CHAPTER 35

IP ユニキャスト ルーティングの設定

この章では、スイッチで IP Version 4（IPv4）ユニキャスト ルーティングを設定する方法について説明します。スイッチは、スタティック ルーティングや Routing Information Protocol（RIP）などの基本的なルーティング機能をサポートしています。

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

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

この章で説明する内容は、次のとおりです。

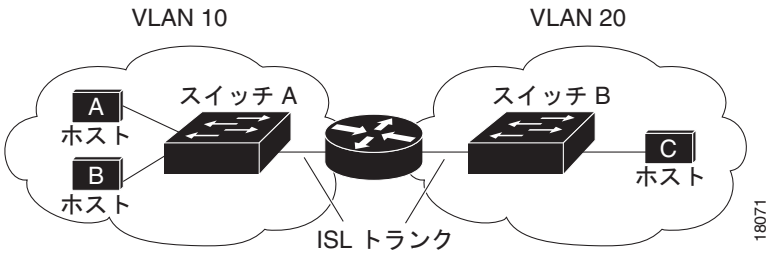
（注） スイッチにルーティング パラメータを設定する場合、使用できるユニキャスト ルート数が最大となるようにシステム リソースを割り当てるには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用し、ルーティング テンプレートに Switch Database Management（sdm）機能を設定します。SDM テンプレートの詳細については、第 6 章「SDM テンプレートの設定」、またはこのリリースのコマンド リファレンスの **sdm prefer** コマンドを参照してください。

IP ルーティングの概要

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

図 35-1 に基本的なルーティング トポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。

図 35-1　　ルーティング トポロジの例



VLAN10 内のホスト A が VLAN10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN20 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 VLAN10 インターフェイスでトラフィックを受信します。ルータはルーティング テーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

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

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

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しないため、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。

ルータはダイナミック ルーティング プロトコルを使用して、トラフィックを転送するのに最適なルートをダイナミックに計算します。ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトル プロトコルは 1 つ以上のメトリックを使用し、最適なルートを計算します。これらのプロトコルは簡単に設定して使用できます。

スイッチは単一の距離メトリック（コスト）を使用して、最適パスを決定する Routing Information Protocol（RIP）のみをサポートしています。デフォルト ルーティングとスタティック ルーティングもサポートしています。

ルーティングを設定する手順

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

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

- ルーテッド ポート：**no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポート
- 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。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネル グループにバインドして作成されたポート チャネル論理インターフェイス 詳細については、「レイヤ 3 EtherChannel の設定」（P.34-13）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.35-5）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。ソフトウェアに、設定できるルーテッド ポートおよび SVI の個数制限はありません。ただし、ハードウェアによって制限されるため、設定できるルーテッド ポートおよび SVI の数と、実装されている機能の数と量の相互関係によっては、CPU 使用率が影響を受けることがあります。システム メモリをルーティング用に最適化するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用します。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチで 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 12 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 アドレス指定の設定

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

アドレス指定のデフォルト設定

表 35-1 に、アドレス指定のデフォルト設定を示します。

表 35-1　アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義。
ARP	アドレス解決プロトコル（ARP）キャッシュに永続的なエントリはありません。 カプセル化：標準イーサネット形式の ARP。 タイムアウト：14400 秒（4 時間）。
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）
IP クラスレス ルーティング	イネーブル。
IP デフォルト ゲートウェイ	ディセーブル。
IP 指定ブロードキャスト	ディセーブル（すべての IP 指定ブロードキャストが廃棄されます）。
IP ドメイン	ドメイン リスト：ドメイン名は未定義。 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、または 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 転送がイネーブルとなります。 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。

表 35-1　アドレス指定のデフォルト設定 （続き）

機能	デフォルト設定
IP ホスト	ディセーブル。
ICMP Router Discovery Protocol（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 アドバタイズメント • アドバタイズメント間の最大インターバル：600 秒 • アドバタイズメント間の最小インターバル：最大インターバルの 0.75 倍 • 初期設定：0
IP プロキシ ARP	イネーブル。
IP ルーティング	ディセーブル。
IP サブネットゼロ	ディセーブル。

ネットワーク インターフェイスへの IP アドレスの割り当て

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

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクは、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）コンフィギュレーション ファイルに設定を保存します。

サブネット ゼロの使用

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

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

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

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

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

クラスレス ルーティング

スイッチがルーティングを行うように設定されている場合、クラスレス ルーティング動作はデフォルトでイネーブルになっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛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ションするために使用されるクラス C アドレス スペースの連続ブロックから構成され、クラス B アドレス スペースの急速な枯渇を回避するために設計されました。

図 35-2 では、クラスレス ルーティングがイネーブルとなっています。ホストがパケットを 120.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛パケットを受信したルータは、パケットを廃棄します。

図 35-2　IP クラスレス ルーティングがイネーブルの場合

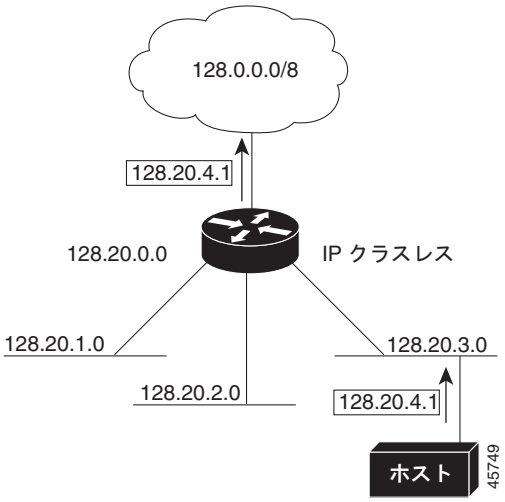
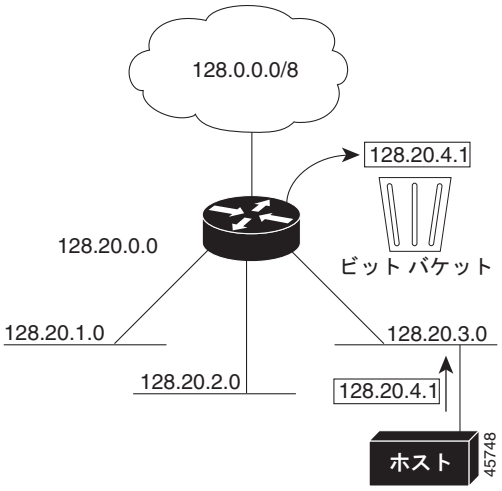


図 35-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ストがパケットを 120.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 35-3　IP クラスレス ルーティングがディセーブルの場合



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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip classless**	クラスレス ルーティング動作をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

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

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

アドレス解決方法の設定

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

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

スイッチでは次の形式のアドレス解決を使用できます。

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

スイッチでは、ARP と同様の機能（逆アドレス解決プロトコル（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）を持つ RARP を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server** *address* インターフェイス コンフィギュレーション コマンドを使用します。

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

アドレス解決を設定するために必要な作業は次のとおりです。

- 「スタティック ARP キャッシュの定義」（P.35-9）
- 「ARP カプセル化の設定」（P.35-10）
- 「プロキシ ARP のイネーブル化」（P.35-10）

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 アドレス間を動的にマッピングできます。ほとんどのホストでは動的なアドレス解決がサポートされているため、通常スタティック 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。それにより、IP アドレスを MAC アドレスに変換するためにスイッチによって使用される永続的なエントリが、ARP キャッシュにインストールされます。任意で、指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**arp** *ip-address hardware-address type*	ARP キャッシュ内で IP アドレスを MAC（ハードウェア）アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。 • **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（SNAP）カプセル化（トークンリングおよび FDDI インターフェイス用） • **sap**：HP の ARP タイプ
ステップ 3	**arp** *ip-address hardware-address type* [*alias*]	（任意）指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 5	**arp timeout** *seconds*	（任意）ARP キャッシュ エントリがキャッシュに保持される期間を設定します。デフォルトは 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）コンフィギュレーション ファイルに設定を保存します。

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

ARP カプセル化の設定

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	**arp** {**arpa** | **snap**}	ARP カプセル化方法を指定します。 • **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）コンフィギュレーション ファイルに設定を保存します。

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

プロキシ ARP のイネーブル化

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

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

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

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

IP ルーティングがディセーブルの場合のルーティング支援機能

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

プロキシ ARP

プロキシ ARP は、他のルートを取得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 アドレスを判別できると想定されています。送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを評価します。最適なルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信し、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設定されています。ディセーブル化されたプロキシ ARP をイネーブルにするには、「プロキシ ARP のイネーブル化」（P.35-10）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機能します。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行うか、IP Control Message Protocol（ICMP）リダイレクト メッセージを送信して、ホストが使用する必要があるローカル 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。この方法の欠点は、デフォルトのルータが停止状態になるか、使用できなくなった場合に、検出方法がないことです。

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）コンフィギュレーション ファイルに設定を保存します。

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

ICMP Router Discovery Protocol（IRDP）

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

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

インターフェイスで IRDP ルーティングを行う場合に必要な作業は、インターフェイスで IRDP 処理をイネーブルにすることだけです。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータは必要に応じて変更できます。

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**	インターフェイス上で IRDP 処理をイネーブルにします。
ステップ 4	**ip irdp multicast**	（任意）IP ブロードキャストの代わりとして、マルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズメントを送信します。 **（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必要があるサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 5	**ip irdp holdtime** *seconds*	（任意）アドバタイズメントが有効である IRDP 期間を設定します。デフォルトは **maxadvertinterval** 値の 3 倍です。**maxadvertinterval** 値よりも大きい値（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）アドバタイズメント間の IRDP の最大インターバルを設定します。デフォルトは 600 秒です。
ステップ 7	**ip irdp minadvertinterval** *seconds*	（任意）アドバタイズメント間の 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、この値は新しいデフォルト値（**maxadvertinterval** の 0.75 倍）に変更されます。
ステップ 8	**ip irdp preference** *number*	（任意）デバイスの IRDP 初期設定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。大きい値を設定すると、ルータの初期設定レベルも高くなります。

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

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

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

ブロードキャスト パケットの処理方法の設定

IP インターフェイス アドレスを設定した後で、ルーティングをイネーブルにしたり、1 つ以上のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛のデータ パケットです。スイッチでは、次の 2 種類のブロードキャストがサポートされています。

- 指定ブロードキャスト パケットは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。指定ブロードキャスト 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 パケットは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 24 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 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームが伝播されます。ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。現在のほとんどの IP 実装では、ブロードキャスト アドレスとして使用するアドレスを設定できます。スイッチ内の実装機能をはじめ、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ス方式が複数サポートされています。

これらの方式をイネーブルにするには、次に示す作業を実行します。

- 「指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化」（P.35-13）
- 「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.35-15）
- 「IP ブロードキャスト アドレスの確立」（P.35-16）
- 「IP ブロードキャストのフラッディング」（P.35-16）

指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP 指定ブロードキャストは廃棄されるため、転送されません。IP 指定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場合、インターフェイスでは IP 指定ブロードキャストの転送をイネーブルにできます。**ip forward-protocol** グローバル コンフィギュレーション コマンドを使用して設定されたプロトコルだけが転送されます。

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 リストで許可されている IP パケットだけを、指定ブロードキャストから物理ブロードキャストに変換できます。アクセス リストの詳細については、第 32 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 指定ブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip directed-broadcast** [*access-list-number*]	インターフェイス上で、指定ブロードキャストから物理ブロードキャストへの変換を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 リストによって許可された IP パケットだけが変換可能となります。 （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 VPN Routing and Forwarding（VRF; VPN ルーティング/転送）インターフェイスで設定でき、VRF 認識です。指定ブロードキャスト トラフィックが VRF 内でだけルーティングされます。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルおよびポートを指定します。 • **udp**：UDP 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**：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**	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

UDP ブロードキャスト パケットおよびプロトコルの転送

ユーザ データグラム プロトコル（UDP）は TCP と同様に IP のホスト間レイヤ プロトコルです。UDP は、2 つのエンド システム間で、オーバーヘッドの小さいコネクションレスのセッションを提供しますが、受信されたデータグラムの確認応答は行いません。ネットワーク ホストは時により UDP ブロードキャストを使用し、アドレス、設定、および名前に関する情報を検索することがあります。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、UDP ブロードキャストが通常通りに転送されないことがあります。この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、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。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と 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*』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP 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）情報を伝達します。

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

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

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

IP ブロードキャスト アドレスの確立

（デフォルトの）最も一般的な IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレスです（255.255.255.255）。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

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

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

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

IP ブロードキャストのフラッディング

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

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

フラッディングを行う場合、パケットは次の条件を満たす必要があります（これらの条件は、IP ヘルパー アドレスを使用してパケットの転送を考慮する場合の条件と同じであることに注意してください）。

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

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスを設定します。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内を伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値は 1 つずつ減らされます。

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出される（場合によっては宛先アドレスが変更される）と、その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、UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

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

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

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

スパニング ツリーベースのフラッディングを向上させるには、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、UDP データグラムのフラッディングを高速化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

IP アドレスの監視およびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になった場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を消去できます。表 35-2 に、内容を消去するために使用するコマンドを示します。

表 35-2　キャッシュ、テーブル、データベースをクリアするコマンド

コマンド	目的
clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。
clear host {*name* | *}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {*network* [*mask*] |*}	IP ルーティング テーブルから 1 つ以上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、およびデータベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティング パスなど、特定の統計情報を表示できます。表 35-3 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 35-3　キャッシュ、テーブル、データベースを表示するコマンド

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

IP ユニキャスト ルーティングのイネーブル化

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします

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

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

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

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

RIP の設定

Routing Information Protocol（RIP）は、小規模な同種ネットワーク間で使用するために作成された 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 ユーザ データグラム プロトコル（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。このプロトコルは RFC 1058 に規定されています。RIP の詳細については、『*IP Routing Fundamentals*』（Cisco Press 刊）を参照してください。

（注） RIP は、スイッチでサポートされる唯一のルーティング プロトコルです。

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

RIP では、異なる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、ルート内で経由できるルータ数です。直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークには到達できません。この範囲が小さい（0 ～ 15）ため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルト ネットワークが RIP によって取得された場合、またはルータが最終ゲートウェイで、RIP

がデフォルト メトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しないと、RIP アップデート中にアドバタイズされません。

ここでは、次の設定情報について説明します。

RIP のデフォルト設定

表 35-4 に、RIP のデフォルト設定を示します。

表 35-4　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 の起動	**version** ルータ コンフィギュレーション コマンドに準拠。
IP スプリット ホライズン	メディアにより異なる。
Neighbor	未定義。
ネットワーク	指定なし。
オフセット リスト	ディセーブル。
出力遅延	0 ミリ秒。
タイマー基準	• update：30 秒。 • invalid：180 秒。 • holddown：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 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

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

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

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

	コマンド	目的
ステップ 10	**no validate-update-source**	（任意）着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の環境で、この機能をディセーブルにすることはお勧めしません。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）送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなる RIP アップデートのパケットには、パケット間の遅延は追加されません。パケットを低速なデバイスに送信する場合は、8 ～ 50 ミリ秒の範囲でパケット間遅延を追加できます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip protocols**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

RIP 認証の設定

RIP バージョン 1 では、認証がサポートされていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キー チェーンによって指定されます。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。「認証鍵の管理」（P.35-39）に記載されている作業も実行してください。

スイッチは、RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードをサポートします。デフォルトはプレーン テキストです。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip rip authentication key-chain** *name-of-chain*	RIP 認証をイネーブルにします。
ステップ 4	**ip rip authentication mode** [**text** | **md5**}	プレーン テキスト認証（デフォルト）または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** [*interface-id*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を防止するには、**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発信元である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、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。

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

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカルな 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である場合、自動サマリーと IP サマリー アドレス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、インターフェイスのスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

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

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

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイスのギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスが

まだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

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

```
Switch(config)# router rip
Switch(config-router)# interface gi0/2
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 ホライゾンの設定

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発信元である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、アプリケーションでスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

インターフェイスでスプリット ホライズンをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよび IP サブネットを設定します。
ステップ 4	**no ip split-horizon**	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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。

スタブ ルーティングの設定

スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を軽減します。スイッチでは、Protocol-Independent Multicast（PIM）スタブ ルーティングと Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティングがサポートされます。

スタブ ルーティングについては、次のセクションで説明します。

PIM スタブ ルーティングの概要

PIM スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を軽減します。PIM スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートだけが PIM スタブ ルーティングを設定しているスイッチを通過します。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメインに接続されるか、他のレイヤ 2 デバイスを接続先とするインターフェイスに接続されます。直接接続されるマルチキャスト（IGMP）受信者と送信元だけが、レイヤ 2 アクセス ドメイン内で許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットの送信や処理を行いません。

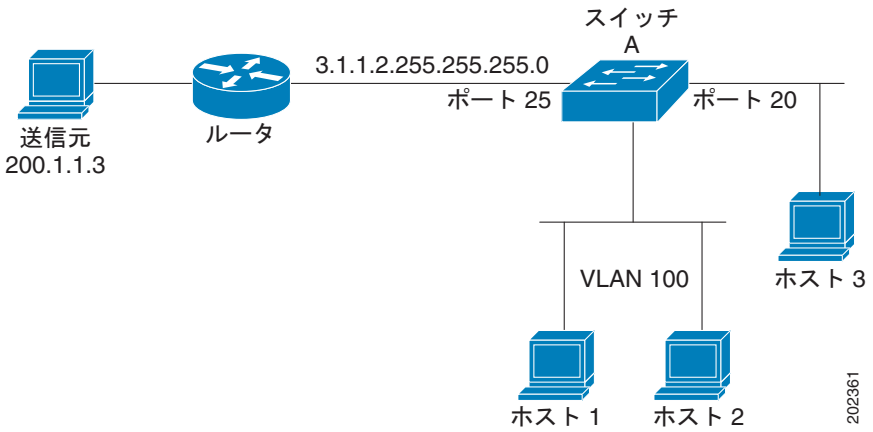
PIM スタブ ルーティングを使用する場合、IP マルチキャスト ルーティングを使用するように分散ルータとリモート ルータを設定し、スイッチだけを PIM スタブ ルータとして設定する必要があります。スイッチは、分散ルータ間で中継トラフィックをルーティングしません。また、スイッチにルーテッド アップリンク ポートを設定する必要があります。スイッチ アップリンク ポートは SVI では使用できません。

スイッチに PIM スタブ ルーティングを設定する場合は、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「EIGRP スタブ ルーティングの概要」（P.35-28）および「EIGRP スタブ ルーティングの設定」（P.35-29）を参照してください。

冗長 PIM スタブ ルータ トポロジはサポートされません。マルチキャスト トラフィックをシングル アクセス ドメインにフォワーディングする PIM ルータが複数存在すると、冗長トポロジになります。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能は、非冗長アクセス ルータ トポロジだけをサポートします。非冗長トポロジを使用することで、PIM 受動インターフェイスは自身がアクセス ドメイン上の唯一のインターフェイスで指定ルータであると想定します。

図 35-4 では、スイッチ A ルーテッド アップリンク ポート 25 はルータに接続されています。PIM スタブ ルーティングは VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定では、直接接続されたホストはマルチキャスト送信元 200.1.1.3 からのトラフィックを受信できます。詳細については、「PIM スタブ ルーティングの設定」（P.35-26）を参照してください。

図 35-4　PIM スタブ ルータ設定



PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。アップリンク PIM インターフェイスと PIM 受動インターフェイスの 2 種類の PIM インターフェイスをサポートします。PIM パッシブ モードで設定されたルーテッド インターフェイスは、PIM 制御トラフィックを送信せず、転送しません。IGMP トラフィックだけを送信し、転送します。

PIM スタブ ルーティング設定の概要

インターフェイスで PIM スタブ ルーティングをイネーブルにするときは、次の注意事項に従ってください。

- PIM スタブ ルーティングを設定する前に、スタブ ルータとセントラル ルータ両方に IP マルチキャスト ルーティングを設定する必要があります。また、スタブ ルータのアップリンク インターフェイスで PIM モード（Dense-Mode（DM）、Sparse-Mode（SM）、または Dense-Sparse-Mode（SM-DM））を設定する必要があります。
- PIM スタブ ルータは、分散ルータの間で中継トラフィックをルーティングしません。ユニキャスト（EIGRP）スタブ ルーティングがこの動作を実行します。PIM スタブ ルータの動作を支援するようユニキャスト スタブ ルーティングを設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」（P.35-29）を参照してください。
- 直接接続されるマルチキャスト（IGMP）受信者と送信元だけが、レイヤ 2 アクセス ドメイン内で許可されます。PIM プロトコルはアクセス ドメインではサポートされません。
- 冗長 PIM スタブ ルータ トポロジはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ 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。この手順は任意です。

	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	**interface** *interface-id*	PIM スタブ ルーティングをイネーブルに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。
ステップ 3	**ip pim passive**	インターフェイスに PIM スタブ機能を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip pim interface**	各インターフェイスでイネーブルにする PIM スタブを示します。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、**no ip pim passive** 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。

次の例では、IP マルチキャスト ルーティングはイネーブルです。スイッチ A PIM アップリンク ポート 25 は、**SM-DM** がイネーブルである ルーテッド アップリンク ポートとして設定されます。図 35-4 では、PIM スタブ ルーティングは VLAN 100 インターフェイスとギガビット イーサネット ポート 20 でイネーブルになっています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

PIM スタブが各インターフェイスでイネーブルであるか確認するには、**show ip pim interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet0/20 v2/P 0 30 1 10.1.1.1
```

PIM スタブの設定およびステータスに関する情報を表示するには、特権 EXEC コマンドを使用します。

- **show ip pim interface** は、各インターフェイスでイネーブルである PIM スタブを示します。
- **show ip igmp detail** は、特定のマルチキャスト送信元グループに加入した対象のクライアントを示します。
- **show ip igmp mroute** は、マルチキャスト ストリームが送信元から対象のクライアントに転送されたことを確認します。

EIGRP スタブ ルーティングの概要

EIGRP スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を軽減します。EIGRP スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートだけが EIGRP スタブ ルーティングを設定しているスイッチを通過します。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

（注）　スイッチは、完全な EIGRP ルーティングをサポートしていません。スイッチには EIGRP スタブ ルーティング機能が含まれています。この機能は、ルーティング テーブルからネットワークのその他のスイッチに、接続ルートまたはサマリー ルートだけをアドバタイズします。スイッチは、アクセス レイヤで EIGRP スタブ ルーティングを使用して、他のタイプのルーティング アドバタイズメントの必要性をなくします。マルチ VRF CE と EIGRP スタブ ルーティングを同時に設定しようとすると、設定は許可されません。

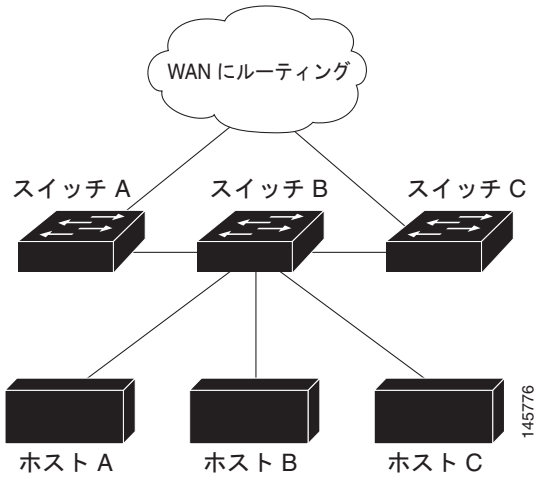
eigrp stub ルータ コンフィギュレーション コマンドの入力後に、**eigrp stub connected summary** コマンドだけが有効になります。Command-Line Interface（CLI; コマンドライン インターフェイス）ヘルプには、**receive-only** キーワードと **static** キーワードが表示されることがあり、これらのキーワードを入力できますが、スイッチの動作は常に、**connected** キーワードと **summary** キーワードが設定されている場合と同じです。

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

スタブ 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 ルータのクエリーを実行せず、スタブ ピアを保持するルータはそのピアのクエリーを実行しません。スタブ ルータは、分散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 35-5 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。スイッチ B は、スイッチ A から取得したルートをアドバタイズしません（その逆も同様）。

図 35-5　EIGRP スタブ ルータ設定



デフォルト ルートだけをリモート ルータに送信するよう分散ルータを設定する場合は、リモート ルータで **ip classless** グローバル コンフィギュレーション コマンドを使用する必要があります。デフォルトでは、**ip classless** コマンドは、EIGRP スタブ ルーティング機能をサポートするすべての Cisco IOS イメージでイネーブルになっています。

スタブ機能がない場合、分散ルータからリモート ルータに送信されたルートがフィルタリングまたはサマライズされた後でも、問題が発生することがあります。企業ネットワーク内でルートが失われると、EIGRP はクエリーを分散ルータに送信することができます。ルートがサマライズされている場合でも、分散ルータが代わりにリモート ルータにクエリーを送信します。EIGRP スタブ ルーティング機能を使用すると、ネットワーク管理者は、クエリーがリモート ルータに送信されないようにできます。

（注）　EIGRP スタブ ルーティングは、スタブ ルータだけで設定する必要があります。スタブ ルータは、コア中継トラフィックが通過しない、ネットワーク コアまたはディストリビューション レイヤに接続されたルータとして定義されます。スタブ ルータには、分散ルータ以外の EIGRP ネイバーを指定できません。この制限を無視すると、望ましくない動作が発生します。

EIGRP スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2*』の「Configuring EIGRP Stub Routing」の部分を参照してください。このマニュアルには Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティングのリモート ルータまたはスポーク ル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 eigrp 1**	EIGRP プロセスを実行するリモート ルータまたは分散ルータを設定し、ルータ設定モードを開始します。
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。

	コマンド	目的
ステップ 4	**eigrp stub** [**receive-only** | **connected** | **static** | **summary**]	EIGRP スタブ ルータとしてリモート ルータを設定します。キーワードの意味は次のとおりです。 • 受信専用ネイバーとしてルータを設定するには、**receive-only** を入力します。 • 接続ルートをアドバタイズするには、**connected** を入力します。 • スタティック ルートをアドバタイズするには、**static** を入力します。 • サマリー ルートをアドバタイズするには、**summary** を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip eigrp neighbor detail**	EIGRP でのスタブ ルータとしてリモート ルータが設定されていることを確認します。出力の最終行は、リモート ルータまたはスポーク ルータのスタブ ステータスを示しています。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特権 EXEC コマンド **show ip eigrp neighbor detail** を分散ルータから入力し、設定を確認します。

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。この機能は、IP ベースまたは IP サービス イメージを実行しているスイッチで使用可能です。IP ベース イメージの場合を除いて、プロトコル関連機能は RIP だけで使用可能です。この章に記載された IP ルーティング プロトコル独立コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』の「IP Routing Protocol-Independent Commands」の章を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

ここでは、次の設定情報について説明します。

- 「Cisco Express Forwarding の設定」（P.35-30）
- 「等コスト ルーティング パスの個数の設定」（P.35-32）
- 「スタティック ユニキャスト ルートの設定」（P.35-32）
- 「デフォルトのルートおよびネットワークの指定」（P.35-33）
- 「ルート マップによるルーティング情報の再配信」（P.35-34）
- 「ルーティング情報のフィルタリング」（P.35-37）
- 「認証鍵の管理」（P.35-39）

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 スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。CEF は、高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、より多くの CPU 処理能力をパケット転送専用にできます。動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効化されます。高速スイッチング キャッシュ エントリが無効になると、トラフィッ

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

CEF の 2 つの主要な構成要素は、分散 FIB と分散隣接テーブルです。

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

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

CEF はデフォルトで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ている場合は、**ip cef** グローバル コンフィギュレーション コマンドを使用して再度イネーブルにできます。

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 コマンドを使うことは、ソフトウェア転送トラフィックのデバッグに効果的です。ソフトウェア転送パスのインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。

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

CEF がディセーブルになっている場合に、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グローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef**	CEF 操作をイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	**ip route**-cache cef	ソフトウェア転送トラフィック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 に関連するインターフェイス情報を表示します。

	コマンド	目的
ステップ 8	**show cef interface** [*interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 9	**show adjacency**	CEF の隣接テーブル情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

等コスト ルーティング パスの個数の設定

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

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

ルーティング テーブルにインストールされるパラレル 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 rip**	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、デフォルトは 4 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip protocols**	*Maximum path* フィールドの設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

スタティック ユニキャスト ルートの設定

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *prefix mask* {*address* | *interface*} [*distance*]	スタティック ルートを確立します。

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

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

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、管理距離の値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトの管理距離が設定されています（表 35-5 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 ルートの管理距離がダイナミック プロトコルの管理距離よりも大きい値になるように設定します。

表 35-5　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距離

ルート送信元	デフォルト距離
接続されたインターフェイス	0
スタティック ルート	1
不明	225

インターフェイスを指し示すスタティック ルートは、RIP を通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが、ルーティング テーブルで接続済みとして見なされた結果、静的な性質を失うためです。ただし、network コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しない限り、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、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。ソフトウェアが、転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクストホップをスタティック ルート内で検出できない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

デフォルトのルートおよびネットワークの指定

ルータは、その他すべてのネットワークへのルートを判別できないことがあります。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛に指定します（スマート ルータには、インターネットワーク全体のルーティング テーブル情報が格納されます）。これらのデフォルト ルートはダイナミックに取得することも、ルータごとに設定することもできます。ほとんどのダイナミックな内部ルーティング プロトコルは、スマート ルータがダイナミックなデフォルト情報を生成し、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、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

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

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

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

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

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、他に設定する必要はありません。ルーティング テーブルはシステムによって定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。シスコ製ルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、管理距離およびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。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る場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

ルート マップによるルーティング情報の再配信

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

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルートマップ コンフィギュレーション コマンドは、ルート マップの条件部分を定義します。**match** コマンドは、一致しなければならない条件を指定します。**set** コマンドは、ルーティング アップデートが match コマンドによって定義される条件と一致した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に依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものです。

route-map コマンドの後に、**match** コマンドおよび **set** コマンドをそれぞれ 1 つ以上指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合は、match 以外何も実行されません。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。

（注）　**set** ルート マップ コンフィギュレーション コマンドが指定されていないルート マップは CPU に送信され、これによって 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** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます（宛先ベース ルーティング）。ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに set 句が適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

（注） ステップ 3 に続くステップは任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-tag* [**permit** | **deny**] [*sequence number*]	再配信を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。 *map-tag*：ルート マップ用のわかりやすい名前を指定します。**redistribute** ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 （任意）**permit** が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートが再配信されます。**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）：同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を指定する番号です。
ステップ 3	**match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	名前または番号を指定し、標準アクセス リストと一致させます。1 ～ 199 の整数を指定できます。
ステップ 4	**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 の指定された値を指定できます。
ステップ 5	**match ip next-hop** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアクセス リスト（番号 1 ～ 199）のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。
ステップ 6	**match tag** *tag value* [*...tag-value*]	1 つ以上のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ～ 4294967295 の整数を指定できます。
ステップ 7	**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 8	**match ip route-source** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	指定されたアドバタイズ済みアクセス リストによって指定されるアドレスと一致させます。

	コマンド	目的
ステップ 9	**set level** {**level-1** | **level-2** | **level-1-2**}	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。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show route-map**	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

ルーティング ドメイン間でルートを配信したり、ルート再配信を制御できます。

ルート再配信を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは前述の手順で定義されたキーワードと同じあることに注意してください。

	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	**router rip**	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。ルートマップを指定しないと、すべてのルートが再配信されます。キーワード **route-map** に *map-tag* を指定しないと、ルートは配信されません。
ステップ 4	**default-metric** *number*	現行のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します（RIP）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show route-map**	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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的にメトリック変換が行われることがあります。

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

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、ここで説明されている作業を実行します。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータがダイナミックにルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用して、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続けるようにします。

多数のインターフェイスが存在するネットワークでは、手動でパッシブに設定することを避けるため、**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することで、すべてのインターフェイスをデフォルトでパッシブに設定できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router rip**	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 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	**passive-interface default**	（任意）すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	**no passive-interface** *interface type*	（任意）隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	**network** *network-address*	（任意）ルーティング プロセス用のネットワーク リストを指定します。*network-address* は IP アドレスです。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

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

ルーティング アップデートのアドバタイズメントおよび処理の制御

アクセス コントロール リストと **distribute-list** ルータ コンフィギュレーションコマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズメントを抑制し、他のルータが 1 つ以上のルートを取得しないようにできます。**distribute-list** ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます

ルーティング アップデートのアドバタイズメント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 rip**	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メントを許可または拒否します。
ステップ 4	**distribute-list** {*access-list-number* | *access-list-name*} **in** [*type-number*]	アップデートにリストされたルートの処理を抑制します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。*管理距離*は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティング プロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。管理距離の値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルの管理距離が最短であるルートがルータによって選択されます。表 35-5（P.35-33）に、さまざまなルーティング情報送信元のデフォルトの管理距離を示します。

各ネットワークには独自の要件があるため、管理距離を割り当てる一般的な注意事項はありません。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router rip**	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*]	管理距離を定義します。 *weight*：管理距離は 10 ～ 255 の整数です。単独で使用した場合、*weight* はデフォルトの管理距離を指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。管理距離が 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 IP 拡張アクセス リストです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	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距離を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

距離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。

認証鍵の管理

鍵管理を使用すると、ルーティング プロトコルで使用される認証鍵を制御できます。一部のプロトコルでは、鍵管理を使用できません。認証鍵は RIP Version 2 で使用できます。

認証鍵を管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証鍵を管理するには、キー チェーンを定義してそのキー チェーンに属する鍵を識別し、各鍵の有効期間を指定します。各鍵には、ローカルに格納される独自の鍵 ID（**key** *number* キー チェーン コンフィギュレーション コマンドで指定）があります。鍵 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）認証鍵が一意に識別されます。

有効期間が指定された複数の鍵を設定できます。存在する有効な鍵の個数に関係なく、1 つの認証パケットだけが送信されます。鍵番号は小さい方から大きい方へソフトウェアによって順に調べられ、最初に見つかった有効な鍵が使用されます。鍵変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があることに注意してください。

認証鍵を管理するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *name-of-chain*	キー チェーンを識別し、キー チェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *number*	鍵番号を識別します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 4	**key-string** *text*	キー ストリングを識別します。ストリングには 1 ～ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定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）鍵を受信する期間を指定します。 *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* を指定した無制限で、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）鍵を送信する期間を指定します。 *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* を指定した無制限で、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**	認証鍵情報を表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

IP ネットワークの監視およびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを削除したり、ステータスを表示したりするには、表 35-6 に示す特権 EXEC コマンドを使用します。

表 35-6　IP ルートの削除またはルート ステータスの表示を行うコマンド

コマンド	目的
clear ip route {*network* [*mask* | *]}	IP ルーティング テーブルから 1 つ以上のルートを削除します。
show ip protocols	アクティブなルーティング プロトコル プロセスのパラメータおよびステートを表示します。
show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]	ルーティング テーブルの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、または指定されたルート マップだけを表示します。