CHAPTER 41

IP ユニキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP バージョン 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。ルーティングをイネーブルにするには、スイッチが IP サービス イメージを実行している必要があります。

（注） スイッチが IP サービス イメージを実行している場合、IP バージョン 6（IPv6）ユニキャスト ルーティングもイネーブルにして、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にインターフェイスを設定できます。スイッチの IPv6 の設定の詳細については、第 42 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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] で、次のコマンド リファレンスを参照してください。

- 『*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。

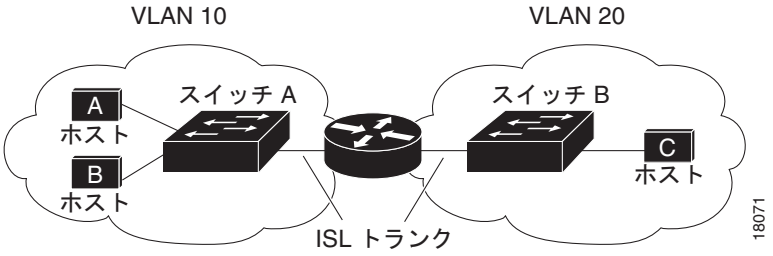
（注）　スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用すると、Switch Database Management（SDM）機能をルーティング テンプレートに設定できます。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」またはこのリリースのコマンド リファレンスで **sdm prefer** コマンドを参照してください。

IP ルーティングの概要

一部のネットワーク環境では、VLAN は個別の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 ネットワークでは、各サブネットワークは個々の VLAN にマッピングされます。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のまま維持できます。ただし、異なる VLAN でのネットワーク装置が相互に通信するには、VLAN 間のトラフィックをルーティング（VLAN 間ルーティング）するためにレイヤ 3 装置（ルータ）を使用する必要があります。トラフィックを該当する宛先 VLAN にルーティングするように、1 つまたは複数のルータを設定します。

図 41-1 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 内に、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 41-1　　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 と通信する必要がある場合、ホスト A はホスト B を宛先とする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に、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 テーブルをチェックし、適切な発信インターフェイスを検索し、VLAN 20 インターフェイスのパケットをスイッチ B に転送します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティングのタイプ

ルータおよびレイヤ 3 スイッチは、次の 3 つ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
- 事前にプログラムされているトラフィックのスタティック ルート
- ルーティング プロトコルによるルートのダイナミックな計算

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 ルーティングでは、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および外部に転送されます。スタティック ルーティングは、安全であり、帯域幅もほとんど使用しませんが、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ないため、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。

ルータでは、トラフィックを転送する最適ルートをダイナミックに計算するために、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには、次の 2 種類があります。

- 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 テーブルを維持し、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、最適ルートを計算します。これらのプロトコルは簡単に設定および使用できます。
- 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）の交換に基づいて、ネットワーク トポロジの複雑なデータベースを維持します。LSA はネットワークのイベントがきっかけで発生し、コンバージェンスに要する時間やこれらの変更への対応に必要な時間を短縮します。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とリソースが必要になります。

スイッチでサポートされるディスタンスベクトル プロトコルは、Routing Information Protocol（RIP）と Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）です。RIP は単一の距離メトリック（コスト）を使用して最適なパスを決定し、BGP はパス ベクトル 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拡張 IGRP（EIGRP）もサポートされます。

ルーティングを設定する手順

デフォルトでは、スイッチ上で IP ルーティングがディセーブルになっています。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 ルーティングの設定情報の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。

次の手順では、次のいずれかのレイヤ 3 インターフェイス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 コマンドを使用して、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 コマンドを使用して作成された VLAN インターフェイスです。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です。詳細については、「レイヤ 3 EtherChannel の設定」（P.40-14）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.41-5）を参照してください。

（注）　レイヤ 3 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。ユーザが設定可能なルーテッド ポートおよび SVI の数は、ソフトウェアによって制限されません。ただし、ハードウェアの制限により、この数と、実装された機能の組み合わせとの関係が、CPU 使用率に影響を与える可能性があります。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には、スイッチで 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 16 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 アドレッシングの設定

IP ルーティングを設定するには、レイヤ 3 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 アドレッシング機能の設定手順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。

アドレッシングのデフォルト設定

表 41-1 に、アドレッシングのデフォルト設定を示します。

表 41-1　アドレッシングのデフォルト設定

機能	デフォルト設定
IP アドレス	定義なし。
ARP（アドレス解決プロトコル）	Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュに相手先固定エントリはありません。 カプセル化：標準のイーサネット形式の ARP。 タイムアウト：14400 秒（4 時間）。

表 41-1　アドレッシングのデフォルト設定 （続き）

機能	デフォルト設定
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 ブロードキャストは廃棄されます)。
IP ドメイン	ドメイン リスト：ドメイン名は定義されていません。 ドメイン検索：イネーブル。 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、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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 転送がイネーブルになります。 ローカル ブロードキャスト：ディセーブル Spanning Tree Protocol（STP; スパニング ツリー プロトコル）：ディセーブル 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。
IRDP	ディセーブル。 イネーブルの場合のデフォルト： • ブロードキャスト IRDP アドバタイズ • アドバタイズ間の最大インターバル：600 秒 • アドバタイズ間の最小インターバル：最大インターバルの 0.75 倍 • 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、特殊な用途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、IP アドレスに関する公式な説明が掲載されています。

インターフェイスには、1 つのプライマリ IP アドレスを指定できます。マスクは、IP アドレスのネットワーク番号を表すビットを特定します。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）。
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*] **show ip interface** [*interface-id*] **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）設定をコンフィギュレーション ファイルに保存します。

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）を使用できます。また、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、推奨しません）。

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 アップデートにサブネット 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）設定をコンフィギュレーション ファイルに保存します。

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

デフォルトでは、ルーティングするように設定されたスイッチで、クラスレス ルーティング動作は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 スペースをシミュレートするために使用されるクラス C アドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するように設計されています。

図 41-2 では、クラスレス ルーティングがイネーブルになっています。ホストがパケットを 128.20.4.1 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ルータが受信すると、ルータはパケットを廃棄します。

図 41-2　IP クラスレス ルーティングがイネーブルの場合

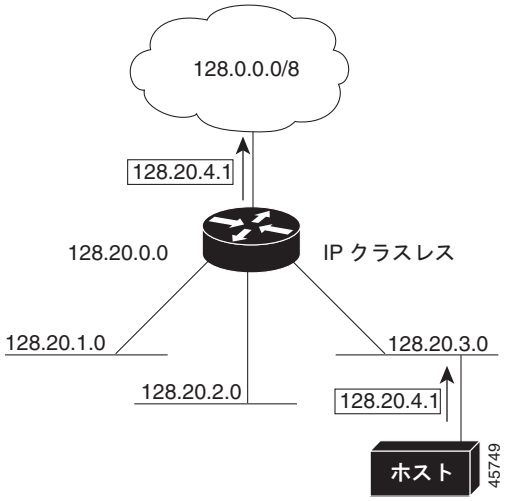
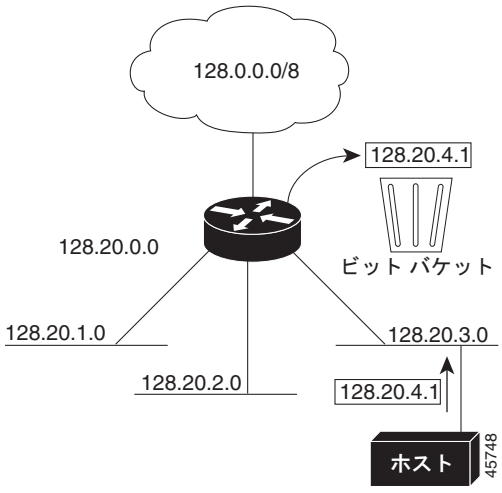


図 41-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、および 128.20.3.0 に接続されています。ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 41-3　IP クラスレス ルーティングがディセーブルの場合



認識不能な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。
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）設定をコンフィギュレーション ファイルに保存します。

デフォルトに戻して、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のパケットが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、アドレス解決を使用します。IP を使用する装置は、ローカル セグメントまたは LAN 上の装置を一意に定義するローカル アドレス（MAC アドレス）と、装置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。

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て、データ リンク（レイヤ 2）装置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。ソフトウェアがイーサネット上の装置と通信するために、装置の MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを判別するプロセスを、*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は、*逆アドレス解決*と呼ばれます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- 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るために使用されます。ARP は IP アドレスを入力と解釈し、関連付けられた MAC アドレスを学習します。次に、IP アドレスと MAC アドレスの関連付けを ARP キャッシュに保存され、すぐに取得できます。次に、IP データグラムがリンクレイヤ フレームにカプセル化され、ネットワーク上で送信されます。イーサネット以外の IEEE 802 ネットワークでの IP データグラムまたは ARP 要求および応答のカプセル化は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）で指定されます。
- プロキシ ARP は、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 と同様の機能である Reverse Address Resolution Protocol（RARP; 逆アドレス解決プロトコル）も使用できます（RARP パケットがローカル MAC アドレスでなく IP アドレスを要求する点を除く）。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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*』を参照してください。

アドレス解決を設定するには、次の作業を実行します。

- 「スタティック ARP キャッシュの定義」（P.41-9）
- 「ARP カプセル化の設定」（P.41-10）
- 「プロキシ ARP のイネーブル化」（P.41-10）

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、通常はスタティック 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相手先固定エントリを、ARP キャッシュに確保できます。任意で、指定の 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 エントリを相手先固定エントリにしない場合は、ARP エントリのタイムアウト時間を指定できます。

IP アドレスと MAC アドレス間をスタティックにマッピングするには、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	**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。 • **arpa**：ARP カプセル化（イーサネット インターフェイス用） • **snap**：Subnetwork Address Protocol カプセル化（トークン リングおよび Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）用） • **sap**：HP の ARP タイプ
ステップ 3	**arp** *ip-address hardware-address type* [*alias*]	（任意）指定の 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時間を設定します。デフォルト値は 14400 秒（4 時間）です。指定できる範囲は 0 ～ 2147483 秒です。
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** または **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）設定をコンフィギュレーション ファイルに保存します。

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 キャッシュからすべての非スタティック エントリを削除するには、**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

デフォルトでは、IP インターフェイスでイーサネット ARP 形式の ARP カプセル化（**arpa** キーワードで表される）はイネーブルになっています。ネットワークの必要性に応じて、カプセル化方式を 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 カプセル化方式を指定します。 • **arpa**：アドレス解決プロトコル • **snap**：Subnetwork Address Protocol
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）設定をコンフィギュレーション ファイルに保存します。

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、スイッチはプロキシ ARP を使用します。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。

ディセーブル化されているプロキシ 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*]	特定の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）設定をコンフィギュレーション ファイルに保存します。

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.41-11）
- 「デフォルト ゲートウェイ」（P.41-11）
- 「ICMP Router Discovery Protocol（IRDP）」（P.41-12）

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しています。スイッチが送信元と異なるネットワーク上のホストに宛てた ARP 要求を受信した場合、そのホストへの最適ルートがあるかどうかを調べます。最適ルートがある場合、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 要求を実行します。

プロキシ ARP はデフォルトでイネーブルになっています。プロキシ ARP をディセーブルにしたあとにイネーブルにするには、「プロキシ ARP のイネーブル化」（P.41-10）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限り有効です。

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、または Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）リダイレクト メッセージを返信するという方法で、ホストが使用するローカル ルータを定義します。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。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

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）設定をコンフィギュレーション ファイルに保存します。

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。

ICMP Router Discovery Protocol（IRDP）

ルータ検出を使用すると、スイッチは IRDP を使用し、他のネットワークへのルートをダイナミックに学習します。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、ルータ検出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、ルータ検出パケットを受信します。スイッチは RIP ルーティングのアップデートを受信し、この情報からルータの場所を推測することもできます。実際には、ルーティング装置によって送信されたルーティング テーブルは、スイッチに格納されません。どのシステムがデータを送信しているのかが追跡されるだけです。IRDP を使用することの利点は、プライオリティと、パケットが受信されなくなってから装置がダウンしていると見なされるまでの時間を、ルータごとに両方指定できることです。

検出された各装置は、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 Transmission Control Protocol（TCP; 伝送制御プロトコル）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。必要に応じて、これらのパラメータを変更できます。

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、IRDP アドバタイズをマルチキャスト アドレス（224.0.0.1）に送信します。 **（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 との互換性が維持できます。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。

	コマンド	目的
ステップ 8	**ip irdp preference** *number*	（任意）装置にプリファレンス レベルを設定します。指定できる範囲は –2^{31} ～ 2^{31} です。デフォルト値は 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。
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）設定をコンフィギュレーション ファイルに保存します。

maxadvertinterval 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **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 パケットの処理の設定

IP インターフェイス アドレスを設定したあとに、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。スイッチは次の 2 種類のブロードキャストをサポートします。

- ダイレクト ブロードキャスト パケット。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ます。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。
- フラッディング ブロードキャスト パケット。すべてのネットワークに送信されます。

（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、およびマルチキャスト 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 29 章「ポートベース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 装置であるため、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 ストームが伝播します。ブロードキャスト ストームの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。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。スイッチ内の機能をはじめ、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ッシング方式が複数サポートされています。

ここでは、これらの方式をイネーブルにするために行う作業について説明します。

- 「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.41-14）
- 「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.41-15）
- 「IP ブロードキャスト アドレスの確立」（P.41-16）
- 「IP ブロードキャストのフラッディング」（P.41-16）

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 ブロードキャストは廃棄されるため、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廃棄されると、ルータが DoS 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インターフェイスでは、IP ダイレクト 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 コマンドを使用して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 リストを指定できます。アクセス リストを指定すると、アクセス リストで許可された IP パケットだけをダイレクト ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、第 38 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アクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可された IP パケットだけを変換できます。 **（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 Virtual Private Network（VPN; 仮想私設網）Routing/Forwarding（VRF; VPN ルーティング/転送）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 内だけで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、ルータによって転送されるプロトコルとポートを指定します。 • **udp**：User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データグラムを転送します。 *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。 • **nd**：Network Disk（ND）データグラムを転送します。 • **sdns**：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*] または **show running-config**	特定の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）設定をコンフィギュレーション ファイルに保存します。

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、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレス型セッションを 2 つのエンド システム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、および名前に関する情報を判別します。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、通常 UDP ブロードキャストは転送されません。このような状況を修復するには、特定のクラスのブロードキャストをヘルパー 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します。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て、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（ND）プロトコルも指定できます。

デフォルトでは、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、UDP と ND 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*』に記載されている **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のデフォルトで転送されるポートの一覧があります。

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 Bootstrap Protocol（BOOTP）転送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）情報を伝送します。

インターフェイス上で 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*] または **show running-config**	特定の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）設定をコンフィギュレーション ファイルに保存します。

特定の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

最も一般的な（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*	デフォルト値とは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*]	特定の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）設定をコンフィギュレーション ファイルに保存します。

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式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、ループも防止できます。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ルータで送信する場合、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、パケットは次の基準を満たす必要があります（これらの基準は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベル ブロードキャストである必要があります。
- パケットは IP レベル ブロードキャストである必要があります。
- パケットは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、Domain Name System（DNS; ドメイン ネーム システム）、Time、Network Basic Input/Output System（NetBIOS）、ND、または BOOTP パケットであるか、**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 である必要があります。

- パケットの Time To Live（TTL; 存続可能時間）値が 2 以上である必要があります。

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。宛先アドレスは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を介して伝播するにつれ、宛先アドレスが変更される場合があります。送信元アドレスは変更されません。TTL 値は減少します。

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から送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、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て 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て 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）設定をコンフィギュレーション ファイルに保存します。

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ます。

スパニング ツリーベースのフラッディングを向上させるには、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て 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）設定をコンフィギュレーション ファイルに保存します。

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 アドレッシングのモニタ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る場合、または無効である疑いがある場合は、**clear** 特権 EXEC コマンドを使用してすべての内容を削除できます。表 41-2 に、内容を消去するコマンドを示します。

表 41-2　キャッシュ、テーブル、データベースの消去を行うコマンド

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 キャッシュを消去します。
clear host {*name* | *}}	ホスト名およびアドレス キャッシュから特定のエントリ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、パケットがネットワーク上で通過するルーティング パスなど、特定の統計情報を表示できます。表 41-3 に、IP 統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 41-3　キャッシュ、テーブル、データベースの表示を行うコマンド

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、およびキャッシュされた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

デフォルトでは、スイッチはレイヤ 2 スイッチング モード、IP ルーティングがディセーブルになっています。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*	**（注）** 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（ルーティングするネットワークを指定する **network**（RIP）ルータ コンフィギュレーション コマンドなど）を使用する場合があります。特定の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。
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）設定をコンフィギュレーション ファイルに保存します。

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
```

次の項で説明するように、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。

- 「RIP の設定」（P.41-19）
- 「OSPF の設定」（P.41-25）
- 「EIGRP の設定」（P.41-34）
- 「BGP の設定」（P.41-42）
- 「プロトコル独立機能の設定」（P.41-89）（任意）

RIP の設定

Routing Information Protocol（RIP）は、小規模な同種ネットワークで使用するために作成された Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）です。RIP は、ブロードキャスト User Datagram Protocol（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。このプロトコルについては、RFC 1058 で説明されています。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

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）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キングされます。240 秒が経過してもアップデートが届かない場合、アップデートを行わない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の数です。直接接続された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することはできません。このように範囲（0 ～ 15）が狭いため、RIP は大規模な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装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 によって学習された場合、またはルータがラスト リゾート 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、次の設定情報について説明します。

RIP のデフォルト設定

表 41-4 に、RIP のデフォルト設定を示します。

表 41-4　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。 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 のトリガー	**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	定義なし。
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	• update：30 秒。 • invalid：180 秒。 • holdown：180 秒。 • flush：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 のパケットを受信し、バージョン 1 のパケットを送信。

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。IE 3000 スイッチでは、ネットワーク番号を設定するまで RIP コンフィギュレーション コマンドは無視されます。

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）。
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。 **（注）** RIP コマンドを有効にするには、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ネイバー 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て、RIP によって学習したルートへの着信および発信メトリックを増加させます。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。 • *update*：ルーティング アップデートの送信間隔。デフォルト値は 30 秒です。 • *invalid*：ルートが無効と宣言されたあとの時間。デフォルト値は 180 秒です。 • *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。 • *flush*：ルーティング アップデートが延期される時間。デフォルト値は 240 秒です。
ステップ 8	**version** {**1** | **2**}	（任意）RIP バージョン 1 または 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 およびバージョン 2 を受信しますが、送信するのはバージョン 1 だけです。 インターフェイス コマンド **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} を使用して、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て（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、スイッチは着信 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、送信元 IP アドレスが有効でない場合はアップデートを廃棄します。通常の環境では、この機能をディセーブルにすることは推奨しません。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）送信される RIP アップデートのインターパケット遅延を追加します。 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、インターパケット遅延を追加することはできません。パケットを低速な装置に送信する場合は、8 ～ 50 ミリ秒のインターパケット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）設定をコンフィギュレーション ファイルに保存します。

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および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 は認証をサポートしません。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の 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。このため、「認証キーの管理」（P.41-104）に記載されている作業も実行してください。

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 2 つの認証モードがスイッチでサポートされます。デフォルトはプレーン テキストです。

インターフェイス上で 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）設定をコンフィギュレーション ファイルに保存します。

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がその情報の送信元のインターフェイスで、ルータによって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、スプリット ホライズンをディセーブルにすることがアプリケーションに必要である場合を除き、一般的にこの機能をディセーブルにすることは推奨しません。

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。

（注） スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリーはともにアドバタイズされません。

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、インターフェイスでスプリット 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。

	コマンド	目的
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）設定をコンフィギュレーション ファイルに保存します。

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 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。この例で、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の場合、（**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 gigabitethernet1/2
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がその情報の送信元のインターフェイスで、ルータによって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を最適化できます（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、スプリット ホライズンをディセーブルにすることがアプリケーションに必要である場合を除き、一般的にこの機能をディセーブルにすることは推奨しません。

インターフェイス上でスプリット 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。

	コマンド	目的
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*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、Open Shortest Path First（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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「OSPF Commands」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、非ブロードキャスト、ポイントツーポイント ネットワークに分類されます。スイッチはブロードキャスト（イーサネット、トークン リング、FDDI）と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）をサポートします。

OSPF は、IP ネットワーク専用の内部ゲートウェイ プロトコル（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。シスコ実装は RFC 1253 の OSPF Management Information Base（MIB; 管理情報ベース）をサポートします。

シスコ実装は、次の主な機能を含む 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ます。
- 任意の IP ルーティング プロトコルによって学習されたルートは、別の IP ルーティング プロトコルに再配信できます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって学習されたルートをインポートできます。OSPF ルートを RIP にエクスポートすることもできます。
- エリア内のネイバー 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、再送信間隔、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 dead と hello 間隔、認証キーなどがあります。
- 仮想リンクがサポートされます。
- RFC 1587 に基づく Not-So-Stubby-Area（NSSA）がサポートされます。

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。最小限の設定では、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。使用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、次の設定情報について説明します。

- 「OSPF のデフォルト設定」（P.41-26）
- 「基本的な OSPF パラメータの設定」（P.41-27）

OSPF のデフォルト設定

表 41-5 に、OSPF のデフォルト設定を示します。

表 41-5　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。 再送信間隔：5 秒。 送信遅延：1 秒。 プライオリティ：1。 hello 間隔：10 秒。 dead 間隔：hello 間隔の 4 倍。 認証なし。 パスワードの指定なし。 MD5 認証はディセーブル。
エリア	認証タイプ：0（認証なし）。 デフォルト コスト：1。 範囲：ディセーブル。 スタブ：スタブ エリアは未定義。 NSSA：NSSA エリアは未定義。
自動コスト	100 Mbps。
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、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。 dist2（エリア間のすべてのルート）：110。 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。すべての発信リンクステート アドバタイズ（LSA）がインターフェイスにフラッディングされます。
IP OSPF 名前検索	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。

表 41-5　OSPF のデフォルト設定 （続き）

機能	デフォルト設定
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 が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 ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
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 ペーシング	240 秒。
タイマー Shortest Path First（SPF）	spf-delay：5 秒。 spf-holdtime：10 秒。
仮想リンク	エリア ID または ルータ ID は未定義。 hello 間隔：10 秒。 再送信間隔：5 秒。 送信遅延：1 秒。 dead 間隔：40 秒。 認証キー：キーは未定義。 メッセージダイジェスト キー（MD5）：キーは未定義。

1. NSF = ノンストップ フォワーディング

OSPF NSF 認識

IP サービス イメージは IPv4 の OSPF NSF 認識をサポートします。ネイバー ルータが NSF 対応である場合、レイヤ 3 スイッチでは、プライマリ Route Processor（RP; ルート プロセッサ）に障害が発生してルータのバックアップ RP によって処理が引き継がれる前、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 RP を手動でリロードしている間、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はできません。この機能の詳細については、次の URL の『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a0080153edd.shtml

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。

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、内部的に使用されている識別パラメータで、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	**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。1 つのコマンドにワイルドカード マスクを指定して、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進値または IP アドレスを指定できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、プロセス番号 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 間隔、dead 間隔、認証キー）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間で一貫している必要があります。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。

（注）　**ip ospf** インターフェイス コンフィギュレーション コマンドはすべて任意です。

OSPF インターフェイス パラメータを変更するには、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	**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明示的に指定します。
ステップ 4	**ip ospf retransmit-interval** *seconds*	（任意）リンクステート アドバタイズの送信間隔の秒数を指定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。

	コマンド	目的
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の秒数を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 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 指定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。指定できる範囲は 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の秒数を設定します。値はネットワークのすべてのノードで同じである必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
ステップ 8	**ip ospf dead-interval** *seconds*	（任意）最後の装置で 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の秒数を設定します。値はネットワークのすべてのノードで同じである必要があります。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は hello 間隔の 4 倍です。
ステップ 9	**ip ospf authentication-key** *key*	（任意）ネイバー 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ネイバー 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）MD5 認証をイネーブルにします。 • *keyid*：1 ～ 255 の ID • *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ブロックします。デフォルトでは、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 OSPF は新しい 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。
ステップ 13	**show ip ospf interface** [*interface-name*]	OSPF 関連の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 認識ステータスを表示します。出力は、次のいずれかに一致します。 • *Options is 0x52* *LLS Options is 0x1 (LR)* これらの両方の行が表示される場合、ネイバー スイッチが NSF 認識です。 • *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）設定をコンフィギュレーション ファイルに保存します。

設定されたパラメータ値を削除するか、またはデフォルト値に戻すには、これらのコマンドの **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 Not-So-Stubby-Area（NSSA）への不正アクセスをパスワードに基づい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。代わりに、Autonomous System（AS; 自律システム）外の宛先に対するデフォルトの外部ルートが、エリア境界ルータ（ABR）によってスタブ エリアに生成されます。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 AS 外部ルートをインポートできます。

ルート サマライズとは、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 コマンドを使用して、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）特定のエリアへの不正アクセスのパスワードに基づいた阻止を可能にします。ID には 10 進値または 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）エリアで 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 アドバタイズをスタブ エリアに送信できなくなります。
ステップ 6	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**no-summary**]	（任意）エリアを Not-So-Stubby-Area 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。次のいずれかのキーワードを選択します。 • **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 ではなく通常のエリアにインポートする場合に選択します。 • **default-information-originate** : タイプ 7 LSA を NSSA にインポートする場合に、ABR で選択します。 • **no-summary** : 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、エリア境界ルータ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。

	コマンド	目的
ステップ 9	**show ip ospf** [*process-id*]	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て、設定を確認します。
	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）設定をコンフィギュレーション ファイルに保存します。

設定されたパラメータ値を削除するか、またはデフォルト値に戻すには、これらのコマンドの **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.41-94）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 コマンドを使用して、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的である場合に仮想リンクを確立するには、2 つのエリア境界ルータ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 エリアから設定することはできません。
- 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の再配信を設定すると、ルートは自動的に自律システム境界ルータ（ASBR）になります。ASBR を設定し、強制的に OSPF ルーティング ドメイン内にデフォルト 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 Domain Name Server（DNS; ドメイン ネーム サーバ）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、ルータを簡単に識別できます。
- 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。高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てこれらのリンクのコストを区別できます。
- 管理ディスタンスは、ルーティング情報の送信元の信頼性を示す値です。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。管理ディスタンスが 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（エリア間）、別のエリアへのルート（エリア間）、および再配信によって学習された別のルーティング ドメインからのルート（外部）の 3 つの管理ディスタンスが使用されます。どの管理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 つの装置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 が送信元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、送信元の装置を受動インターフェイスに設定する必要があります。両方の装置は、受信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 がトポロジの変更を受信してから Shortest Path First（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.41-28）、仮想リンクのデフォルト設定については表 41-5（P.41-26）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 ドメイン内にデフォルト 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 名前検索を設定します。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、エリア境界ルータ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 のディスタンスの値を変更します。各タイプのルートのデフォルトのディスタンスは 110 です。指定できる範囲は 1 ～ 255 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。
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。 • *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。 • *spf-holdtime*：最初と 2 番めの SPF 計算間の遅延。指定できる範囲は 1 ～ 600000 ミリ秒です。 • *spf-wait*：SPF 計算の最大待機時間（ミリ秒単位）。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に 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」（P.41-34）を参照してください。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、およびエージング機能をペーシングして、ルータをより効率的に使用することが可能になります。この機能はデフォルトでイネーブルになっています。デフォルトのペーシング間隔は 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 ペーシング間隔は、ルータがリフレッシュ、チェックサム、およびエージングを行う LSA 数に反比例します。たとえば、データベースに約 10,000 個の LSA が格納されている場合、ペーシング間隔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、ペーシング間隔を長くし、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 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）設定をコンフィギュレーション ファイルに保存します。

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 アドレスで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）設定をコンフィギュレーション ファイルに保存します。

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

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 41-6 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 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 41-6　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情報を表示します。
show ip ospf [*process-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	OSPF データベースに関連する情報のリストを表示します。
show ip ospf border-routes	内部 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 関連の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 関連の仮想リンク情報を表示します。

EIGRP の設定

拡張 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ディスタンス情報を使用しますが、EIGRP ではコンバージェンス プロパティと動作効率が大幅に改善されています。

コンバージェンス テクノロジーには、Diffusing Update Algorithm（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ループが発生しなくなり、トポロジの変更に関連するすべての装置を同時に同期できます。トポロジの変更の影響を受けないルータは、再計算から除外されます。

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、トランスポートレイヤのホップ 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 によって学習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 ルートを宛先方向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。受信ごとに完全更新パケットを処理する必要がないため、CPU 使用率が低下します。
- プロトコル独立型ネイバー探索メカニズム。このメカニズムを使用して、ネイバー ルータを確認します。
- Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）。
- 任意のルート サマライズ。
- 大規模ネットワークへの対応。

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ダイナミックに学習するために、ルータで使用されるプロセスです。ネイバーが到達不能になった場合、または操作不能になった場合、ルータもこの情報を検出する必要があります。ネイバー探索および回復は、サイズの小さな hello パケットを定期的に送信することにより、わずかなオーバーヘッドで実現されます。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学習します。このように判別された場合、ネイバー ルータはルーティング情報を交換できます。
- *信頼性のあるトランスポート 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 パケットが混在する送信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。効率を高めるために、必要な場合だけ信頼性が確保されます。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それぞれ 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通知する、レシーバー宛ての情報をパケットに格納して、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）では、確認応答（ACK パケット）を要求します。信頼性のあるトランスポートであれば、保留中の未確認応答がある場合、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、コンバージェンスに要する時間を短く保つことができます。
- *DUAL 有限ステート 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ます。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追跡します。DUAL は、ディスタンス情報（メトリック）を使用して効率的なループフリー パスを選択します。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ネイバー 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、再計算を行う必要があります。この結果、新しい後継ルータが決定されます。ルートの再計算にかかる時間によって、コンバージェンスに要する時間が変わります。再計算はプロセッサを集中的に使用するため、必要でない場合は、再計算を行わないようにしてください。トポロジに変更が発生すると、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 レイヤ プロトコルに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。このモジュールは、EIGRP パケットを解析し、受信した新しい情報を DUAL に通知する作業も行います。EIGRP は DUAL にルーティング判断を行うように要求しますが、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学習されたルートの再配信も行います。

ここでは、次の設定情報について説明します。

EIGRP のデフォルト設定

表 41-7 に、EIGRP のデフォルト設定を示します。

表 41-7　EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。クラスフル ネットワーク境界を通過するときに、この境界にサブプレフィクスがサマライズされます。
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。メトリックは次のとおりです。 • 帯域幅：0 kbps 以上 • 遅延（10 マイクロ秒単位）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ～ 255 の任意の数値（255 は信頼性が 100%） • 負荷：0 ～ 255 の数値で表される有効帯域幅（255 は 100% の負荷） • Maximum Transmission Unit（MTU; 最大伝送ユニット）：バイトで表された最大伝送ユニットのサイズ（0 または任意の正の整数）
ディスタンス	内部ディスタンス：90 外部ディスタンス：170
EIGRP ネイバー変更ログ	ディセーブル。隣接の変更はログに記録されません。
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	低速の 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	低速の 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。

表 41-7　EIGRP のデフォルト設定 （続き）

機能	デフォルト設定
IP サマリー アドレス	サマリー集約アドレスは未定義。
メトリックの重み	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。 ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
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分散。
差異	1（等価コスト ロード バランシング）

1. NSF = ノンストップ フォワーディング

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 アップデート中にアドバタイズされません。

（注）　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、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.41-24）も参照）。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP NSF 認識

EIGRP NSF 認識機能は IP サービス イメージの IPv4 でサポートされています。ネイバー ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータのプライマリ ルート プロセッサ（RP）に障害が発生してバックアップ RP によって処理が引き継がれる間、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 RP を手動でリロードしている間、ネイバー 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はできません。この機能の詳細については、次の URL の『*EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801600l0.html

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任意です。

	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 number*	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。AS 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	**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 4	**eigrp log-neighbor-changes**	（任意）EIGRP ネイバー変更ログをイネーブルにして、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 5	**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に入念に設定されていますが、調整することも可能です。 **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 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て、EIGRP によって学習したルートへの着信および発信メトリックを増加させます。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	**no 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ディセーブルにします。
ステップ 8	**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 9	**end**	特権 EXEC モードに戻ります。

ステップ 10	**show ip protocols**	設定を確認します。
		NSF 認識の場合、出力に次のように表示されます。
		`*** IP Routing is NSF aware ***`
		`EIGRP NSF enabled`

ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、これらのコマンドの **no** 形式を使用します。

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パーセンテージを設定します。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（自動サマリー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。デフォルト値は、低速の NBMA ネットワークの場合は 60 秒、それ以外のネットワークの場合は 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。デフォルト値は、低速の NBMA ネットワークの場合は 180 秒、それ以外のネットワークの場合は 15 秒です。 ⚠ **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て、ルート情報がその情報の送信元のインターフェイスからルータによってアドバタイズされるようにします。
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）設定をコンフィギュレーション ファイルに保存します。

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、これらのコマンドの **no** 形式を使用します。

EIGRP ルート認証の設定

EIGRP ルート認証を使用すると、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 チェーンを指定して、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、キー番号を指定します。
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、キー文字列を指定します。
ステップ 9	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの受信可能期間を指定します。 *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）キーの送信可能期間を指定します。 *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**	認証キーの情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、これらのコマンドの **no** 形式を使用します。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能は、ルーテッド トラフィックをエンド ユーザにより近い場所に移動することでリソースの利用率を低減させます。

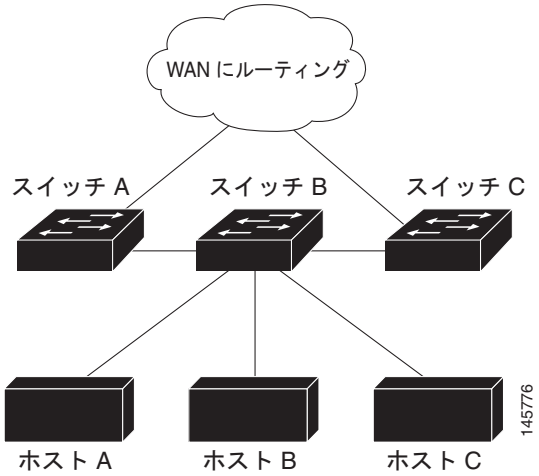
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザに対して許容される IP トラフィックのルートは、EIGRP スタブ ルーティングで設定されたスイッチを介したルートだけです。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他の装置に接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用する場合、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ディストリビューション ルータとリモート 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 ステータスを通知するパケットを受信するネイバーは、スタブ ルータに対してルートのクエリーを実行せず、スタブ ピアを持つルータはそのピアに対するクエリーを実行しません。スタブ ルータは、ディストリビューション ルータに依存してすべてのピアに適切なアップデートを送信します。

図 41-4 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、サマリー ルートをスイッチ A および 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 41-4　　EIGRP スタブ ルータ設定



（注） **eigrp stub** ルータ コンフィギュレーション コマンドを入力すると、**eigrp stub connected summary** コマンドだけが有効になります。CLI ヘルプでは **receive-only** および **static** キーワードが表示されることがありますが、IP ベース イメージを実行するスイッチは、常に **connected** および **summary** キーワードが設定されている場合と同様に動作します。

EIGRP スタブ ルーティングの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2*』の「Configuring EIGRP Stub Routing」を参照してください。

EIGRP のモニタ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 41-8 に、ネイバーの削除および統計情報の表示に使用する特権 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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。

表 41-8　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 用に設定されたインターフェイスの情報を表示します。
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 プロセスの送受信されたパケット数を表示します。

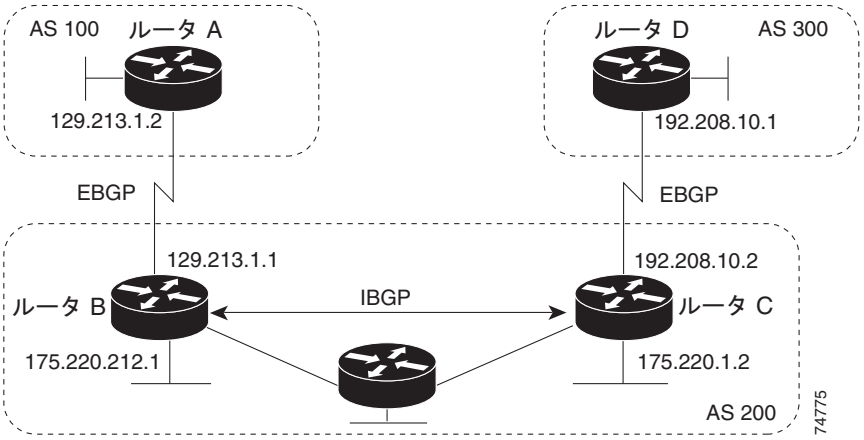
BGP の設定

Border Gateway Protocol（BGP）は Exterior Gateway Protocol（EGP; エクステリア ゲートウェイ プロトコル）です。自律システム間で、ループの発生しないルーティング情報の交換を保証するドメイン間ルーティング システムを設定するために使用されます。自律システムは、同じ管理下で動作して、RIP や OSPF などの Interior Gateway Protocol（IGP）を境界内で実行し、Exterior Gateway Protocol（EGP）を使用して相互接続するルータで構成されます。BGP Version 4 は、インターネットでドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。BGP の詳細については、『*Internet Routing Architectures*』（Cisco Press 刊）、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」の章を参照してください。

BGP コマンドおよびキーワードの詳細については、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*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 C「Cisco IOS Release 12.2(55)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 アップデートを交換する場合、同じ自律システム（AS）に属するルータは *Internal BGP*（IBGP; 内部 BGP）を実行し、異なる自律システムに属するルータは *External BGP*（EBGP; 外部 BGP）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。違いは、ルーティング アップデートが AS 間で交換されるか（EBGP）、または AS 内で交換されるか（IBGP）という点です。図 41-5 に、EBGP と IBGP の両方が稼動するネットワークを示します。

図 41-5　EBGP、IBGP、および複数の自律システム



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF などの AS 内で稼動する IGP に BGP ルーティング情報を再配信して、AS 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 Transmission Control Protocol（TCP; 伝送制御プロトコル）を使用します（特にポート 179）。ルーティング情報を交換するために相互に 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 41-5 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フル パスを示す一連の AS 番号です。BGP はこの情報を使用して、ループのない自律システム マップを作成します。

このネットワークには、次の特性があります。

- ルータ A および B では EBGP が稼動し、ルータ B および C では IBGP が稼動しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼動し、2 つのネイバーが相互に到達する限り、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは論理的にフル メッシュ構造である必要があります。BGP4 は、論理フル メッシュに関する要件を軽減する 2 つの技術（*連合*と*ルート リフレクタ*）を提供します。
- AS 200 は、AS 100 および AS 300 の*中継 AS* です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアは、キープアライブ メッセージ（接続がアップ状態であることを確認）、および通知メッセージ（エラーや特殊条件に応答）も交換します。

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*のリストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワーク到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシーの判断を行うために使用できます。

Cisco IOS が稼動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である場合を除く）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.41-51）を参照してください。

BGP Version 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することで、ルーティング テーブルのサイズを削減できます。CIDR では BGP 内部のネットワーク クラスの概念が排除され、IP プレフィクスのアドバタイズがサポートされています。

ここでは、次の設定情報について説明します。

- 「BGP のデフォルト設定」（P.41-44）
- 「BGP ルーティングのイネーブル化」（P.41-47）
- 「ルーティング ポリシーの変更の管理」（P.41-50）
- 「BGP 判断属性の設定」（P.41-51）
- 「ルート マップによる BGP フィルタリングの設定」（P.41-53）
- 「ネイバーによる BGP フィルタリングの設定」（P.41-54）
- 「BGP フィルタリング用のプレフィクス リストの設定」（P.41-55）
- 「BGP コミュニティ フィルタリングの設定」（P.41-56）
- 「BGP ネイバーおよびピア グループの設定」（P.41-58）
- 「集約アドレスの設定」（P.41-60）
- 「ルーティング ドメイン連合の設定」（P.41-61）
- 「BGP ルート リフレクタの設定」（P.41-61）
- 「ルート ダンプニングの設定」（P.41-62）
- 「BGP のモニタおよびメンテナンス」（P.41-63）

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Routing Protocols」にある「Configuring BGP」の章を参照してください。特定の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。これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

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 C「Cisco IOS Release 12.2(55)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 41-9 に、BGP の基本的な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 ProtocolsRelease 12.2*』で特定のコマンドを参照してください。

表 41-9　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：定義なし
AS パス アクセス リスト	定義なし。
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-path* を考慮し、外部 BGP ピアからの類似ルートは比較されません。 • ルータ ID の比較：ディセーブル

表 41-9　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：定義なし。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。 • 形式：シスコのデフォルト形式（32 ビットの番号）
BGP 連合 ID/ ピア	• ID：設定なし • 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 プリファレンス	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。イネーブルの場合は次のようになります。 • 半減期は 15 分 • 再利用値は 750（10 秒増分） • 抑制値は 2000（10 秒増分） • 最大抑制時間は半減期の 4 倍（60 分）
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合はループバック 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	• 外部ルート管理ディスタンス：20（指定できる値は 1 ～ 255） • 内部ルート管理ディスタンス：200（指定できる値は 1 ～ 255） • ローカル ルート管理ディスタンス：200（指定できる値は 1 ～ 255）
配信リスト	• 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 • 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 プレフィクス リスト	定義なし。
Multi Exit Discriminator（MED）	• 常に比較：ディセーブル。異なる自律システム内のネイバーからのパスに対して MED を比較しません。 • 最適パスの比較：ディセーブル。 • 最も条件の悪いパスである MED の除外：ディセーブル。 • 決定的な MED 比較：ディセーブル。

表 41-9　BGP のデフォルト設定 （続き）

機能	デフォルト設定
ネイバー	• アドバタイズの間隔：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズ：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • 配信リスト：定義なし • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィクスの最大数：制限なし • ネクストホップ（BGP ネイバーのネクストホップとなるルータ）：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし。割り当てメンバーなし • プレフィクス リスト：指定なし • リモート AS（ネイバー BGP テーブルへのエントリ追加）：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ属性送信：ネイバーへの送信なし • シャットダウンまたはソフト再設定：ディセーブル • タイマー：キープアライブは 60 秒、ホールドタイムは 180 秒 • アップデート送信元：最適ローカル アドレス • バージョン：BGP Version 4 • 重み：BGP ピアによって学習されたルートは 0、ローカル ルータから取得されたルートは 32768
NSF[1] 認識	ディセーブル。ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。 **（注）** 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で、IPv4 でイネーブルにできます。
ルート リフレクタ	設定なし。
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 = ノンストップ フォワーディング

ノンストップ フォワーディング認識

BGP NSF 認識機能は IP サービス イメージの IPv4 で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。ネイバー ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータのプライマリ ルート プロセッサ（RP）に障害が発生してバックアップ RP によって処理が引き継がれる間、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 RP を手動でリロードしている間、ネイバー ルータからパケットを転送し続けます。

詳細については、次の URL の『*BGP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015fede.html

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 AS 内に、*外部ネイバー*は異なる自律システム内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダ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 AS 番号の範囲は 64512 ～ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号は廃棄されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と*同期化*されるまで、待機する必要があります。同期化はデフォルトでイネーブルになっています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または自律システム内のすべてのルータで BGP が稼動している場合は、同期化をディセーブルにし、IGP 内で伝送されるルートを少なくして、BGP がより短時間で収束するようにします。

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限り必要）。
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 AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ～ 65535 です。64512 ～ 65535 はプライベート自律システム番号専用です。
ステップ 4	**network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。

	コマンド	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスに任意のルータ インターフェイス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 AS パスからプライベート AS 番号を削除します。
ステップ 7	**no synchronization**	（任意）BGP と IGP の間の同期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 テーブルに挿入されます。
ステップ 9	**bgp fast-external-fallover**	（任意）外部ネイバー間のリンクがダウンした場合に、BGP セッションを自動的にリセットします。デフォルトでは、セッションがただちにリセットされることはありません。
ステップ 10	**bgp graceful-restart**	（任意）スイッチでの NSF 認識をイネーブルにします。デフォルトでは、NSF 認識はディセーブルになっています。
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*
	または
	show ip bgp neighbor
		設定を確認します。
		NSF 認識（グレースフル リスタート）がネイバーでイネーブルになっていることを確認します。
		スイッチおよびネイバーで NSF 認識がイネーブルになっている場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised and received`
		NSF 認識がスイッチではイネーブルになっているが、ネイバーではディセーブルになっている場合は、次のメッセージが表示されます。
		`Graceful Restart Capability: advertised`

ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP AS 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 AS 番号を追加するには、**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 41-5 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 ピアが稼動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 に対してこのコマンドを実行した場合の出力を示します。

```
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
```

state = established 以外の情報が出力された場合、ピアは稼動していません。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。テーブルが新しい情報で更新されるたびに、テーブルのバージョン番号が増加します。テーブルのバージョン番号が継続的に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 コマンドによる IP ネットワークへの参照で制御されるのは、アドバタイズされるネットワークだけです。これは、Interior Gateway Protocol（IGP）とは対照的です。EIGRP などの IGP でも、**network** コマンドを使用してアップデートの送信先を指定します。

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。特定の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。スイッチ プロンプトで疑問符を入力した場合に表示されるにもかかわらず、このスイッチでサポートされない BGP コマンドのリストについては、付録 C「Cisco IOS Release 12.2(55)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 ポリシーの変更の管理

ピアのルーティング ポリシーには、着信または発信ルーティング テーブルの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。あとで BGP のフィルタ、重み、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハード リセットとソフト リセットの 2 種類があります。このスイッチでは、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。事前設定を行わずにソフト 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る必要があります。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 メッセージで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 リフレッシュ要求やルーティング情報をダイナミックに交換したり、それぞれの発信ルーティング テーブルをあとで再アドバタイズしたりすることができます。

- ソフト リセットによってネイバーから着信アップデートが生成される場合のリセットを、*ダイナミック着信ソフト 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る場合のリセットを、*発信ソフト リセット*といいます。

ソフト着信リセットが発生すると、新しい着信ポリシーが有効になります。ソフト発信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、新しいローカル発信ポリシーが有効になります。発信ポリシーのリセット中に一連の新しいアップデートが送信されると、新しい着信ポリシーも有効になる場合があります。

表 41-10 に、ハード リセットとソフト リセットの利点と欠点を示します。

表 41-10　ハード リセットとソフト リセットの利点と欠点

リセットのタイプ	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 Forwarding Information Base（FIB; 転送情報ベース）テーブルのプレフィクスが失われます。ハード リセットの使用は推奨しません。
発信ソフト リセット	ルーティング テーブルのアップデートが設定されず、保管もされません。	着信ルーティング テーブルのアップデートがリセットされません。
ダイナミック着信ソフト リセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブルの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。

BGP ピアがルート リフレッシュ機能をサポートしているかどうかの確認や、BGP セッションのリセットを行うには、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	**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してい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。 *Received route refresh capability from peer.*
ステップ 2	**clear ip bgp** {***** | *address* | *peer-group-name*}	指定された接続のルーティング テーブルをリセットします。 • すべての接続をリセットする場合は、アスタリスク（*****）を入力します。 • 特定の接続をリセットする場合は、IP *アドレス*を入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	**clear ip bgp** {***** | *address* | *peer-group-name*} **soft out**	（任意）指定された接続の着信ルーティング テーブルをリセットするには、発信ソフト 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。 • すべての接続をリセットする場合は、アスタリスク（*****）を入力します。 • 特定の接続をリセットする場合は、IP *アドレス*を入力します。 • ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	**show ip bgp** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

BGP スピーカーが複数の自律システムから受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達するための最適パスを 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素に基づいて行われます。

BGP ピアは、1 つのプレフィクスに対して 2 つの EBGP パスをネイバー AS から学習する場合、最適パスを選択して IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルで、同じネイバー AS から複数の EBGP パスを学習する場合、単一の最適パスではなく、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。

BGP が最適パスを選択する際に属性を評価する順序を次に示します。

1. パスで指定されているネクストホップにアクセス不能な場合、アップデートが削除されます。BGP のネクストホップ属性（ソフトウェアによって自動判別される）は、宛先に到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、このアドレスは通常、**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. 重みが最大のパスが優先されます（シスコ独自のパラメータ）。重み属性はルータにローカルであるため、ルーティング アップデートでは伝播されません。デフォルトでは、ルータ送信元のパスに対する重み属性は 32768 で、その他のパスに対する重み属性は 0 です。重みが最大のルートが優先されます。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 プリファレンスが最大のルートが優先されます。ローカル プリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル プリファレンス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 ルータで実行されている BGP から送信されたルートが優先されます。
5. AS パスが最短のルートが優先されます。
6. 送信元のタイプが最小のルートが優先されます。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 によって学習されたルートは、不明な送信元のルートや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のネイバー AS 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が優先されます。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）パスが優先されます。
9. 最も近い IGP ネイバー（最小の IGP メトリック）を経由して到達できるルートが優先されます。つまり、ルータは、宛先に到達するための AS 内の最短の内部パス（BGP のネクストホップへの最短パス）を優先します。
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。
    - 最適ルートと対象のルートがともに外部ルートである。
    - 最適ルートと対象のルートの両方が、同じネイバー AS（自律システム）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 アドレス値が最小のルートが優先されます。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、実装に依存する場合があります。

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 AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp best-path as-path ignore**	（任意）ルートの選択中に AS パスの長さ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する特定の IP アドレスを入力し、ネイバーへの BGP アップデートに対するネクストホップ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。指定できる値は 0 ～ 65535 です。重みが最大のルートが優先されます。別の BGP ピアから学習したルートのデフォルトの重みは 0、ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	**default-metric** *number*	（任意）優先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 が設定されていないルートも、すべてこの値に設定されます。指定できる範囲は 1 ～ 4294967295 です。最小値のルートが最優先されます。

	コマンド	目的
ステップ 7	**bgp bestpath med missing-as-worst**	（任意）MED が設定されていないパスは無限の値が設定されていると見なし、そのパスの優先順位が最も低く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）自律システムが異なるネイバーからのパスの 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 の比較は同じ AS 内のパス間でだけ行われます。
ステップ 9	**bgp bestpath med confed**	（任意）連合内の異なるサブ自律システム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 AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	**bgp default local-preference** *value*	（任意）デフォルトのローカル プリファレンス値を変更します。指定できる範囲は 0 ～ 4294967295 です。デフォルト値は 100 です。最大のローカル プリファレンス値が優先されます。
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 テーブルに格納されます。指定できる範囲は 1 ～ 16 です。パスの数を複数に設定すると、パス間のロード バランシングが可能になります（スイッチ ソフトウェアでは最大 32 の等価コスト ルートを使用できますが、スイッチ ハードウェアでは 1 ルートあたり 17 以上のパスは使用しません）。
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** **show ip bgp neighbors**	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ステートに戻すには、各コマンドの **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

BGP 内でルート マップを使用すると、ルーティング情報の制御や変更を行ったり、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することができます。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.41-94）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）と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。

	コマンド	目的
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。 • 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 ピアリング アドレスに設定し、サードパーティのネクストホップを上書きします。 • BGP ピアの発信ルート マップの場合は、ネクストホップをローカル ルータのピアリング アドレスに設定し、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*]	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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 アドバタイズをフィルタリングするには、**as-path access-list** グローバル コンフィギュレーション コマンドや **neighbor filter-list** ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。**neighbor distribute-list** ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。distribute-list フィルタはネットワーク番号に適用されます。**distribute-list** コマンドの詳細については、「ルーティング アップデートのアドバタイズおよび処理の制御」（P.41-102）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、アップデートのフィルタリングや、各属性の変更を行うことができます。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受信されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには **match as-path access-list** ルート マップ コマンドが、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 コマンドが、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 コマンドがそれぞれ必要です。

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 AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 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。 **（注）** **neighbor prefix-list** ルータ コンフィギュレーション コマンドを使用してアップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。
ステップ 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。

	コマンド	目的
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）設定をコンフィギュレーション ファイルに保存します。

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 AS パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現に基づくアクセス リストです（正規表現の作成方法の詳細については、『*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、AS 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 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）設定をコンフィギュレーション ファイルに保存します。

BGP フィルタリング用のプレフィクス 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クス リストを使用できます。プレフィクス リストを使用すると、大規模なリストのロードや検索のパフォーマンスが改善する、差分更新がサポートされる、CLI（コマンドライン インターフェイス）設定が簡素化される、柔軟性が増すなどの利点が生じます。

プレフィクス リストによるフィルタリングでは、アクセス リストを照合する場合と同様に、プレフィクス リストに記載されたプレフィクスとルートのプレフィ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。プレフィクスが許可されるか拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィクス リストはすべてのプレフィクスを許可する。
- 指定されたプレフィクスがプレフィクス リスト内のどのエントリとも一致しない場合は、暗黙拒否が使用される。
- プレフィクス リストの複数のエントリが指定されたプレフィクスと一致する場合は、シーケンス番号が最小のプレフィクス リスト エントリが特定される。

デフォルトでは、シーケンス番号が自動生成されます。デフォルトの増分単位は 5 です。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。シーケンス番号の増分単位には任意の値を指定できます。増分単位に 1 を指定すると、リストに追加エントリを挿入できなくなります。増分単位に非常に大きい値を指定すると、値が足り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クス リストを使用する場合は、あらかじめプレフィクス リストを設定しておく必要があります。プレフィクス リストの作成や、プレフィクス リストへのエントリの追加を行うには、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	**ip prefix-list** *list-name* [**seq** *seq-value*] **deny** | **permit** *network*/*len* [**ge** *ge-value*] [**le** *le-value*]	シーケンス番号（任意）を指定してプレフィクス リストを作成し、条件が一致する場合のアクセスを拒否（**deny**）または許可（**permit**）します。**permit** コマンド **deny** コマンドを少なくとも 1 つ入力する必要があります。 • *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。 • （任意）**ge** および **le** の値は、照合するプレフィクス長の範囲を指定します。*ge-value* および *le-value* に指定する値は、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**]	プレフィクス リストまたはプレフィクス 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）設定をコンフィギュレーション ファイルに保存します。

プレフィクス リストと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。プレフィクス リストからエントリを削除するには、**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

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいて、BGP でルーティング情報の配信を制御する方法の 1 つです。この属性によって、宛先が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することができます。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、COMMUNITIES 属性（任意）によって識別されます。この属性は推移的かつグローバルで、その範囲は 1 ～ 4294967200 です。事前に定義されている既知のコミュニティの一部を次に示します。

- **internet**：対象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。すべてのルータがこのコミュニティに属します。
- **no-export**：EBGP ピアに対象のルートをアドバタイズしません。
- **no-advertise**：ピア（内部または外部）に対象のルートをアドバタイズしません。
- **local-as**：ローカル自律システムの外部のピアに対象のルートをアドバタイズしません。

許可するルーティング情報、他のネイバーよりも優先するルーティング情報、または他のネイバーに配信するルーティング情報は、コミュニティに基づいて制御できます。BGP スピーカーは、ルートの学習、アドバタイズ、または再配信を行うときに、ルートのコミュニティの設定、追加、または変更を行う場合があります。ルートを集約すると、その集約の 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るようになります。

コミュニティ リストを使用すると、ルート マップの match コマンドで使用するコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成することもできます。一致が見つかるまでステートメントがチェックされ、いずれかのステートメントで一致が見つかり次第、テストが終了します。

COMMUNITIES 属性および match コマンドをコミュニティに基づいて設定する場合は、「ルート マップによるルーティング情報の再配信」（P.41-94）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 リストの作成および適用を行うには、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	**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。 • *community-list-number* は 1 ～ 99 の整数です。この値によって、コミュニティの許可グループまたは拒否グループが 1 つまたは複数識別されます。 • *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**	この IP アドレスのネイバーに COMMUNITIES 属性を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。
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。

	コマンド	目的
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および解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長の形式で表示されます。シスコのデフォルトのコミュニティの形式は NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 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）設定をコンフィギュレーション ファイルに保存します。

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（同じ発信ルート 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 グループを作成してオプションを割り当て、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは remote-as（設定されている場合）、version、update-source、out-route-map、out-filter-list、out-dist-list、minimum-advertisement-interval、next-hop-self など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対して行われた変更も継承します。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 グループのメンバーにします。
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。ピア グループが **remote-as** *number* を使用して設定されていない場合は、このコマンドを使用して、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）ネイバーに説明を関連付けます。
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。

	コマンド	目的
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community**	（任意）この IP アドレスのネイバーに COMMUNITIES 属性を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）内部 BGP セッションで、TCP 接続用の操作インターフェイスをすべて使用できるようにします。
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 セッションを許可します。マルチホップ ピアの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 AS として使用する AS 番号を指定します。指定できる範囲は 1 ～ 65535 です。
ステップ 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間隔を設定します。
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）は最大割合を表します。この値に達すると警告メッセージが生成されます。デフォルト値は 75% です。
ステップ 14	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	（任意）ネイバーに対する BGP アップデートでのネクストホップ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 ピア間の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）この IP アドレスのネイバーに COMMUNITIES 属性を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。 • *keepalive* インターバルで指定した時間内に、キープアライブ メッセージがピアに送信されます。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 60 秒です。 • *holdtime* は、ピアからのキープアライブ メッセージを受信しなかった場合に、そのピアを非アクティブと宣言するまでの間隔です。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 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対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の保管を開始するようにソフトウェアを設定します。

	コマンド	目的
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）設定をコンフィギュレーション ファイルに保存します。

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。ディセーブルになっ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）を使用すると、集約ルート（または*スーパーネット*）を作成して、ルーティング テーブルのサイズを最小にすることができます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、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 つ以上存在する場合は、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、AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すために、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）AS 設定パス情報を生成します。このコマンドは、前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET になります。このルートは絶えず取り消しや更新を行う必要があるため、多数のパスを集約する場合は、このキーワードを使用しないでください。
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条件に基づいて、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）設定をコンフィギュレーション ファイルに保存します。

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 メッシュを減らす方法の 1 つは、自律システムを複数のサブ自律システムに分割し、単一の自律システムとして認識される単一の連合にグループ化することです。各自律システムの内部はフル メッシュ構造になっており、同じ連合内の他の自律システムへの接続がいくつか確立されます。異なる自律システム内のピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様の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 プリファレンス情報が維持されるため、すべての自律システムで単一の 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 ...*]	連合に属する自律システムと、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** **show ip bgp network**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

BGP ルート リフレクタの設定

BGP では、すべての IBGP スピーカーをフル 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止するには、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し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 スピーカーをフル メッシュ構造にする必要がありません。学習したルートをネイバーに渡す場合に別の方法が使用されるためです。*ルート リフレクタ*に設定された内部 BGP ピアは、IBGP によって学習されたルートを一連の IBGP ネイバーに送信します。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）の 2 つのグループに分類されます。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します。ルート リフレクタとそのクライアント ピアは、*クラスタ*を形成します。非クライアント ピアは相互にフル 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 リフレクタでは、ネイバーに応じて、次のいずれかの処理が実行されます。

- 外部 BGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズする。
- 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する。
- 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する（したがって、クライアントをフル 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 ポイント障害を回避するために、複数のルート リフレクタをクラスタに設定する場合があります。このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID（4 バイト）を設定する必要があります。クラスタとして機能するルート リフレクタは、すべてフル メッシュ構造にする必要があります。また、一連の同一なクライアント ピアと非クライアント 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 リフレクション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が他のクライアントに反映されます。ただし、クライアントがフル メッシュ構造の場合、ルート リフレクタはクライアントにルートを反映す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 ID とクラスタ リスト属性を表示します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート ダンプニングの設定

ルート フラップ ダンプニングは、インターネットワーク全体にフラッピング ルートが伝播するのを最小限に抑えるための BGP 機能です。ルートを使用できる状態と使用できない状態が交互に繰り返される場合、そのルートはフラッピングしていると見なされます。ルート ダンプニングがイネーブルになっている場合は、フラッピングしているルートに*ペナルティ*値が割り当てられます。ルートの累積ペナルティが制限値（設定可能）に達すると、そのルートが稼動している場合でも、BGP によってルートのアドバタイズが抑制されます。*再利用制限値*は、ペナルティと比較される設定可能な値です。ペナルティが再利用制限値よりも小さくなると、抑制されたルートが稼動中であれば、アドバタイズが再開されます。

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

BGP ルート ダンプニングを設定するには、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 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 ダンプニングの各要素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。
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）ダンプニングされたルートを表示します（抑制されるまでの時間も表示されます）。
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、ルートがダンプニング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）設定をコンフィギュレーション ファイルに保存します。

フラップ ダンプニングをディセーブルにするには、キーワードを指定せずに **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。ダンプニングの各要素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 のモニタおよびメンテナンス

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

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

表 41-8 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.com のホーム ページにアクセスして、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

表 41-11　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ーを削除します。

表 41-11　IP BGP の clear および show コマンド （続き）

コマンド	目的
show ip bgp *prefix*	プレフィクスがアドバタイズされている、ピア グループおよびピア 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 プレフィクスなどのプレフィ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のネットワーク 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 AS 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	送信元の自律システムと矛盾するルートを表示します。
show ip bgp regexp *regular-expression*	コマンドラインで入力された特定の正規表現と一致する AS 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 ネイバーから学習し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 コマンドを使用して、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージのロギングをイネーブルに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）プロトコルは、Open System Interconnection（OSI; 開放型システム間相互接続）モデルのネットワーク レイヤに関する標準です。ISO ネットワーク アーキテクチャでは、アドレスを Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）および Network Entity Title（NET）と呼びます。OSI ネットワーク内の各ノードには、1 つまたは複数の NET が 設定されます。また、NSAP アドレスも多数設定されます。

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、スイッチでのコネクションレス型ルーティングをイネーブルにした場合、スイッチはルーティング関連機能を実行せず、転送の判断だけを行います。ダイナミック ルーティングの場合は、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。このスイッチは、ISO CLNS ネットワークの OSI ルーティング プロトコルに基づく 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ています。

ダイナミック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ています。エリア内のすべてのルータは、すべてのシステム ID への到達方法を認識します。エリア間のルータは、適切なエリアへの到達方法を認識します。IS-IS は、*ステーション ルーティング*（エリア内）および*エリア ルーティング*（エリア間）の 2 つのレベルのルーティングをサポートしています。

ISO IGRP と IS-IS NSAP アドレッシング方式の主な違いは、エリア アドレスの定義です。どちらもレベル 1 ルーティング（エリア内ルーティング）にはシステム ID を使用しますが、エリア ルーティングにおけるアドレスの指定方法が異なります。ISO IGRP NSAP アドレスには、3 つの個別のルーティング用フィールド（*ドメイン*、*エリア*、*システム ID*）が含まれています。IS-IS アドレスには、2 つのフィールド（単一の連続した*エリア*フィールド（ドメイン フィールドとエリア フィールドで構成）、*システム ID*）が含まれています。

（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。この章で使用されてい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 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 プロトコルです（ISO 10589 を参照）。他のルーティング プロトコルとは異なり、IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成し、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。各レイヤ 3 スイッチまたはルータに複数の IS-IS ルーティング プロセスを指定するには、マルチエリア IS-IS 設定構文を使用します。次に、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。

小規模な IS-IS ネットワークは、ネットワーク内のすべてのルータを含む単一エリアとして作成されます。大規模になったネットワークは、通常、すべてのエリアから接続されているすべてのレベル 2 ルータで構成されるバックボーン エリアに再編成され、このバックボーン エリアからローカル エリアに接続されます。ローカル エリア内のルータは、すべてのシステム ID への到達方法を認識します。エリア間のルータはバックボーンへの到達方法を、バックボーン ルータは他のエリアへの到達方法を認識します。

ルータは、ローカル エリア内のルーティング（ステーション ルーティング）を実行する場合、レベル 1 隣接を確立します。レベル 1 エリア間のルーティング（エリア ルーティング）を実行する場合は、レベル 2 隣接を確立します。

単一の Cisco ルータは、最大 29 個のエリア内のルーティングに参加できます。また、バックボーンでは、レベル 2 ルーティングを実行できます。一般に、各ルーティング プロセスは 1 つのエリアに対応します。デフォルトでは、設定されたルーティング プロセスの最初のインスタンスによって、レベル 1 とレベル 2 の両方のルーティングが実行されます。追加のルータ インスタンスを設定することもでき、追加されたインスタンスはレベル 1 エリアとして自動的に処理されます。IS-IS ルーティング プロセスの各インスタンスのパラメータは、個別に設定する必要があります。

IS-IS マルチエリア ルーティングの場合、レベル 2 ルーティングを実行するように設定できるプロセスは 1 つだけです。ただし、各シスコ製装置にはレベル 1 エリアを 29 個まで定義できます。どのプロセスにもレベル 2 ルーティングが設定されている場合、すべての追加プロセスは自動的にレベル 1 として設定されます。このプロセスは、レベル 1 ルーティングを同時に実行するように設定できます。レベル 2 ルーティングがルータ インスタンスに対して適切でない場合は、**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 機能を削除します。レベル 2 ルータとして別のルータ インスタンスを設定する場合も、**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」を参照してください。この項で使用してい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について簡単に説明します。内容は次のとおりです。

IS-IS のデフォルト設定

表 41-12 に、IS-IS のデフォルト設定を示します。

表 41-12　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）エラーの無視	イネーブル。
IS-IS タイプ	従来の IS-IS：ルータはレベル 1（ステーション）およびレベル 2（エリア）のルータとして機能します。 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はレベル 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 隣接ステート変更ログ	ディセーブル。
LSP 生成スロットリング タイマー	2 つの連続する LSP 生成間の最大インターバル：5 秒。 最初の LSP 生成遅延：50 ミリ秒。 最初と 2 番めの LSP 生成間のホールドタイム：5000 ミリ秒。
LSP 最大存続時間（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。ハードウェアまたはソフトウェアの変更中に、NSF 対応のネイバー ルータからのパケット転送をレイヤ 3 スイッチで継続できます。
Partial Route Computation（PRC）スロットリング タイマー	最大 PRC 待機インターバル：5 秒。 トポロジ変更後の最初の PRC 計算遅延：2000 ミリ秒。 最初と 2 番めの 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。
パスワード	エリアまたはドメインのパスワードは定義されていません。認証はディセーブルになっています。
set-overload-bit	ディセーブル。引数を入力せずにイネーブルにすると、過負荷ビットがただちに設定され、**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。

表 41-12　IS-IS のデフォルト設定 （続き）

機能	デフォルト設定
Shortest Path First（SPF）スロットリング タイマー	連続する SPF 間の最大インターバル：10 秒。 トポロジ変更後の最初の SPF 計算：5500 ミリ秒。 最初と 2 番めの SPF 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 = ノンストップ フォワーディング。

ノンストップ フォワーディング認識

統合 IS-IS NSF 認識機能は、IPv4 に対してサポートされています。この機能により、NSF を認識する Customer Premises Equipment（CPE; 宅内装置）ルータが、NSF 対応ルータによるパケットのノンストップ フォワーディングの実行を支援できます。ローカル ルータが NSF を実行しているとは限りませんが、その NSF 認識により、NSF 対応のネイバー ルータにあるルーティング データベースとリンクステート データベースの完全性と正確性が、スイッチオーバー プロセスの間も維持されます。

この機能は自動的にイネーブルになるため、設定する必要がありません。この機能の詳細については、次の URL の『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a00801541c7.shtml

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、ルーティング プロセスごとに名前と NET を指定します。次に、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 プロセスのインスタンスごとに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 プロセスのインスタンスごと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します。
ステップ 3	**router isis** [*area tag*]	指定されたルーティング プロセスの IS-IS ルーティングをイネーブルにして、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。 （任意）IS-IS ルータを割り当てるエリアを指定するには、*area tag* 引数を使用します。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。 最初に設定した IS-IS インスタンスは、デフォルトではレベル 1-2 です。それ以降に設定したインスタンスは、自動的にレベル 1 になります。ルーティングのレベルを変更するには、**is-type** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**net** *network-entity-title*	ルーティング プロセスの NET を設定します。マルチエリア IS-IS を設定する場合は、ルーティング プロセスごとに NET を指定します。NET およびアドレスには、名前を指定できます。

	コマンド	目的
ステップ 5	**is-type** {**level-1** | **level-1-2** | **level-2-only**}	（任意）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、またはその両方（デフォルト）として機能するように、ルータを設定できます。 • **level-1**：ステーション ルータとしてだけ機能します。 • **level-1-2**：ステーション ルータおよびエリア ルータとして機能します。 • **level 2**：エリア ルータとしてだけ機能します。
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て、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** コマンドを入力して、レイヤ 3 モードにします。
ステップ 8	**ip router isis** [*area tag*]	インターフェイスに ISO CLNS 用の 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 デジグネータを付加します。
ステップ 9	**clns router isis** [*area tag*]	インターフェイスで 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。いずれか 1 つのインターフェイスが IS-IS ルーティング用に設定されている場合は、IS-IS に対応しているエリア内のすべてのインターフェイスに IP アドレスを設定する必要があります。
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**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、IP ルーティング プロトコルとして従来の IS-IS を実行するように、3 つのルータを設定する例を示します。従来の IS-IS では、すべてのルータがレベル 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 gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
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 gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
```

```
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 gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
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

次に、設定可能な任意の IS-IS グローバル パラメータの一部を示します。

- ルート マップで制御されるデフォルト ルートを設定すると、デフォルト ルートを IS-IS ルーティング ドメインに強制的に設定することができます。また、ルート マップで設定可能なその他のフィルタリング オプションを指定することもできます。
- 内部チェックサム エラーとともに受信した IS-IS LSP を無視したり、壊れた LSP を消去して、LSP の発信側で LSP を再生成するように、ルータを設定することができます。
- エリアおよびドメインにパスワードを割り当てることができます。
- ルーティング テーブル内でサマリー アドレスによって表される集約アドレスを作成できます（ルート サマライズ）。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。サマリーのアドバタイズに使用されるメトリックは、すべてのルートの中で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、およびリフレッシュを行わずに LSP がルータ データベース内に存続できる最大時間を設定できます。
- LSP 生成、Shortest Path First 計算、および Partial Route Computation のスロットリング タイマーを設定できます。
- IS-IS 隣接のステートが変更（アップまたはダウン）された場合に、ログ メッセージを生成するようにスイッチを設定できます。
- ネットワーク内のリンクの最大伝送ユニット（MTU）サイズが 1500 バイト未満である場合は、LSP MTU の値を小さくして、ルーティングを引き続き実行することができます。
- partition avoidance ルータ コンフィギュレーション コマンドを使用すると、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 ホスト間でフル接続が切断された場合に、エリアの分割を防止することができます。

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 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 ドメインに強制的に設定します。ルート マップが設定されている場合に **route-map** *map-name* を入力すると、ルーティング プロセスによってデフォルト ルートが生成されます。
ステップ 5	**ignore-lsp-errors**	（任意）内部チェックサム エラーを含む LSP を消去せず、無視するように、ルータを設定します。デフォルトでは、このコマンドはイネーブルになっています（壊れた LSP は廃棄されます）。壊れた 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）エリア認証パスワードを設定します。このパスワードはレベル 1（ステーション ルータ レベル）の LSP に挿入されます。
ステップ 7	**domain-password** *password*	（任意）ルーティング ドメイン認証パスワードを設定します。このパスワードはレベル 2（エリア ルータ レベル）の LSP に挿入されます。
ステップ 8	**summary-address** *address mask* [**level-1** | **level-1-2** | **level-2**]	（任意）指定された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）計算でそのルータを無視できるように、過負荷ビット（hippity ビット）を設定します。 • （任意）**on-startup**：起動時にだけ過負荷ビットを設定します。**on-startup** を指定しない場合は、過負荷ビットがただちに設定され、**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** を指定する場合は、秒数または **wait-for-bgp** を入力する必要があります。 • *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、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。 • **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、BGP が収束するまで設定されたままになります。BGP が収束したことが 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 インターバルを秒単位で設定します。指定できる範囲は 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）リフレッシュを実行しない場合に、LSP パケットがルータ データベース内に存続する最大時間を設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 1200 秒（20 分）です。指定された時間が経過すると、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 LSP 生成スロットリング タイマーを設定します。 • *lsp-max-wait*：2 つの連続する LSP 生成間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 5 です。 • *lsp-initial-wait*：最初の LSP 生成遅延（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 50 です。 • *lsp-second-wait*：最初と 2 番めの LSP 生成間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5000 です。

	コマンド	目的
ステップ 13	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]	（任意）IS-IS Shortest Path First（SPF）スロットリング タイマーを設定します。 • *spf-max-wait*：連続する SPF 間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 10 です。 • *spf-initial-wait*：トポロジ変更後の最初の SPF 計算（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5500 です。 • *spf-second-wait*：最初と 2 番めの SPF 計算間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5500 です。
ステップ 14	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*]	（任意）IS-IS Partial Route Computation（PRC）スロットリング タイマーを設定します。 • *prc-max-wait*：2 つの連続する PRC 計算間の最大インターバル（秒単位）。指定できる範囲は 1 ～ 120 です。デフォルト値は 5 です。 • *prc-initial-wait*：トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 2000 です。 • *prc-second-wait*：最初と 2 番めの PRC 計算間のホールドタイム（ミリ秒単位）。指定できる範囲は 1 ～ 10000 です。デフォルト値は 5000 です。
ステップ 15	**log-adjacency-changes** [**all**]	（任意）IS-IS 隣接のステート変更をログ記録するようにルータを設定します。End System-to-Intermediate System PDU や Link State Packet（LSP）など、Intermediate System-to-Intermediate System Hello に関連しないイベントによって生成されたすべての変更をログに含める場合は、**all** を入力します。
ステップ 16	**lsp-mtu** *size*	（任意）最大 LSP パケット サイズをバイト単位で指定します。指定できる範囲は 128 ～ 4352 です。デフォルト値は 1497 バイトです。 **（注）** ネットワーク内のあるリンクで MTU サイズが小さくなった場合は、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、すべてのレベル 1 隣接ルータ、およびエンド ホスト間でフル接続が切断された場合、レベル 1 エリア プレフィクスのレベル 2 バックボーンへのアドバタイズを停止するように IS-IS レベル 1-2 境界ルータを設定します。
ステップ 18	**end**	特権 EXEC モードに戻ります。
ステップ 19	**show clns**	設定を確認します。
ステップ 20	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ルートの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。パスワードをディセーブルにするには、**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 アドレッシング、LSP リフレッシュ インターバル、LSP 存続時間、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、各コマンドの **no** 形式を使用します。出力形式をディセーブルにするには、**no partition avoidance** ルータ コンフィギュレーション コマンドを使用します。

IS-IS インターフェイス パラメータの設定

特定のインターフェイス固有の IS-IS パラメータは、接続された他のルータとは関係なく、任意に設定することができます。ただし、一部の値（乗数や間隔など）をデフォルトから変更する場合は、複数のルータおよびインターフェイスでもこれらを変更する必要があります。インターフェイス パラメータのほとんどは、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 レベルの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; サービス品質）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 間隔（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。IS-IS hello パケットで送信されるホールドタイムを判別するためにインターフェイスで使用されます。このホールドタイムによって、ネイバーがダウンしていると宣言されるまで、そのネイバが別の hello パケットを待機する時間が決定されます。また、ルートを再計算できるように、障害リンクまたはネイバーを検出する速度も決定されます。hello パケットが頻繁に失われ、IS-IS 隣接に無用な障害が発生する場合は、環境内の hello 乗数を変更してください。hello 乗数を大きくし、その分 hello 間隔を小さくすると、リンク障害を検出するための所要時間を増加させることなく、hello プロトコルの信頼性を高めることができます。
- その他の間隔：
  - Complete Sequence Number PDU（CSNP）間隔。CSNP は、データベースの同期を維持するために指定ルータから送信されます。
  - 再送信間隔。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 再送信スロットル間隔。IS-IS LSP をポイントツーポイント リンクで再送信する最大レート（パケット間のミリ秒数）です。この間隔は、*同じ* LSP の連続する再送信間隔である再送信間隔とは異なります。
- 指定ルータの選定優先度。このパラメータを使用すると、マルチアクセス ネットワークに必要な隣接数を削減できるため、ルーティング プロトコル トラフィック数やトポロジ データベースのサイズが削減されます。
- インターフェイス回路タイプ。指定されたインターフェイス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** コマンドを入力して、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）指定されたインターフェイスのメトリック（コスト）を設定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 10 です。レベルを入力しない場合は、デフォルト値がレベル 1 とレベル 2 の両方のルータに適用されます。

	コマンド	目的
ステップ 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**]	（任意）スイッチから送信される hello パケットの間隔を指定します。デフォルトでは、hello 間隔 *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 間隔が小さいほどトポロジ変更が短時間で検出されますが、ルーティング トラフィックは増大します。 • **minimal**：ホールドタイムが 1 秒になるように、hello 乗数に基づいて hello 間隔が計算されます。 • *seconds*：指定できる範囲は 1 ～ 65535 です。デフォルト値は 10 秒です。
ステップ 5	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**]	（任意）隣接装置がダウンしているとルータによって宣言されるまでに、ネイバーが失う IS-IS hello パケットの数を指定します。指定できる範囲は 3 ～ 1000 です。デフォルト値は 3 です。小さい hello 乗数を使用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ことがあります。
ステップ 6	**isis csnp-interval** *seconds* [**level-1** | **level-2**]	（任意）インターフェイスの IS-IS Complete Sequence Number PDU（CSNP）間隔を設定します。指定できる範囲は 0 ～ 65535 です。デフォルト値は 10 秒です。
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 の再送信間隔を秒単位で設定します。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値を指定する必要があります。指定できる範囲は 0 ～ 65535 です。デフォルト値は 5 秒です。
ステップ 8	**isis retransmit-throttle-interval** *milliseconds*	（任意）IS-IS LSP 再送信スロットル間隔を設定します。この間隔は、ポイントツーポイント リンクで IS-IS LSP を再送信する最大レート（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** コマンドによって決まります。
ステップ 9	**isis priority** *value* [**level-1** | **level-2**]	（任意）指定ルータの選定に使用する優先度を設定します。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のネイバーに必要な隣接タイプを設定します（インターフェイス回路タイプを指定します）。 • **level-1**：現在のノードとそのネイバーに共通のエリア アドレスが少なくとも 1 つ存在する場合に、レベル 1 隣接を確立します。 • **level-1-2**：ネイバーがレベル 1 およびレベル 2 の両方として設定されていて、共通のエリアが少なくとも 1 つ存在する場合に、レベル 1-2 隣接を確立します。共通のエリアが存在しない場合は、レベル 2 隣接が確立されます。これはデフォルトです。 • **level 2**：レベル 2 隣接を確立します。ネイバー ルータがレベル 1 ルータの場合は、隣接が確立されません。
ステップ 11	**isis password** *password* [**level-1** | **level-2**]	（任意）インターフェイス用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なっています。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 の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のデフォルトは、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*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ISO IGRP および IS-IS のモニタおよびメンテナンス

CLNS キャッシュの内容をすべて削除したり、特定のネイバーまたはルートの情報を削除したりすることができます。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 CLNS または IS-IS 統計情報を表示することができます。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 41-13 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の特権 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 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 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 41-13　ISO CLNS および 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エンド システム（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中継システム（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 ネットワークに関する情報を表示します。
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	ES ネイバー エントリを、関連付けられたエリアを含めて表示します。
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に関する CLNS 固有の情報または ES-IS 情報を表示します。
show clns neighbor	IS-IS ネイバーに関する情報を表示します。
show clns protocol	現在のルータの 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	現在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での宛先をすべて表示します。
show clns traffic	現在のルータが確認した CLNS パケットに関する情報を表示します。
show ip route isis	IS-IS 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 Shortest Path First（SPF）計算の履歴を表示します。
show isis topology	すべてのエリア内の接続されている全ルータ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 1 つのルート マップだけを表示します。
trace clns *destination*	ネットワーク内の指定された宛先までパケットがたど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

Virtual Private Network（VPN; 仮想私設網）を使用すると、カスタマーは ISP バックボーン ネットワーク上で帯域幅を安全に共有することができます。VPN は共通のルーティング テーブルを共有するサイトの集まりです。カスタマー サイトは、1 つまたは複数のインターフェイスによってサービス プロバイダー ネットワークに接続されます。サービス プロバイダーは、各インターフェイスを、VPN ルーティング/フォワーディング（VRF）テーブルと呼ばれる VPN ルーティング テーブルに関連付けます。

IE 3000 スイッチは、IP サービス イメージを稼動している場合、Customer Edge（CE; カスタマー エッジ）装置の複数の VPN ルーティング/フォワーディング（multi-VRF）インスタンスをサポートします（multi-VRF CE）。サービス プロバイダーは、multi-VRF CE により、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 をサポートするための Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は使用されません。MPLS VRF の詳細については、Cisco.com のホーム ページにアクセスして、『*Cisco IOS Switching Services Configuration Guide, Release 12.2*』を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

multi-VRF CE の概要

multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートして、VPN 間で IP アドレスを重複使用できるようにするための機能です。multi-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 つまたは複数のレイヤ 3 インターフェイスを各 VRF に関連付けることによっ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、物理インターフェイス（イーサネット ポートなど）と論理インターフェイス（VLAN SVI など）のどちらにもすることができますが、複数の VRF に属することはできません。

（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、次の装置が含まれます。

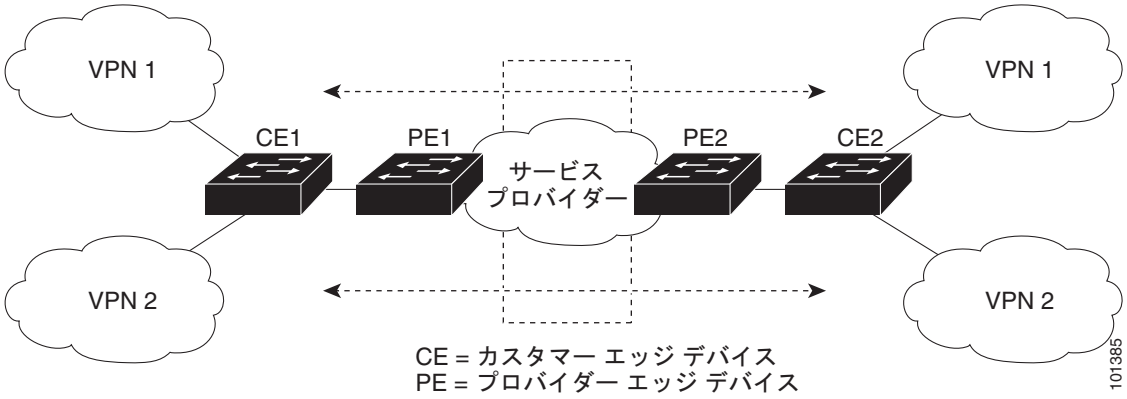
- カスタマー エッジ（CE）装置。この装置を使用すると、カスタマーは、1 つまたは複数のプロバイダー エッジ ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE 装置は、サイトのローカル ルートをルータにアドバタイズして、そこからリモート VPN ルートを学習します。IE 3000 スイッチは、CE に設定することができます。

- プロバイダー エッジ（PE）ルータ。このルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE 装置とルーティング情報を交換します。PE では、直接接続している VPN の VPN ルートを維持するだけでよいため、サービス プロバイダーのすべての VPN ルートを維持する必要はありません。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 内に存在する場合は、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、内部 BGP（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。これらは、CE 装置に接続していないサービス 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、複数のカスタマーが 1 つの CE を共有でき、CE と PE の間で物理リンクが 1 つだけ使用されます。CE を共有すると、各カスタマー用の個別の VRF テーブルが維持されます。パケットのスイッチングやルーティングは、独自のルーティング テーブルに基づいて、カスタマーごとに行われます。multi-VRF CE では、制限付きの PE 機能が CE 装置に拡張されます。これにより、VRF テーブルを個別に維持する機能が CE 装置に与えられるため、VPN のプライバシおよびセキュリティが支店にまで拡張されます。

図 41-6 に、IE3000 スイッチを複数の仮想 CE として使用した構成例を示します。このシナリオは、小規模な企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。この場合、IE3000 スイッチには multi-VRF CE のサポートが必要です。multi-VRF CE はレイヤ 3 機能であるため、VRF の各インターフェイスはレイヤ 3 インターフェイスにする必要があります。

図 41-6　　複数の仮想 CE として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、multi-VRF CE 関連のデータ構造内の VLAN ID と Policy Label（PL; ポリシー ラベル）の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

multi-VRF CE が設定されている場合、レイヤ 3 転送テーブルは次の 2 つのセクションに概念的に分割されます。

- multi-VRF CE ルーティング セクション。このセクションには、各 VPN からのルートが格納されます。
- グローバル ルーティング セクション。このセクションには、インターネットなど、非 VPN ネットワークへのルートが格納されます。

各 VRF の VLAN ID は別々のポリシー 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 設定機能は、学習した新しい 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、multi-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、ポートの内部 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 対応ネットワークでのパケット転送プロセスを次に示します。

- スイッチは、VPN からパケットを受信すると、入力ポリシー ラベル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、ラベルを削除し、そのラベルを使用して正しい 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装置に転送します。
- CE は、出力 PE からパケットを受信すると、入力ポリシー ラベルを使用して正しい 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、パケットを VPN 内で転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に関連付けられているレイヤ 3 インターフェイスを指定します。次に、VPN 内、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全体に VPN ルーティング情報を配信する場合は、ルーティング プロトコルとして BGP を使用することを推奨します。multi-VRF CE ネットワークでは、次の 3 つの主要コンポーネントを設定します。

- 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ーのリスト。VPN ルート ターゲットは、VPN コミュニティ メンバーごとに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ーに VRF 到達可能性情報を伝播します。VPN コミュニティ内のすべての PE ルータに 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 ネットワーク全体のすべての VPN コミュニティ メンバー間で、すべてのトラフィックを転送します。

multi-VRF CE のデフォルト設定

表 41-14 に、VRF のデフォルト設定を示します。

表 41-14　VRF 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。 ギガビット イーサネット スイッチ：12000。
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。

multi-VRF CE 設定時の注意事項

（注）　multi-VRF CE を使用するには、IP サービス イメージをスイッチにインストールする必要があります。

ネットワークに VRF を設定する場合は、次の点に注意してください。

- multi-VRF CE が設定されたスイッチは、複数のカスタマーによって共有されます。各カスタマーには、独自のルーティング テーブルが設定されます。
- 各カスタマーは別々の VRF テーブルを使用するため、同じ IP アドレスを再利用できます。各 VPN では、IP アドレスを重複使用できます。
- multi-VRF CE では、複数のカスタマーが、プロバイダー エッジ（PE）とカスタマー エッジ（CE）の間で同じ物理リンクを共有できます。複数の VLAN が設定されたトランク ポートでは、パケットがカスタマーごとに分離されます。各カスタマーには独自の VLAN が設定されます。
- multi-VRF CE では、一部の MPLS-VRF 機能がサポートされません（ラベル交換、LDP 隣接、ラベル付きパケットなど）。
- PE ルータでは、multi-VRF CE を使用した場合と複数の CE を使用した場合の違いはありません。図 41-6 では、複数の仮想レイヤ 3 インターフェイスが multi-VRF CE 装置に接続されています。
- スイッチでは、物理ポート、VLAN SVI、またはこれら両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートを介して接続することができます。
- カスタマーは、他のカスタマーと重複しない限り、複数の VLAN を使用できます。カスタマーの VLAN は、特定のルーティング テーブル ID にマッピングされます。この ID は、スイッチに格納されている適切なルーティング テーブルを識別するために使用されます。
- IE3000 スイッチは、1 つのグローバル ネットワークと最大 26 の VRF をサポートします。
- 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、次の理由により、外部 BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE との通信に複数のアルゴリズムを必要としない。
  - BGP は、さまざまな管理者によって稼動されているシステム間でルーティング情報を交換するように設計されている。
  - BGP では、ルートの属性を CE に簡単に送信できる。
- 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。
- multi-VRF CE 内のラインレート マルチキャスト転送がサポートされます。
- マルチキャスト VRF は、同じインターフェイスのプライベート VLAN とは共存できません。
- 最大 1000 のマルチキャスト ルートがサポートされ、すべての VRF で共有できます。
- VRF を設定しない場合は、105 のポリシーを設定できます。
- VRF が 1 つでも設定されている場合は、41 のポリシーを設定できます。
- ポリシーが 42 以上設定されている場合は、VRF を設定できません。
- VRF とプライベート VLAN は、相互に排他的な関係にあります。プライベート VLAN では、VRF をイネーブルにすることはできません。同様に、VLAN インターフェイスで VRF が設定されている VLAN では、プライベート VLAN をイネーブルにすることはできません。
- スイッチ インターフェイスでは、VRF と Policy-Based Routing（PBR; ポリシーベース ルーティング）は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにすることはできません。
- スイッチ インターフェイスでは、VRF と Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）は、相互に排他的な関係にあります。WCCP がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、WCCP をイネーブルにすることはできません。

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。コマンドの構文および使用方法の詳細については、このリリースに対応した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。
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て、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）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、エクスポート、またはインポートおよび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。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* には、ステップ 4 で入力した *route-distinguisher* と同じ値を指定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て、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。インターフェイスには、ルーテッド ポートまたは SVI を設定できます。
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）設定をコンフィギュレーション ファイルに保存します。

VRF を削除して、そのインターフェイスをすべて削除するには、**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。VRF からインターフェイスを削除するには、**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。

マルチキャスト VRF の設定

VRF テーブル内に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。コマンドの構文および使用方法の詳細については、このリリースに対応した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。

	コマンド	目的
ステップ 4	**rd** *route-distinguisher*	ルート識別子を指定して、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）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、エクスポート、またはインポートおよび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。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* には、ステップ 4 で入力した *route-distinguisher* と同じ値を指定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 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て、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。インターフェイスには、ルーテッド ポートまたは SVI を設定できます。
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。
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 関連レイヤ 3 インターフェイスで Protocol Independent Multicast（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）設定をコンフィギュレーション ファイルに保存します。

multi-VRF CE 内でのマルチキャストの設定に関する詳細については、『*Cisco IOS IP Multicast Configuration Guide, Release 12.4.*』を参照してください。

VRF 認識サービスの設定

IP サービスは、グローバル インターフェイス上に設定することができ、グローバル ルーティング インスタンス内で実行します。複数のルーティング インスタンスで実行するように拡張された IP サービスが VRF 認識です。システム内で設定された VRF は、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームとは独立したモジュールに実装されます。VRF とは、Cisco IOS における複数のルーティング インスタンスを表します。各プラットフォームがサポートする VRF 数にはそれぞれ制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、指定した VRF 内のホストに ping を実行することができる。
- アドレス解決プロトコル（ARP）エントリは個別の VRF で学習される。ユーザは特定の VRF の ARP エントリを表示できる。

次のサービスは VRF 認識です。

- ARP（アドレス解決プロトコル）
- ping
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）

- RADIUS
- Syslog
- traceroute
- FTP および TFTP

（注）　Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）の VRF 認識サービスはサポートされていません。

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。コマンドの構文および使用方法の詳細については、このリリースに対応した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。コマンドの構文および使用方法の詳細については、このリリースに対応した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。コマンドの構文および使用方法の詳細については、このリリースに対応した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 でのパケットの 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 トラップ動作の受信側、および SNMP トラップの送信に使用する 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 インフォーム動作の受信側、および SNMP インフォームの送信に使用する 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 アクセスで使用する VRF でのリモート 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。コマンドの構文および使用方法の詳細については、このリリースに対応した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**	物理インターフェイスの場合、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。
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。

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 サーバで AAA をイネーブルにする必要があります。スイッチでは、**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 コマンドがサポートされています（次の URL の『*Per VRF AAA Feature Guide*』を参照）。
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

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。コマンドの構文および使用方法の詳細については、このリリースに対応した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 メッセージの送信先 Syslog サーバのホスト アドレスを指定します。

	コマンド	目的
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ログ記録します。
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。コマンドの構文および使用方法の詳細については、このリリースに対応した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の VPN VRF 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 および TFTP を VRF 認識にするには、FTP/TFTP CLI をいくつか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ている 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に [t]ftp に通知します。この例では、VRF テーブルが宛先 IP アドレスを検索するために使用されます。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しません。つまり、VRF が送信元インターフェイスに設定されていなくても、そのインターフェイスの CLI を使用してパケットを特定のインターフェイスに送信することができます。

FTP 接続の送信元 IP アドレスを指定するには、**ip ftp source-interface** show mode 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、このコマンドの **no** 形式を使用します。

	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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

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。ここでは OSPF の設定について説明しますが、他のプロトコルでも手順は同じです。

（注）　VRF インスタンス内で実行する EIGRP ルーティング プロセスを設定する場合は、**autonomous-system** *autonomous-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、AS（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 ルーティングのイネーブル化、VPN 転送テーブルの指定を行い、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）隣接ステートの変更をログ記録します。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のネットワーク 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）設定をコンフィギュレーション ファイルに保存します。

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*	他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定して、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network** *network-number* **mask** *network-mask*	ネットワークとマスクを指定して、BGP の使用をアナウンスします。
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のネットワーク 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。

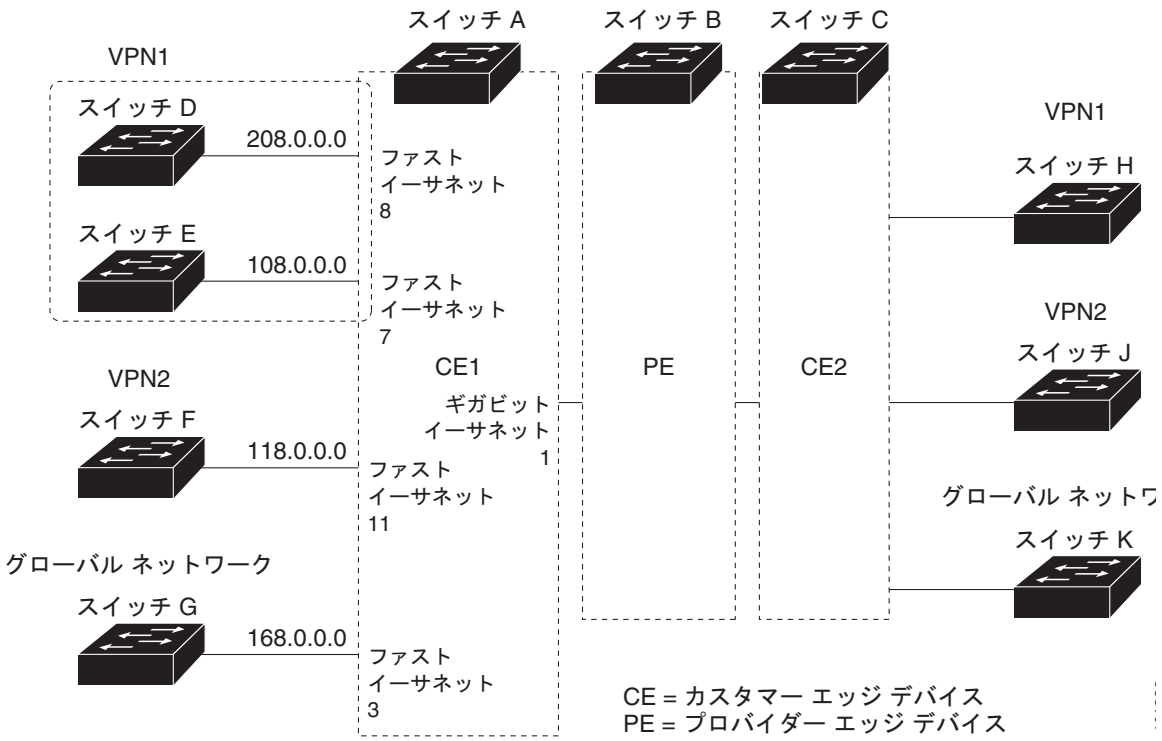
	コマンド	目的
ステップ 6	**address-family ipv4 vrf** *vrf-name*	PE/CE ルーティング セッションの BGP パラメータを定義して、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor** *address* **remote-as** *as-number*	PE と CE のルータ間の BGP セッションを定義します。
ステップ 8	**neighbor** *address* **activate**	IPv4 アドレス ファミリのアドバタイズをアクティブにします。
ステップ 9	**end**	特権 EXEC 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）設定をコンフィギュレーション ファイルに保存します。

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、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 41-7 は、図 41-6 とほぼ同じネットワークの物理接続を簡素化した例です。VPN1、VPN2、およびグローバル ネットワークでは、プロトコルに OSPF が使用されています。CE/PE 接続には BGP が使用されています。図のあとには、IE3000 スイッチを CE スイッチ A として設定し、カスタマー スイッチ D および F に対して VRF を設定する例を示します。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、内容はほぼ同じです。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 スイッチでのスイッチ A へのトラフィックを設定するためのコマンドも含まれています。

図 41-7　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て 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。ファスト イーサネット ポート 8 および 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 gigabitethernet1/5
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 fastethernet1/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config)# interface fastethernet1/11
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 および 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 および VPN2 の OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
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 vl2
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 ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
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 vl1
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 VPN1 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 fastethernet1/2
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 VPN2 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 fastethernet1/1
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

次のコマンドをスイッチ B（PE ルータ）に対して使用すると、CE 装置（スイッチ A）への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 gigabitthernet1/0.10
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 gigabitthernet1/0.10
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 のステータスの表示

multi-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 41-15 の特権 EXEC コマンドを使用します。

表 41-15　multi-VRF CE の情報を表示するためのコマンド

コマンド	目的
show ip protocols vrf *vrf-name*	VRF に関連付けられているルーティング プロトコルの情報を表示します。
show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に関連付けられている IP ルーティング テーブルの情報を表示します。
show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義済みの 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。

プロトコル独立機能の設定

ここでは、IP ルーティング プロトコル独立機能の設定方法について説明します。この章に記載されている 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.com のホーム ページにアクセスして、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocol-Independent Commands」を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

ここでは、次の設定情報について説明します。

- 「Cisco Express Forwarding の設定」（P.41-90）
- 「等価コスト ルーティング パスの個数の設定」（P.41-91）
- 「スタティック ユニキャスト ルートの設定」（P.41-92）
- 「デフォルトのルートおよびネットワークの指定」（P.41-93）
- 「ルート マップによるルーティング情報の再配信」（P.41-94）
- 「ポリシーベース ルーティングの設定」（P.41-97）
- 「ルーティング情報のフィルタリング」（P.41-101）
- 「認証キーの管理」（P.41-104）

Cisco Express Forwarding の設定

Cisco Express Forwarding（CEF）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 テクノロジーです。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 負荷が小さいため、より多くの CPU 処理能力をパケット転送に振り分けることができます。ダイナミック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、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF は、Forwarding Information Base（FIB; 転送情報ベース）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 の主要コンポーネントは、分散 FIB と分散隣接テーブルの 2 つです。

- FIB では、ルーティング テーブルや情報ベースと同様に、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 テーブルが更新され、その変更内容が FIB に反映されます。FIB では、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 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るため、CEF ではルート 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。
- ネットワーク内のノードがあるリンク層において 1 ホップだけで相互に到達可能な場合、そ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てレイヤ 2 アドレッシング情報を追加します。隣接テーブルには、すべての FIB エントリのレイヤ 2 ネクストホップ アドレスが格納されます。

スイッチは、ギガビット速度のラインレート IP トラフィックを達成するために Application Specific Integrated Circuit（ASIC; 特定用途向け集積回路）を使用するため、CEF 転送はソフトウェア転送パス（CPU によって転送されるトラフィック）にだけ適用されます。

デフォルトでは、CEF はグローバルにイネーブルになっています。何らかの理由でディセーブルになった場合は、**ip cef** グローバル コンフィギュレーション コマンドを使用すると、再度イネーブルにすることができます。

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 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 をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックを簡単にデバッグできます。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ための **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は、インターフェイス上で CEF をディセーブルにしないでください。

ディセーブルになっている CEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上で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**	CEF の動作をイネーブルにします。

	コマンド	目的
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	ソフトウェア転送トラフィック用のインターフェイスで 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。
ステップ 7	**show cef linecard** [**detail**]	CEF 関連のインターフェイス情報を表示します。
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 CEF 詳細情報を表示します。
ステップ 9	**show adjacency**	CEF 隣接テーブルの情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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ルータに複数存在する場合、これらのルートは等価コストであると見なされます。ルーティング テーブルに複数の等価コスト ルートが格納されている場合は、これらを*パラレル パス*と呼ぶこともあります。ネットワークへの等価コスト パスがルータに複数存在する場合、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、パスに障害が発生した場合でも冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散させて、使用可能な帯域幅を有効利用することもできます。

等価コスト ルートはルータによって自動的に学習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 32 の等価コスト ルートを使用できますが、スイッチ ハードウェアでは 1 ルートあたり 17 以上のパスは使用しません。

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。
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 プロトコルのデフォルト値は 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）設定をコンフィギュレーション ファイルに保存します。

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 ルートはユーザ定義のルートです。スタティック ユニキャスト ルートを使用すると、送信元と宛先の間のパケットの送受信が指定したパスによって行われるようになります。ルータが特定の宛先へのルートを作成できない場合、スタティック ルートが重要になる場合があります。スタティック ルートは、ルーティング不能なすべてのパケットの送信先であるラスト リゾート ゲートウェイを指定する場合に役立ちます。

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**	ルーティング テーブルの現在のステートを表示して、設定を確認します。
ステップ 5	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

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。

スイッチは、ユーザが削除するまでスタティック ルートを保持します。ただし、スタティック ルートは、管理ディスタンスの値を割り当てることによって、ダイナミック ルーティング情報で上書きすることができます。各ダイナミック ルーティング プロトコルには、デフォルトの管理ディスタンスが設定されています（表 41-16 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 ルートの管理ディスタンスがダイナミック ルーティング プロトコルの管理ディスタンスよりも大きくなるように設定します。

表 41-16　ダイナミック ルーティング プロトコルのデフォルトの管理ディスタンス

ルート送信元	デフォルトのディスタンス
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
拡張 IGRP サマリー ルート	5
外部 BGP	20
内部拡張 IGRP	90
IGRP	100
OSPF	110
内部 BGP	200
不明	225

インターフェイスをポイントするスタティック 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 プロトコルによっ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、ルーティング テーブルでは、インターフェイスをポイントするスタティック ルートが接続されると、そのスタティックな性質が失われたと見なされるためです。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 ルートを定義した場合は、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限り、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、その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。転送ルータのアドレスとして指定されたアドレスの有効なネクストホップがスタティック ルート内に見つからなくなった場合は、そのスタティック ルートも IP ルーティング テーブルから削除されます。

デフォルトのルートおよびネットワークの指定

ルータが他のすべてのネットワークへのルートを学習することはできません。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 ルートにスマート ルータを指定します（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、ダイナミックに学習されるか、ルータごとに設定されます。内部ダイナミック ルーティング プロトコルのほとんどは、スマート ルータを使用して生成したダイナミックなデフォルト情報を他のルータに転送するメカニズムを備えています。

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、その装置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。

ネットワーク用のデフォルトを生成しているルータでは、自身のデフォルト ルートが必要になる場合があります。ルータが自身のデフォルト ルートを生成する方法の 1 つとして、適切な装置を経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定する方法があります。

ネットワークへのスタティック ルートをスタティック デフォルト ルートとして定義するには、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**	ラスト リゾート ゲートウェイ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）設定をコンフィギュレーション ファイルに保存します。

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 プロトコルでデフォルト情報を送信する場合、これ以外の設定は必要ありません。ルーティング テーブルは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場合があります。Cisco ルータでは、管理ディスタンスとメトリック情報を使用して、デフォルト ルートやラスト リゾート ゲートウェイを設定します。

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 コマンドを使用して、デフォルト ルートの候補を指定します。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れば、そのネットワークは候補の 1 つと見なされ、最適なデフォルト パスへのゲートウェイがラスト リゾート 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することができます。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、一致する必要がある基準を指定するコマンドです。**set** コマンドは、ルーティング アップデートが match コマンドで定義された条件を満たす場合に実行されるアクションを指定します。再配信はプロトコル独立機能ですが、**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に固有のものです。

match コマンドおよび **set** コマンドは、**route-map** のあとにそれぞれ 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、条件がすべて満たされていると見なされます。**set** コマンドを指定しない場合、match コマンド以外の処理は実行されません。このため、**match** または **set** コマンドを少なくとも 1 つ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 コマンドが指定されていないルート マップは CPU に送られるため、CPU 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** として指定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 コマンドが適用されます。一致基準を満たしてないパケットは、通常のルーティング チャネルを通じて転送されます。

match コマンドと set コマンドによるエントリの実行が成功すると、BGP ルート マップ **continue** コマンドを使用して、ルート マップの追加エントリを実行できます。**continue** コマンドを使用すると、より多くのモジュラー ポリシー定義を設定および構成できるため、特定のポリシーを同じルート マップ内で繰り返し設定する必要がなくなります。スイッチは、発信ポリシーの **continue** コマンドをサポートしています。ルート マップの **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 IOS Release 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*]	再配信の制御に使用するルート マップを定義して、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。 *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対象のルート マップを参照します。複数のルート マップで同じマップ タグ名を共有することもできます。 （任意）**permit** が指定され、このルート マップの一致基準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。 *sequence number*（任意）：同じ名前ですでに設定されているルート マップのリスト内に設定される、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 as-path** *path-list-number*	BGP AS 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て、標準アクセス リストと一致させます。番号には、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 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 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。それぞれ、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のアクセス リストによって指定されるアドレスと一致させます。
ステップ 11	**match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**]}	指定された **route-type** と一致させます。 • **local**：ローカルに生成された BGP ルート。 • **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。 • **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 ダンプニングの各要素を設定します。
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。

	コマンド	目的
ステップ 14	**set origin** {**igp** | **egp** *as* | **incomplete**}	BGP 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のエリアです。
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）。 • *bandwidth*：0 ～ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅（Kbps 単位）。 • *delay*：0 ～ 4294967295 の範囲のルート遅延（10 マイクロ秒単位）。 • *reliability*：パケット送信の成功可能性。0 ～ 255 の数値で表され、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。 • *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）。 • *mtu*：ルートの最大伝送ユニット（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、外部 BGP ネイバーにアドバタイズされるプレフィクスの 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 のウェイトを設定します。指定できる値の範囲は、1 ～ 65535 です。
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**	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 24	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、ルートの再配信を制御したりすることができます。

ルートの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、上記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。
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。route-map を指定しない場合、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が使用され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 プロトコルで、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が使用され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**	設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

再配信をディセーブルにするには、このコマンドの **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は、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、設定したメトリックを再配信されたルートに割り当てます。さまざまなルーティング プロトコル間でルーティング情報を制御せずに交換すると、ルーティング ループが発生し、ネットワークの動作が著しく低下することもあります。

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メトリック変換が行われることもあります。

- RIP はスタティック ルートを自動的に再配信することができます。スタティック ルートのメトリックには 1（直接接続）が割り当てられます。
- デフォルト モードが有効になっている場合、どのプロトコルでも他のルーティング プロトコルを再配信することができます。

ポリシーベース ルーティングの設定

ポリシーベース ルーティング（PBR）を使用すると、トラフィック フローの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小さくします。PBR では、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 ポリシーを指定したり、実装したりすることができます。

- 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、等価アクセスおよび送信元依存のルーティング、対話形式とバッチ トラフィックに基づくルーティング、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高帯域幅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 データは低帯域幅で低コストのリンクで送信することができます。

PBR を使用する場合は、Access Control List（ACL; アクセス制御リスト）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。パケットは、ルート マップで定義された基準に基づいて、適切なネクストホップに転送（ルーティング）されます。

- パケットがどのルート マップ ステートメントとも一致しない場合は、すべての set コマンドが適用されます。
- 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ていません。

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.41-94）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 の一致基準を指定することができます。このプロセスは、一致が見つかるまでルート マップを介して行われます。一致が見つからない場合は、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、暗黙的な拒否エントリがあります。

match コマンドの条件が満たされた場合は、set コマンドを使用して、パス内のネクストホップ ルータを識別する IP アドレスを指定することができます。

PBR の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。スイッチ プロンプトで疑問符を入力した場合に表示されるにもかかわらず、このスイッチでサポートされない PBR コマンドのリストについては、付録 C「Cisco IOS Release 12.2(55)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。

（注） このソフトウェア リリースでは、IPv4 および IPv6 のトラフィックを処理する場合の PBR はサポートされていません。

PBR 設定時の注意事項

PBR を設定するときには、次の点に注意してください。

- PBR を使用するには、IP サービス イメージをスイッチにインストールする必要があります。
- マルチキャスト トラフィックに対しては、ポリシーによるルーティングは行われません。PBR は、ユニキャスト トラフィックに対してだけ適用されます。
- PBR は、ルーテッド ポートまたは SVI 上でイネーブルにできます。
- スイッチでは、PBR の **route-map deny** ステートメントはサポートされていません。
- 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。
- スイッチでは、最大 246 の IP ポリシー ルートマップを定義できます。

- スイッチでは、最大 512 の Access Control Entry（ACE; アクセス制御エントリ）を PBR 用に定義できます。
- ルート マップ内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 と一致させないでください。PBR はこれらのパケットを転送するため、ping または Telnet が失敗したり、ルート プロトコルのフラッピングが発生したりする可能性があります。
  - 拒否 ACE を含む ACL と一致させないでください。拒否 ACE と一致するパケットは CPU に送られるため、CPU 使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。VLAN またはデフォルトのテンプレートでは、PBR 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 10 章「SDM テンプレートの設定」を参照してください。
- スイッチ インターフェイスでは、VRF と PBR は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、VRF をイネーブルにすることはできません。その逆も同様で、VRF がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにはできません。
- スイッチ インターフェイスでは、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）と PBR は、相互に排他的な関係にあります。PBR がインターフェイスでイネーブルになっている場合は、WCCP をイネーブルにすることはできません。その逆も同様で、WCCP がインターフェイスでイネーブルになっている場合は、PBR をイネーブルにはできません。
- PBR で使用される ternary content addressable memory（TCAM; 三値連想メモリ）のエントリの数は、ルート マップ自体、使用される ACL、ACL とルート 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 に基づくポリシーベース ルーティングはサポートされていません。有効な set アクションが設定されていないポリシー マップ、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、サポートされません。
- スイッチでは、サービス品質（QoS）DSCP および PBR ルート マップ内で一致する IP precedence がサポートされています。ただし、次の制限事項があります。
  - QoS 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することはできません。
  - DSCP の透過性と PBR DSCP ルート マップを同じスイッチに設定することはできません。
  - PBR を QoS DSCP とともに設定すると、QoS をイネーブルに設定（**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）することも、ディセーブルに設定（**no mls qos** コマンドを入力）することもできます。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に入るポートの DSCP 信頼状態を設定する必要があります。信頼状態が DSCP 以外の場合、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の DSCP 値が 0 に設定されます。

PBR のイネーブル化

デフォルトでは、スイッチの PBR はディセーブルになっています。PBR をイネーブルにするには、一致基準および match コマンドとすべて一致した場合のアクションを指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match コマンドと一致したものはすべて PBR の対象になります。

PBR の高速スイッチングや実装は、スイッチの速度を低下させない速度で行うことができます。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、事前に PBR をイネーブルにしておく必要があります。デフォルトでは、PBR の高速スイッチングは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（ローカル パケット）に対しては、通常のポリシー ルーティングは行われません。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。デフォルトでは、ローカル PBR はディセーブルになっています。

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*]	パケットの出力場所の制御に使用するルート マップを定義して、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。 • *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 タグ名を共有することもできます。 • （任意）**permit** が指定され、このルート マップの一致基準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。 **（注）** インターフェイスに適用される PBR ルート マップでは、**route-map deny** ステートメントはサポートされません。 • *sequence number*（任意）: 同じ名前で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 つまたは複数の標準または拡張アクセス リストで許可されている、送信元および宛先の IP アドレスを一致させます。 **（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。 **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。
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アクションを指定します。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る必要があります）。
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	**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。

	コマンド	目的
ステップ 7	**ip policy route-map** *map-tag*	レイヤ 3 インターフェイスの PBR をイネーブルにして、使用するルート マップを指定します。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、シーケンス番号が異なる複数のルート マップ エントリを設定することができます。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。 **（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場合、設定が失敗します。
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）ローカル PBR をイネーブルにして、スイッチから送信されるパケットに対してポリシーベース ルーティングを実行します。ローカル PBR は、スイッチで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）設定されたすべてのルート マップ、または指定された 1 つのルート マップだけを表示して、設定を確認します。
ステップ 13	**show ip policy**	（任意）インターフェイスに適用されたポリシー 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 ポリシー ルーティングがイネーブルになっているかどうかを表示します。イネーブルになっている場合は、使用されているルート マップが表示されます。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。インターフェイスの 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たパケットに対するポリシーベース ルーティング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には、次の手順を実行します。

（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ルートをダイナミックに学習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いようにします。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、指定されたルータ インターフェイスに対して送受信されません。

インターフェイスが多数存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を省くためには、**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隣接関係が必要なインターフェイスを手動で設定し、すべてのインターフェイスがデフォルトでパッシブになるように設定します。

パッシブ 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。
ステップ 3	**passive-interface** *interface-id*	指定されたレイヤ 3 インターフェイスによるルーティング 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）設定をコンフィギュレーション ファイルに保存します。

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 モニタ用特権 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 コマンドを使用して、隣接関係を必要とする各インターフェイスを設定します。**default** キーワードは、多くの配信ルータに 200 を超えるインターフェイスが備えられ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

distribute-list ルータ コンフィギュレーション コマンドをアクセス制御リストと組み合わせて使用すると、ルーティング アップデートにおける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学習しないようにすることができます。この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定することができません。

distribute-list ルータ コンフィギュレーション コマンドを使用すると、着信アップデートにリストされている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 には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** | **eigrp**}	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	**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ている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）設定をコンフィギュレーション ファイルに保存します。

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。アップデートにおけるネットワーク アドバタイズ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

ルーティング情報には他の情報よりも正確なものもあるため、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の優先付けを行うことができます。*管理ディスタンス*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。大規模なネットワークでは、他のルーティング プロトコルよりも信頼性が高いルーティング プロトコルが存在する場合があります。管理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。ルータは常に、ルーティング プロトコルの管理ディスタンスが最短のルートを選択します。表 41-16（P.41-92）に、各ルーティング情報の送信元のデフォルトの管理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、管理ディスタンスの割り当てにおける全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。
ステップ 3	**distance** *weight* {*ip-address* {*ip-address mask*}} [*ip access list*]	管理ディスタンスを定義します。 *weight*：管理ディスタンスは 10 ～ 255 の整数です。単独で使用する場合、*weight* はデフォルトの管理ディスタンスを示します。ルーティング情報の送信元として他に指定されているものがない場合に使用されます。管理ディスタンスが 255 のルートは、ルーティング テーブルに格納されません。 （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。

	コマンド	目的
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管理ディスタンスを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

管理ディスタンスの定義を削除するには、**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

キーの管理は、ルーティング プロトコルで使用される認証キーを制御する方法です。一部のプロトコルでは、キーの管理を使用することができません。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には、認証をイネーブルにする必要があります。プロトコルの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と各キーの有効期間を指定します。各キーには、ローカルに格納される固有のキー ID が設定されます（**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）。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個数に関係なく、1 つの認証パケットだけが送信されます。キー番号は小さい方から大きい方へ順に調べられ、最初に見つかった有効なキーが使用されます。キーの変更中は、存続時間が重なっても問題ありません。これらの存続時間は、ルータで認識されている必要があります。

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 チェーンを指定して、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*	キー番号を指定します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string** *text*	キー文字列を指定します。キー文字列には 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することはできません。
ステップ 5	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの受信可能期間を指定します。 *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。

	コマンド	目的
ステップ 6	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	（任意）キーの送信可能期間を指定します。 *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**	認証キーの情報を表示します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。ルートの消去やステータスの表示を行うには、表 41-17 に示す特権 EXEC コマンドを使用します。

表 41-17　IP ルートの消去またはルート 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消去します。
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。
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 1 つのルート マップだけを表示します。