スイッチ：12,000 |
| 転送テーブル | インターフェイスのデフォルトは、グローバル ルーティング テーブルです。 |

# マルチ VRF CE の設定時の注意事項

マルチ VRF CE を使用するには、スイッチで IP サービス フィーチャ セットがイネーブルになっている必要があります。

ネットワークにマルチ VRF CE を設定する場合は、次の考慮事項があります。

- Multi-VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。

- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- Multi-VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。それぞれのお客様には独自の VLAN があります。
- Multi-VRF CE ではサポートされない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータでは、マルチ VRF CE の使用と複数の CE の使用に違いは認識されません。図 39-6 では、複数の仮想レイヤ 3 インターフェイスが Multi-VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF がサポートされます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しない限り、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルを識別する特定のルーティング テーブル ID にマッピングされます。
- スイッチでは、1 つのグローバル ネットワークと最大 26 個の VRF がサポートされます。
- CE と PE の間では、ほとんどのルーティング プロトコル（BGP、OSPF、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP は、ルートの属性を CE に渡す作業を単純化します。
- Multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- VRF がスイッチまたはスイッチ スタックで設定されているかどうかに関係なく、104 個のポリシーを設定できます。
- プライベート VLAN で VRF をイネーブルにできます（その逆も同様）。
- ポリシーベース ルーティング（PBR）がインターフェイスでイネーブルになっている（その逆も同様）場合は、VRF をイネーブルにできません。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）がインターフェイスでイネーブルになっている（その逆も同様）場合は、VRF をイネーブルにできません。

# VRF の設定

1 つまたは複数の VRF を設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip routing** | IP ルーティングをイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **ip vrf** *vrf-name* | VRF に名前を付けて VRF コンフィギュレーション モードを開始します。 |
| ステップ 4 | **rd** *route-distinguisher* | ルート識別子を指定し、VRF テーブルを作成します。自律システム番号と任意の番号（nnn:y）または IP アドレスと任意の番号（A.B.C.D:y）のいずれかを入力します。 |
| ステップ 5 | **route-target** {**export** \| **import** \| **both**} *route-target-ext-community* | 指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。自律システム番号と任意の番号（nnn:y）または IP アドレスと任意の番号（A.B.C.D:y）のいずれかを入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。 |
| ステップ 6 | **import map** *route-map* | （任意）ルート マップを VRF に関連付けます。 |
| ステップ 7 | **interface** *interface-id* | VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。 |
| ステップ 8 | **ip vrf forwarding** *vrf-name* | VRF をレイヤ 3 インターフェイスに関連付けます。 |
| ステップ 9 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show ip vrf** [**brief** \| **detail** \| **interfaces**] [*vrf-name*] | 設定を確認します。設定した VRF に関する情報を表示します。 |
| ステップ 11 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスを VRF から削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

# VRF 認識サービスの設定

IP サービスは、グローバル ルーティング インスタンス内で実行するグローバル インターフェイス上に設定できます。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF とは、Cisco IOS 内の複数のルーティング インスタンスを意味します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

これらのサービスは VRF 認識です。

- ARP
- ping

- 簡易ネットワーク管理プロトコル（SNMP）
- ホットスタンバイ ルータ プロトコル（HSRP）
- Syslog
- traceroute
- FTP および TFTP
- RADIUS

（注）　VRF 認識サービスは、ユニキャスト リバース パス転送（uRPF）またはネットワーク タイム プロトコル（NTP）でサポートされません。

## ARP のユーザ インターフェイス

ARP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| コマンド | 目的 |
|---|---|
| **show ip arp vrf** *vrf-name* | 指定された VRF 内の ARP テーブルを表示します。 |

## ping のユーザ インターフェイス

ping の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| コマンド | 目的 |
|---|---|
| **ping vrf** *vrf-name* **ip-host** | 指定された VRF 内の ARP テーブルを表示します。 |

## SNMP のユーザ インターフェイス

SNMP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **snmp-server trap authentication vrf** | VRF 上のパケットの SNMP トラップをイネーブルにします。 |
| ステップ 3 | **snmp-server engineID remote** *host* **vrf** *vpn-instance engine-id string* | スイッチ上のリモート SNMP エンジンの名前を設定します。 |
| ステップ 4 | **snmp-server host** *host* **vrf** *vpn-instance* **traps** *community* | SNMP トラップ操作の受信側を指定して、SNMP トラップの送信に使用される VRF テーブルを指定します。 |
| ステップ 5 | **snmp-server host** *host* **vrf** *vpn-instance* **informs** *community* | SNMP 情報操作の受信側を指定して、SNMP 情報の送信に使用される VRF テーブルを指定します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **snmp-server user** *user group* **remote** *host* **vrf** *vpn-instance security model* | SNMP アクセス用に、VRF 上にあるリモート ホストの SNMP グループにユーザを追加します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

## HSRP のユーザ インターフェイス

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが、確実に適切な IP ルーティング テーブルに追加されます。

HSRP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **no switchport** | レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。 |
| ステップ 4 | **ip vrf forwarding** *vrf-name* | インターフェイス上に VRF を設定します。 |
| ステップ 5 | **ip address** *ip-address* | インターフェイスの IP アドレスを入力します。 |
| ステップ 6 | **standby 1 ip** *ip-address* | HSRP をイネーブルにして、仮想 IP アドレスを設定します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

## ユニキャスト RPF のユーザ インターフェイス

ユニキャスト RPF は VRF に割り当てられたインターフェイス上に設定可能で、送信元検索が VRF テーブルで実行されます。

ユニキャスト RPF の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 3 | **no switchport** | レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。 |
| ステップ 4 | **ip vrf forwarding** *vrf-name* | インターフェイス上に VRF を設定します。 |
| ステップ 5 | **ip address** *ip-address* | インターフェイスの IP アドレスを入力します。 |
| ステップ 6 | **ip verify unicast reverse-path** | インターフェイスでユニキャスト RPF をイネーブルにします。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

## Syslog のユーザ インターフェイス

Syslog の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **logging on** | ストレージ ルータ イベント メッセージのロギングをイネーブルにしたり、一時的にディセーブルにしたりします。 |
| ステップ 3 | **logging host** *ip-address* **vrf** *vrf-name* | ロギング メッセージが送信される Syslog サーバのホスト アドレスを指定します。 |
| ステップ 4 | **logging buffered** *logging buffered size* **debugging** | 内部バッファへのメッセージを記録します。 |
| ステップ 5 | **logging trap debugging** | Syslog サーバに送信されるロギング メッセージを制限します。 |
| ステップ 6 | **logging facility** *facility* | システム ロギング メッセージをロギング ファシリティに送信します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |

## traceroute のユーザ インターフェイス

traceroute の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| コマンド | 目的 |
|---|---|
| **traceroute vrf** *vrf-name ipaddress* | VPN VRF 内の宛先アドレスを検索するため、その名前を指定します。 |

## FTP および TFTP のユーザ インターフェイス

FTP と TFTP が VRF 認識であるためには、FTP/TFTP のコマンドライン インターフェイス（CLI）コマンドを設定する必要があります。たとえば、インターフェイスに付加される VRF テーブルを使用する場合、E1/0 であれば、CLI **ip [t]ftp source-interface E1/0** を設定して、特定のルーティング テーブルを使用するよう [t]ftp に通知する必要があります。この例では、VRF テーブルは宛先 IP アドレスを検索します。これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。つまり、VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

FTP 接続の送信元 IP アドレスを指定するには、**ip ftp source-interface** show モード コマンドを使用します。接続が確立されているインターフェイスのアドレスを使用するには、**no** 形式のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip ftp source-interface** *interface-type interface-number* | FTP 接続の送信元 IP アドレスを指定します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |

TFTP 接続の送信元アドレスとしてインターフェイスの IP アドレスを指定するには、**ip tftp source-interface** show mode コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip tftp source-interface** *interface-type interface-number* | TFTP 接続の送信元 IP アドレスを指定します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |

## VRF 認識 RADIUS のユーザ インターフェイス

VRF 認識 RADIUS を設定するには、まず RADIUS サーバ上で AAA をイネーブルにする必要があります。このサーバは、次の URL の『*Per VRF AAA Feature Guide*』で説明されているように、**ip vrf forwarding** *vrf-name* サーバグループ コンフィギュレーション コマンドと **ip radius source-interface** グローバル コンフィギュレーション コマンドをサポートします。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

# マルチキャスト VRF の設定

VRF テーブル内でマルチキャストを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンド リファレンス、および『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip routing** | IP ルーティング モードをイネーブルにします |
| ステップ 3 | **ip vrf** *vrf-name* | VRF に名前を付けて VRF コンフィギュレーション モードを開始します。 |
| ステップ 4 | **rd** *route-distinguisher* | ルート識別子を指定し、VRF テーブルを作成します。自律システム番号と任意の番号（nnn:y）または IP アドレスと任意の番号（A.B.C.D:y）のいずれかを入力します。 |
| ステップ 5 | **route-target** {**export** \| **import** \| **both**} *route-target-ext-community* | 指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。自律システム番号と任意の番号（nnn:y）または IP アドレスと任意の番号（A.B.C.D:y）のいずれかを入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。 |
| ステップ 6 | **import map** *route-map* | （任意）ルート マップを VRF に関連付けます。 |
| ステップ 7 | **ip multicast-routing vrf** *vrf*-**name distributed** | （任意）VRF テーブルのグローバルなマルチキャスト ルーティングをイネーブルにします。 |
| ステップ 8 | **interface** *interface-id* | VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。 |
| ステップ 9 | **ip vrf forwarding** *vrf-name* | VRF をレイヤ 3 インターフェイスに関連付けます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 10 | **ip address** *ip-address* **mask** | レイヤ 3 インターフェイスの IP アドレスを設定します。 |
| ステップ 11 | **ip pim sparse-dense mode** | VRF に関連付けられたレイヤ 3 インターフェイスで PIM をイネーブルにします。 |
| ステップ 12 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 13 | **show ip vrf** [**brief** \| **detail** \| **interfaces**] [*vrf-name*] | 設定を確認します。設定した VRF に関する情報を表示します。 |
| ステップ 14 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*Cisco IOS IP Multicast Configuration Guide, Release 12.4*』を参照してください。

# VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル（RIP、OSPF、EIGRP、BGP）、またはスタティック ルーティングで設定できます。ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。

（注）　VRF インスタンス内部で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system** a*utonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

VPN 内で OSPF を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router ospf** *process-id* **vrf** *vrf-name* | OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **log-adjacency-changes** | （任意）隣接状態の変更をログします。これがデフォルトの状態になります。 |
| ステップ 4 | **redistribute bgp** *autonomous-system-number* **subnets** | BGP ネットワークから OSPF ネットワークに情報を再配信するようにスイッチを設定します。 |
| ステップ 5 | **network** *network-number* **area** *area-id* | OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show ip ospf** *process-id* | OSPF ネットワークの設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf** *process-id* **vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。

# BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、特権 EXEC モードで次の手順を実行します。

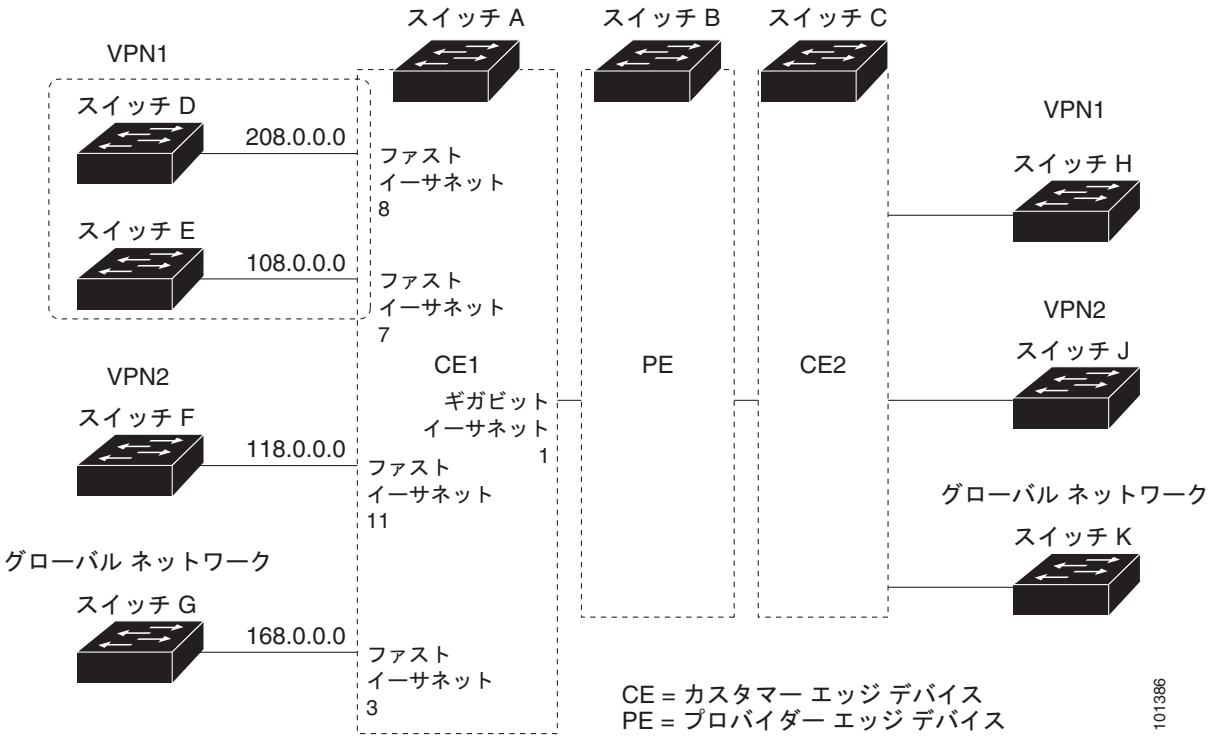
| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **router bgp** *autonomous-system-number* | その他の BGP ルータに自律システム番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 |
| ステップ 3 | **network** *network-number* **mask** *network-mask* | ネットワークとマスクを指定し、BGP を介してアドバタイズします。 |
| ステップ 4 | **redistribute ospf** *process-id* **match internal** | OSPF 内部ルートを再配信するようにスイッチを設定します。 |
| ステップ 5 | **network** *network-number* **area** *area-id* | OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。 |
| ステップ 6 | **address-family ipv4 vrf** *vrf-name* | PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。 |
| ステップ 7 | **neighbor** *address* **remote-as** *as-number* | PE と CE ルータ間の BGP セッションを定義します。 |
| ステップ 8 | **neighbor** *address* **activate** | IPv4 アドレス ファミリのアドバタイズメントをアクティブにします。 |
| ステップ 9 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 10 | **show ip bgp** [**ipv4**] [**neighbors**] | BGP 設定を確認します。 |
| ステップ 11 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

BGP ルーティング プロセスを削除するには、**no router bgp** *autonomous-system-number* グローバル コンフィギュレーション コマンドを使用します。ルーティング特性を削除するには、コマンドにキーワードを指定してこのコマンドを使用します。

# Multi-VRF CE の設定例

図 39-7 は、図 39-6 と同じネットワークの物理接続を単純化した例です。VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。BGP は CE/PE 接続で使用されます。図の後に示されている例は、スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と F の VRF 設定例を示します。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同じです。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 39-7　Multi-VRF CE の設定例




## スイッチ A の設定

スイッチ A では、ルーティングをイネーブルにし、VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビット イーサネット ポート 1 は PE へのトランク接続です。ギガビット イーサネット ポート 8 と 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf v11
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf v12
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティング用に BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf v12
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
```

```
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

### スイッチ D の設定

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

### スイッチ F の設定

スイッチ F は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

### PE スイッチ B の設定

このコマンドをスイッチ B（PE ルータ）で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
```

```
Router(config)# ip cef
Router(config)# interface loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

# Multi-VRF CE ステータスの表示

マルチ VRF CE の設定とステータスに関する情報を表示するには、表 39-15 の特権 EXEC コマンドを使用します。

**表 39-15　マルチ VRF CE 情報を表示するコマンド**

| コマンド | 目的 |
|---|---|
| **show ip protocols vrf** *vrf-name* | VRF に関するルーティング プロトコル情報を表示します。 |
| **show ip route vrf** *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**] | VRF に関する IP ルーティング テーブル情報を表示します。 |
| **show ip vrf** [**brief** \| **detail** \| **interfaces**] [*vrf-name*] | 定義した VRF インスタンスに関する情報を表示します。 |

表示される情報の詳細については、『*Cisco IOS Switching Services Command Reference, Release 12.2*』を参照してください。

# uRPF の設定

ユニキャスト リバース パス転送（uRPF）機能を使用すると、誤った形式の送信元 IP アドレスや偽造（スプーフィング）された送信元 IP アドレスがネットワークに挿入されたために発生する問題を軽減できます。ユニキャスト RPF は、検証可能な送信元 IP アドレスのない IP パケットを廃棄します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的な Denial of Service（DoS; サービス拒絶）攻撃では、偽造の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを活用して、攻撃を突き止めたりフィルタリングしたりする手段を妨げます。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）では、ユニキャスト RPF は、有効な送信元アドレスが割り当てられ、IP ルーティング テーブルとの互換性を持つパケットだけを転送することによって、そのような攻撃を回避します。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

IP ユニキャスト RPF コンフィギュレーション情報の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.2*』の「*Other Security Features*」の項を参照してください。

# プロトコル独立機能の設定

ここでは、IP ルーティング プロトコルに依存しない機能の設定方法について説明します。この機能は、IP ベースまたは IP サービス フィーチャ セットを実行しているスイッチで使用可能です。ただし、IP ベース フィーチャ セットでは、プロトコル関連機能は RIP だけで使用可能です。この章に記載された IP ルーティング プロトコル独立コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocol-Independent Commands」の章を参照してください。このマニュアルには、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

ここでは、次の設定について説明します。


- 「Cisco Express Forwarding および分散型シスコ エクスプレス フォワーディングの設定」（P.39-97）
- 「等価コスト ルーティング パスの個数の設定」（P.39-99）
- 「スタティック ユニキャスト ルートの設定」（P.39-100）
- 「デフォルトのルートおよびネットワークの指定」（P.39-101）
- 「ルート マップによるルーティング情報の再配信」（P.39-102）
- 「ポリシーベース ルーティングの設定」（P.39-106）
- 「ルーティング情報のフィルタリング」（P.39-109）
- 「認証キーの管理」（P.39-112）


## Cisco Express Forwarding および分散型シスコ エクスプレス フォワーディングの設定

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。CEF は、高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、より多くの CPU 処理能力をパケット転送専用にできます。スイッチ スタックでは、スタック メンバーによって分散 CEF（dCEF）が使用されます。スタンドアロン スイッチでは、スイッチは CEF を使用します。動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効化されます。高速スイッチング キャッシュ エントリが無効になると、トラフィックは、ルー

ト キャッシュを使用して高速スイッチングされずに、ルーティング テーブルを使用してプロセス スイッチングされます。CEF と dCEF は転送情報ベース（FIB）検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

CEF および dCEF での 2 つの主要なコンポーネントは、分散 FIB と分散隣接テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラーイメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチまたはスイッチ スタックは、Application Specific Integrated Circuit（ASIC; 特定用途向け IC）を使用してギガビットスピードのラインレート IP トラフィックを実現するため、CEF または dCEF 転送はソフトウェア転送パス、つまり CPU が転送するトラフィックだけに適用されます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF または dCEF がイネーブルになっています。**no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF または dCEF を再度イネーブルにするには、**ip cef** または **ip cef distributed** グローバル コンフィギュレーション コマンドを使用します。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

**注意**　CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で CEF または dCEF をディセーブルにしないようにしてください。

CEF または dCEF がディセーブルになっている場合に、インターフェイス上でグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip cef** | スタンドアロン スイッチで CEF 操作をイネーブルにします。 |
| | または | または |
| | **ip cef distributed** | スイッチ スタックで dCEF 操作をイネーブルにします。 |
| ステップ 3 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。 |
| ステップ 4 | **ip route-cache cef** | インターフェイス上で CEF をイネーブルにします。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show ip cef** | すべてのインターフェイスの CEF ステータスを表示します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 7 | **show cef linecard** [**detail**]<br>または<br>**show cef linecard** [*stack-member-number*] [**detail**] | スタンドアロン スイッチで CEF に関連するインターフェイス情報を表示します。<br>または<br>スタック内のすべてのスイッチまたは指定されたスタック メンバーの dCEF に関連するインターフェイス情報を表示します。<br>（任意）*stack-member-number* には、スタック メンバーを指定します。 |
| ステップ 8 | **show cef interface** [*interface-id*] | すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。 |
| ステップ 9 | **show adjacency** | CEF の隣接テーブル情報を表示します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# 等価コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。1 つの IP ルーティング テーブルにおける複数の等コスト ルートを表示するには、*パラレル パス*を使用することもできます。ネットワークへの等コスト パスが複数あるルータは、これらを同時に使用できます。パラレル パスを使用すると、回線に障害が発生した場合に冗長性を確保できます。また、ルータは、パケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。等コスト ルートは、スタック内の各スイッチでサポートされます。

等コスト ルートはルータによって自動的に取得および設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレル パスの最大数は制御可能です。スイッチ ソフトウェアでは、最大である 32 個の等コスト ルートを使用できますが、1 つのルートにつき 16 個を超えるパスがスイッチで使用されることはありません。

ルーティング テーブルに格納されるパラレル パスのデフォルトの最大数を変更するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router** {**bgp** \| **rip** \| **ospf** \| **eigrp**} | ルータ コンフィギュレーション モードを開始します。<br>IP ベース フィーチャ セットを実行しているスイッチは、**rip** キーワードだけをサポートしています。 |
| ステップ 3 | **maximum-paths** *maximum* | プロトコル ルーティング テーブルのパラレル パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合だけ 1 です。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip protocols** | *Maximum path* フィールドの設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト値に戻すには、**no maximum-paths** ルータ コンフィギュレーション コマンドを使用します。

# スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを動的に構築できない場合、スタティック ルートは重要であり、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip route** *prefix mask* {*address* \| *interface*} [*distance*] | スタティック ルートを確立します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show ip route** | 設定を確認するため、ルーティング テーブルを表示します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

スタティック ルートを削除するには、**no ip route** *prefix mask* {*address* | *interface*} グローバル コンフィギュレーション コマンドを使用します。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、アドミニストレーティブ ディスタンスの値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています（表 39-16 を参照）。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのアドミニストレーティブ ディスタンスよりも大きな値になるように設定します。

**表 39-16　ダイナミック ルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス**

| ルートの送信元 | デフォルト距離 |
|---|---|
| 接続されているインターフェイス | 0 |
| スタティック ルート | 1 |
| EIGRP サマリー ルート | 5 |
| EBGP | 20 |
| 内部 EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IBGP | 200 |
| 不明 | 225 |

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが、ルーティング テーブルで接続済みとして見なされた結果、静的な性質を失うた

めです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しないかぎり、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。ソフトウェアが、転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップをスタティック ルート内で検出できない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

# デフォルトのルートおよびネットワークの指定

ルータは、他のすべてのネットワークへのルートを学習できません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛てに指定します（スマート ルータには、インターネットワーク全体のルーティング テーブル情報が格納されます）。これらのデフォルト ルートは動的に取得されるか、ルータごとに設定されます。ほとんどのダイナミックな内部ルーティング プロトコルでは、スマート ルータはダイナミックなデフォルト情報を生成でき、生成された情報は他のルータに転送されます。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルト ルートを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ネットワークへのデフォルトのスタティック ルートを定義するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip default-network** *network number* | デフォルト ネットワークを指定します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show ip route** | 最終ゲートウェイの出力で選択されたデフォルト ルートを表示します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ルートを削除するには、**no ip default-network** *network number* グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、他に設定する必要はありません。ルーティング テーブルはシステムによって定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在することがあります。Cisco ルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、アドミニストレーティブ ディスタンスおよびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定できます。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

# ルート マップによるルーティング情報の再配信

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信できます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。**match** コマンドは、条件が一致する必要があることを指定しています。**set** コマンドは、ルーティング アップデートが match コマンドで定義した条件を満たす場合に行われる処理を指定します。再配信はプロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものです。

**route-map** コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合は、照合処理だけが行われます。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。

（注）　**set** ルート マップ コンフィギュレーション コマンドを使用しないルート マップは、CPU に送信されるので、CPU の使用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベース ルーティング）、ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set 句が適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

BGP ルート マップ **continue** 句を使用すると、match および set 句が正常に実行されてエントリが実行された後で、ルート マップの他のエントリを実行できます。**continue** 句を使用することで、よりモジュール化したポリシー定義の設定と編成を行うことができるため、同じルート マップ内で特定のポリシー設定が繰り返されなくなります。スイッチで発信ポリシーに **continue** コマンドを使用できるようになりました。ルート マップ **continue** 句の使用方法の詳細については、次の URL にある『BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOSRelease 12.4(4)T』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guides_list.html

（注）　次に示すステップ 3 ～ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

再配信用のルート マップを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **route-map** *map-tag* [**permit** \| **deny**] [*sequence number*] | 再配信を制御するために使用するルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。<br>*map-tag*：ルート マップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。<br>[**permit** \| **deny**]（任意）：**permit** が指定され、このルート マップの一致条件が満たされている場合は、set アクションによる制御に従ってルートが再配信されます。**deny** が指定されている場合、ルートは再配信されません。<br>*sequence number*（任意）：同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を定義する番号です。 |
| ステップ 3 | **match as-path** *path-list-number* | BGP 自律システム パス アクセス リストと一致させます。 |
| ステップ 4 | **match community-list** *community-list-number* [**exact**] | BGP コミュニティ リストと一致させます。 |
| ステップ 5 | **match ip address** {*access-list-number* \| *access-list-name*} [*...access-list-number* \| *...access-list-name*] | 名前または番号を指定し、標準アクセス リストと一致させます。1 ～ 199 の整数を指定できます。 |
| ステップ 6 | **match metric** *metric-value* | 指定されたルート メトリックと一致させます。*metric-value* には、0 ～ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。 |
| ステップ 7 | **match ip next-hop** {*access-list-number* \| *access-list-name*} [*...access-list-number* \| *...access-list-name*] | 指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。 |
| ステップ 8 | **match tag** *tag value* [*...tag-value*] | 1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ～ 4294967295 の整数を指定できます。 |
| ステップ 9 | **match interface** *type number* [*...type number*] | 指定されたインターフェイスの 1 つから、指定されたネクストホップへのルートと一致させます。 |
| ステップ 10 | **match ip route-source** {*access-list-number* \| *access-list-name*} [*...access-list-number* \| *...access-list-name*] | 指定されたアドバタイズ済みアクセス リストによって指定されるアドレスと一致させます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 11 | **match route-type** {**local** \| **internal** \| **external** [**type-1** \| **type-2**]} | 指定された**ルート タイプ**と一致させます。<br>• **local**：ローカルに生成された BGP ルート<br>• **internal**：OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート<br>• **external**：OSPF 外部ルート（タイプ 1 またはタイプ 2）または EIGRP 外部ルート |
| ステップ 12 | **set dampening** *halflife reuse suppress max-suppress-time* | BGP ルート ダンピング化係数を設定します。 |
| ステップ 13 | **set local-preference** *value* | ローカル BGP パスに値を割り当てます。 |
| ステップ 14 | **set origin** {**igp** \| **egp** *as* \| **incomplete**} | BGP の送信元コードを設定します。 |
| ステップ 15 | **set as-path** {**tag** \| **prepend** *as-path-string*} | BGP 自律システム パスを変更します。 |
| ステップ 16 | **set level** {**level-1** \| **level-2** \| **level-1-2** \| **stub-area** \| **backbone**} | ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。**stub-area** および **backbone** は、OSPF NSSA およびバックボーン エリアです。 |
| ステップ 17 | **set metric** *metric value* | 再配信されるルートに指定するメトリック値を設定します（EIGRP 専用）。*metric value* は -294967295 ～ 294967295 の整数です。 |
| ステップ 18 | **set metric** *bandwidth delay reliability loading mtu* | 再配信されるルートに指定するメトリック値を設定します（EIGRP 専用）。<br>• *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅（Kb/s 単位）<br>• *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。<br>• *reliability*：0 ～ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。<br>• *loading*：0 ～ 255 の数値で表されるルートの有効帯域幅（255 は 100% の負荷）。<br>• *mtu*：ルートの MTU の最小サイズ（バイト単位）。範囲は 0 ～ 4294967295 です。 |
| ステップ 19 | **set metric-type** {**type-1** \| **type-2**} | 再配信されるルートの OSPF 外部メトリック タイプを設定します。 |
| ステップ 20 | **set metric-type internal** | ネクスト ホップの IGP メトリックと一致するように、External BGP ネイバーにアドバタイズされるプレフィックスの Multi-Exit Discriminator（MED）値を設定します。 |
| ステップ 21 | **set weight** | ルーティング テーブルの BGP ウェイトを設定します。1 ～ 65535 の値を指定できます。 |
| ステップ 22 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 23 | **show route-map** | 設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |
| ステップ 24 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

エントリを削除するには、**no route-map** *map tag* グローバル コンフィギュレーション コマンド、または **no match** や **no set** ルート マップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを配信したり、ルート再配信を制御できます。

ルート再配信を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは前述の手順で定義されたキーワードと同じです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router** {**bgp** \| **rip** \| **ospf** \| **eigrp**} | ルータ コンフィギュレーション モードを開始します。<br>IP ベース フィーチャ セットを実行しているスイッチは、**rip** キーワードだけをサポートしています。 |
| ステップ 3 | **redistribute** *protocol* [*process-id*] {**level-1** \| **level-1-2** \| **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match internal** \| **external** *type-value*] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**] | ルーティング プロトコル間でルートを再配信します。ルート マップを指定しないと、すべてのルートが再配信されます。キーワード **route-map** に *map-tag* を指定しないと、ルートは配信されません。 |
| ステップ 4 | **default-metric** *number* | 現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します（BGP、RIP、OSPF）。 |
| ステップ 5 | **default-metric** *bandwidth delay reliability loading mtu* | EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show route-map** | 設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

再配信をディセーブルにするには、そのコマンドの **no** 形式を使用します。

ルーティング プロトコルのメトリックを、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは 5 つの特性の組み合わせです。このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。ルーティング情報を制御せずにさまざまなルーティング プロトコル間で交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することがあります。

- RIP はスタティック ルートを自動的に再配信できます。スタティック ルートにはメトリック 1（直接接続）が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

# ポリシーベース ルーティングの設定

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を低くします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、バッチ トラフィックではなく対話形式に基づくルーティング、または専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は広帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーション データは狭帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、アクセス コントロール リスト（ACL）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクストホップに転送（ルーティング）されます。

- パケットがルート マップ ステートメントと一致しない場合は、すべての set 句が適用されます。
- ステートメントが許可としてマークされている場合、どのルートマップ ステートメントとも一致しないパケットは通常の転送チャネルを通じて送信され、宛先ベースのルーティングが実行されます。
- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

ルート マップの設定の詳細については、「ルート マップによるルーティング情報の再配信」（P.39-102）を参照してください。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定できます。一致が見つかるまで、ルート マップにこのプロセスが行われます。一致が見つからない場合、通常の宛先ベース ルーティングが行われます。match ステートメント リストの末尾には、暗黙の拒否ステートメントがあります。

match 句を満たす場合は、set 句を使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。表示されているにもかかわらずスイッチでサポートされない PBR コマンドについては、付録 B「Cisco IOS Release 15.0(2)SE でサポートされていないコマンド」を参照してください。

PBR の設定はスタック全体に適用され、すべてのスイッチがスタック マスター設定を使用します。

（注）　このソフトウェア リリースは、IPv4 および IPv6 トラフィック処理時に PBR をサポートしません。

## PBR 設定時の注意事項

PBR の設定を開始する前に、次の点に注意してください。

- PBR を使用するには、スイッチまたはスタック マスターで IP サービス フィーチャ セットがイネーブルになっている必要があります。

- マルチキャスト トラフィックでは、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- PBR には、**route-map deny** ステートメントはサポートされません。
- レイヤ 3 モードの EtherChannel ポート チャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチまたはスイッチ スタックには最大 246 の IP ポリシー ルート マップを定義できます。
- スイッチまたはスイッチ スタックには、PBR 用として最大 512 のアクセス コントロール エントリ（ACE）を定義できます。
- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛てのパケットを許可する ACL と照合させないでください。PBR がこれらのパケットを転送するため、ping または Telnet の失敗やルート プロトコルのフラッピングを発生させる可能性があります。
  - 拒否 ACE を含む ACL と照合させないでください。拒否 ACE と一致するパケットが CPU に送られるため、CPU の利用率が高くなる可能性があります。
- PBR を使用するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用して、まずルーティング テンプレートをイネーブルにする必要があります。PBR は、VLAN とデフォルト テンプレートではサポートされません。SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」を参照してください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、PBR をイネーブルにはできません。
- WCCP と PBR は、スイッチ インターフェイスで相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、WCCP をイネーブルにできません。逆も同様です。インターフェイスで WCCP がイネーブルになっている場合は PBR をイネーブルにできません。
- PBR で使用されるハードウェア エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- パケット長、Type of Service（ToS; サービス タイプ）、set interface、set default next hop、または set default interface に基づポリシーベース ルーティングは、サポートされていません。有効な set アクションがないか、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされていません。
- スイッチは PBR ルート マップの QoS DSCP および IP precedence マッチングをサポートしますが、次の制約があります。
  - DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用できません。
  - DSCP 透過性と PBR DSCP ルート マップを同じスイッチ上に設定できません。
  - QoS DSCP を使用して PBR を設定する場合は、（**mls qos** グローバル コンフィギュレーション コマンドを入力して）QoS をイネーブルに設定するか、（**no mls qos** コマンドを入力して）ディセーブルに設定できます。QoS がイネーブルになっている場合に、トラフィックの DSCP 値が変更されないようにするには、**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを入力して、トラフィックがスイッチを実行するポートで DSCP 信頼状態を設定する必要があります。信頼状態が DSCP ではない場合は、デフォルトでは信頼されていないすべてのトラフィックで DSCP 値が 0 としてマークされます。

## PBR のイネーブル化

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準およびすべての match 句と一致した場合の動作を指定するルート マップを作成する必要があります。次に、そのルート マップのインターフェイスで PBR をイネーブルにする必要があります。そのインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

PBR は、スイッチの速度低下を引き起こさない速度で、高速転送したり実装したりできます。高速スイッチングされた PBR では、ほとんどの match および set コマンドを使用できます。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。PBR の高速スイッチングは、デフォルトでディセーブルになっています。

スイッチで生成されたパケットまたはローカル パケットは、通常はポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。ローカル PBR は、デフォルトでディセーブルに設定されています。

**（注）** PBR をイネーブルにするには、スイッチまたはスタック マスター上で IP サービス フィーチャ セットが稼働している必要があります。

PBR を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **route-map** *map-tag* [**permit**] [*sequence number*] | パケットの送信場所を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。<br>• *map-tag*：ルート マップ用のわかりやすい名前を指定します。**ip policy route-map** インターフェイス コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。<br>• （任意）**permit** が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。<br>**（注）** **route-map deny** ステートメントは、インターフェイスに適用する PBR ルート マップではサポートされません。<br>• *sequence number*（任意）：同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を示す番号です。 |
| ステップ 3 | **match ip address** {*access-list-number* \| *access-list-name*} [*...access-list-number* \| *...access-list-name*] | 1 つ以上の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。<br>**（注）** 拒否 ACE を含む ACL またはローカル アドレス宛てのパケットを許可する ACL は入力しないでください。<br>**match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **set ip next-hop** *ip-address* [*...ip-address*] | 基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します（ネクスト ホップは隣接していなければなりません）。 |
| ステップ 5 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 6 | **interface** *interface-id* | インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。 |
| ステップ 7 | **ip policy route-map** *map-tag* | レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを識別します。1 つのインターフェイスに設定できるルート マップは、1 つだけです。ただし、異なるシーケンス番号を持つ複数のルート マップ エントリを設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。<br>**（注）** IP ポリシー ルート マップに **deny** ステートメントが含まれていると、その設定は失敗します。 |
| ステップ 8 | **ip route-cache policy** | （任意）PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。 |
| ステップ 9 | **exit** | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 10 | **ip local policy route-map** *map-tag* | （任意）スイッチから送信されるパケットにポリシーベース ルーティングを行うために、ローカル PBR をイネーブルにします。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show route-map** [*map-name*] | （任意）設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |
| ステップ 13 | **show ip policy** | （任意）インターフェイスに付加されたポリシー ルート マップを表示します。 |
| ステップ 14 | **show ip local policy** | （任意）ローカル PBR がイネーブルであるかどうか、およびイネーブルである場合は使用されているルート マップを表示します。 |
| ステップ 15 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

エントリを削除するには、**no route-map** *map-tag* グローバル コンフィギュレーション コマンド、または **no match** または **no set** ルート マップ コンフィギュレーション コマンドを使用します。インターフェイス上で PBR をディセーブルにするには、**no ip policy route-map** *map-tag* インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されるパケットに対して PBR をディセーブルにするには、**ip local policy route-map** *map-tag* グローバル コンフィギュレーション コマンドを使用します。

# ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、以下の作業を実行します。

（注）　OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

## 受動インターフェイスの設定

ローカル ネットワーク上の他のルータがダイナミックにルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用します。これによって、ルーティング アップデート メッセージがルータ インターフェイスから送信されなくなります。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、そのインターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークでは、手動でパッシブに設定する必要はありません。**passive-interface default** ルータ コンフィギュレーション コマンドを使用して、すべてのインターフェイスをデフォルトでパッシブに設定できます。その後、隣接関係が必要なインターフェイスを手動で設定できます。

受動インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router** {**bgp** \| **rip** \| **ospf** \| **eigrp**} | ルータ コンフィギュレーション モードを開始します。<br>IP ベース フィーチャ セットを実行しているスイッチは、**rip** キーワードだけをサポートしています。 |
| ステップ 3 | **passive-interface** *interface-id* | 指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。 |
| ステップ 4 | **passive-interface default** | （任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。 |
| ステップ 5 | **no passive-interface** *interface type* | （任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。 |
| ステップ 6 | **network** *network-address* | （任意）ルーティング プロセス用のネットワーク リストを指定します。*network-address* は IP アドレスです。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク監視用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

ルーティング アップデートの送信を再度イネーブルにするには、**no passive-interface** *interface-id* ルータ コンフィギュレーション コマンドを使用します。**default** キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。次に、**no passive-interface** ルータ コンフィギュレーション コマンドを使用し、隣接関係を必要とする各インターフェイスを個別に設定します。**default** キーワードは、ほとんどの配信ルータに 200 を超えるインターフェイスが備わっているインターネット サービス プロバイダーや大規模な企業ネットワークの場合に役立ちます。

## ルーティング アップデートのアドバタイズおよび処理の制御

ACL と **distribute-list** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを取得しないようにできます。この機能は、OSPF で使用した場合は外部ルートだけに適用されるため、インターフェイス名を指定できません。

**distribute-list** ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます （OSPF にこの機能は適用されません）。

ルーティング アップデートのアドバタイズまたは処理を制御するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router** {**bgp** \| **rip** \| **ospf** \| **eigrp**} | ルータ コンフィギュレーション モードを開始します。<br>IP ベース フィーチャ セットを実行しているスイッチは、**rip** キーワードだけをサポートしています。 |
| ステップ 3 | **distribute-list** {*access-list-number* \| *access-list-name*} **out** [*interface-name* \| *routing process* \| *autonomous-system-number*] | アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズを許可または拒否します。 |
| ステップ 4 | **distribute-list** {*access-list-number* \| *access-list-name*} **in** [*type-number*] | アップデートにリストされたルートの処理を抑制します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

フィルタを変更またはキャンセルするには、**no distribute-list in** ルータ コンフィギュレーション コマンドを使用します。アップデート中のネットワーク アドバタイズメントの抑制をキャンセルするには、**no distribute-list out** ルータ コンフィギュレーション コマンドを使用します。

## ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「*アドミニストレーティブ ディスタンス*」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティング プロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。アドミニストレーティブ ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルのアドミニストレーティブ ディスタンスが最短（値が最小）であるルートが選択されます。表 39-16（P.39-100）に、さまざまなルーティング情報送信元のデフォルトのアドミニストレーティブ ディスタンスを示します。

各ネットワークには独自の要件があるため、アドミニストレーティブ ディスタンスを割り当てる一般的な注意事項はありません。

ルーティング情報の送信元をフィルタリングするには、特権 EXEC モードで、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **router** {**bgp** \| **rip** \| **ospf** \| **eigrp**} | ルータ コンフィギュレーション モードを開始します。<br>IP ベース フィーチャ セットを実行しているスイッチは、**rip** キーワードだけをサポートしています。 |
| ステップ 3 | **distance** *weight* {*ip-address* {*ip-address mask*}} [*ip access list*] | アドミニストレーティブ ディスタンスを定義します。<br>*weight* : アドミニストレーティブ ディスタンスは 10 ～ 255 の整数です。単独で使用した場合、*weight* はデフォルトのアドミニストレーティブ ディスタンスを指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。<br>（任意）*ip access list* : 着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip protocols** | 指定されたルーティング プロセス用のデフォルトのアドミニストレーティブ ディスタンスを表示します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

アドミニストレーティブ ディスタンスを削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

# 認証キーの管理

キー管理を使用すると、ルーティング プロトコルで使用される認証キーを制御できます。一部のプロトコルでは、キー管理を使用できません。認証キーは EIGRP および RIP バージョン 2 で使用できます。

認証キーを管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証キーを管理するには、キー チェーンを定義してそのキー チェーンに属するキーを識別し、各キーの有効期間を指定します。各キーには、ローカルにストアされる独自のキー ID（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。

有効期間が指定された複数のキーを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは 1 つだけです。キー番号は小さい方から大きい方へソフトウェアによって順に調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

認証キーを管理するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **key chain** *name-of-chain* | キー チェーンを識別し、キーチェーン 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 | **key** *number* | キー番号を識別します。指定できる範囲は 0 ～ 2147483647 です。 |
| ステップ 4 | **key-string** *text* | キー ストリングを識別します。ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。 |
| ステップ 5 | **accept-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*} | （任意）キーを受信する期間を指定します。<br>*start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は **infinite** です。 |
| ステップ 6 | **send-lifetime** *start-time* {**infinite** \| *end-time* \| **duration** *seconds*} | （任意）キーを送信する期間を指定します。<br>*start-time* および *end-time* 構文には、*hh*:*mm*:*ss Month date year* または *hh*:*mm*:*ss date Month year* のいずれかを使用できます。デフォルトは、デフォルトの *start-time* 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの *end-time* および **duration** は infinite です。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show key chain** | 認証キー情報を表示します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

キー チェーンを削除するには、**no key chain** *name-of-chain* グローバル コンフィギュレーション コマンドを使用します。

# IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを削除したり、ステータスを表示するには、表 39-17 に示す特権 EXEC コマンドを使用します。

**表 39-17　IP ルートの削除またはルート ステータスの表示を行うコマンド**

| コマンド | 目的 |
|---|---|
| **clear ip route** {*network* [*mask* \| *]} | IP ルーティング テーブルから 1 つまたは複数のルートを削除します。 |
| **show ip protocols** | アクティブなルーティング プロトコル プロセスのパラメータおよびステートを表示します。 |
| **show ip route** [*address* [*mask*] [**longer-prefixes**]] \| [*protocol* [*process-id*]] | ルーティング テーブルのステートを表示します。 |
| **show ip route summary** | ルーティング テーブルのステートをサマリー形式で表示します。 |
| **show ip route supernets-only** | スーパーネットを表示します。 |
| **show ip cache** | IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。 |
| **show route-map** [*map-name*] | 設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。 |