



IP ユニキャスト ルーティングの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチ上で 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。IPv6 ルーティングの詳細については、[第 37 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。



(注)

ルーティングは、メトロ IP アクセス イメージが稼動しているスイッチ上でだけサポートされています。

IPv4 ユニキャスト設定の詳細については、『*Cisco IOS IP Configuration Guide*』 Release 12.2 を参照してください。この章で使用するコマンドの構文および使用方法については、次のコマンド リファレンスを参照してください。

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

この章で説明する内容は、次のとおりです。

- 「[IP ルーティングの概要](#)」 (P.36-2)
- 「[ルーティングを設定する手順](#)」 (P.36-3)
- 「[IP アドレス指定の設定](#)」 (P.36-4)
- 「[IPv4 ユニキャスト ルーティングのイネーブル化](#)」 (P.36-19)
- 「[RIP の設定](#)」 (P.36-20)
- 「[OSPF の設定](#)」 (P.36-25)
- 「[EIGRP の設定](#)」 (P.36-38)
- 「[BGP の設定](#)」 (P.36-45)
- 「[ISO CLNS ルーティングの設定](#)」 (P.36-67)
- 「[BFD の設定](#)」 (P.36-78)
- 「[マルチ VRF CE の設定](#)」 (P.36-88)
- 「[プロトコルに依存しない機能の設定](#)」 (P.36-101)
- 「[IP ネットワークのモニタリングおよびメンテナンス](#)」 (P.36-117)



(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 default** 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、バランス リソースに Switch Database Management (SDM; スイッチ データベース管理) 機能を設定する必要があります。レイヤ 2 テンプレートでは、ルーティングはサポートされて

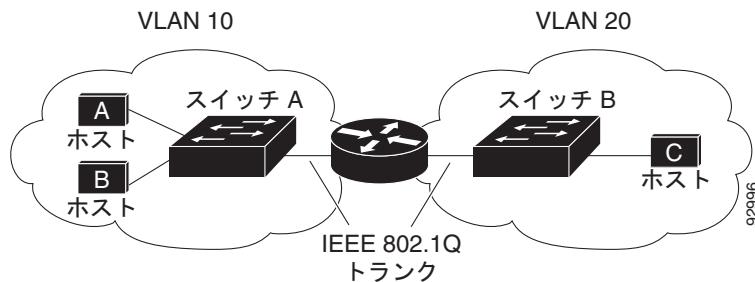
いません。そのため、ルーティングはすべてソフトウェアを介して実行されます。この場合、CPU に負荷がかかり、ルーティングのパフォーマンスが大幅に低下します。SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」、またはこのリリースのコマンドリファレンスの **sdm prefer** コマンドの項を参照してください。

IP ルーティングの概要

IP ネットワークでは、各サブネットワークは 1 つの VLAN に対応しています。ただし、別々の VLAN に属するネットワーク デバイスが相互に通信するには、VLAN 間でトラフィックをルーティング (VLAN 間ルーティング) するレイヤ 3 デバイス (ルータ) が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 36-1 は、基本的なルーティング トポロジを示したものです。スイッチ A は VLAN 10 に、スイッチ B は VLAN 20 にそれぞれ属しています。ルータには、各 VLAN のインターフェイスがあります。

図 36-1 ルーティング トポロジの例



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

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでその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て、適切な発信インターフェイスを特定し、VLAN 20 インターフェイスからパケットをスイッチ B へ転送します。スイッチ B はパケットを受け取り、それをホスト C へ転送します。

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 ルーティングを使用する (ルータにとって宛先が不明な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)
- トラフィックに対して事前にプログラミングされたスタティック ルートを使用する

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経由して、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 ルーティングでは、ネットワーク内の構成の変更に自動的に対応できないため、パケットが宛先に到達しない場合があります。

- ルーティング プロトコルを使用してルートをダイナミックに計算する

ダイナミック ルーティング プロトコルに基づいて、トラフィックを転送する最適ルートがルータによりダイナミックに計算されます。スイッチでは、ルーティング プロトコルとして、Routing Information Protocol (RIP)、Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル)、Open Shortest Path First (OSPF) プロトコル、Enhanced IGRP (EIGRP)、Intermediate System-to-Intermediate System (IS-IS)、および Bidirectional Forwarding Detection (BFD; 双方フォワーディング検出) がサポートされています。

ルーティングを設定する手順

デフォルトでは、IPv4 ルーティングはスイッチ上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、IPv4 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 コンフィギュレーションの詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 を参照してください。

以下で説明する手順では、次に示すレイヤ 3 インターフェイスのうちいずれか 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 コマンドによりレイヤ 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 コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャンネル : **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ンネルグループにバインドして作成されたポートチャン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.35-14) 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.36-5) 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。ソフトウェアには、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、ハードウェアには限界があるため、この個数と実装されている他の機能の数との組み合わせによっては、CPU のパフォーマンスに影響する場合があります。IPv4 ルーティングをサポートするには、**sdm prefer default** 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。

IPv4g 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、スイッチ上で 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 IPv4 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 IPv4 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 ルーティングでは、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、その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介してホストと通信できるようにする必要があります。ここでは、さまざまな IP アドレス指定機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- 「アドレス指定のデフォルト設定」 (P.36-4)
- 「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.36-5)
- 「アドレス解決方法の設定」 (P.36-8)
- 「IP ルーティングがディセーブルの場合のルーティング支援機能」 (P.36-11)
- 「ブロードキャスト パケットの処理方法の設定」 (P.36-13)
- 「IP アドレス指定のモニタリングおよびメンテナンス」 (P.36-18)

アドレス指定のデフォルト設定

表 36-1 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	定義なし。
ARP	Address Resolution Protocol (ARP; アドレス解決プロトコル) 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 ダイレクトブロードキャスト	ディセーブル (すべての IP ダイレクトブロードキャストが廃棄されます)。
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、または UDP フラッド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。 ターボフラッドディング：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。

表 36-1 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
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： <ul style="list-style-type: none"> 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。 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 パケットの送信先は、IP アドレスで表されます。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列を特定するためのものです。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 shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface (UNI; ユーザ ネットワーク インターフェイス) および Enhanced Network Interface (ENI; 拡張ネットワーク インターフェイス) はディセーブル、Network Node Interface (NNI; ネットワーク ノード インターフェイス) はイネーブルです。
ステップ 4	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 5	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 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 アドレスがゼロのサブネットは絶対に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おそれがあります。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。

オール 1 サブネット (131.108.255.0) は使用可能です。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	<code>configure terminal</code>	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	<code>ip subnet-zero</code>	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おけるサブネット ゼロの使用をイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

クラスレス ルーティング

ルーティングを行うように設定されたスイッチ上では、クラスレス ルーティング動作が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受信したルータは、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、連続する複数のクラス C アドレス レンジを 1 つにまとめたブロックにより構成され、それぞれのブロックにより比較的規模の大きな 1 つのアドレス レンジが疑似的に形成されます。スーパーネットは、クラス B アドレス レンジの急速な枯渇を回避するために設計されたものです。

図 36-2 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。ホストから 128.20.4.1 へパケットが送信されると、ルータはその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 36-2 IP クラスレス ルーティングがイネーブルの場合

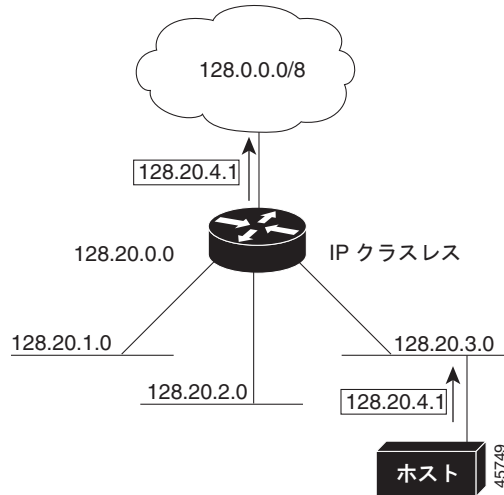
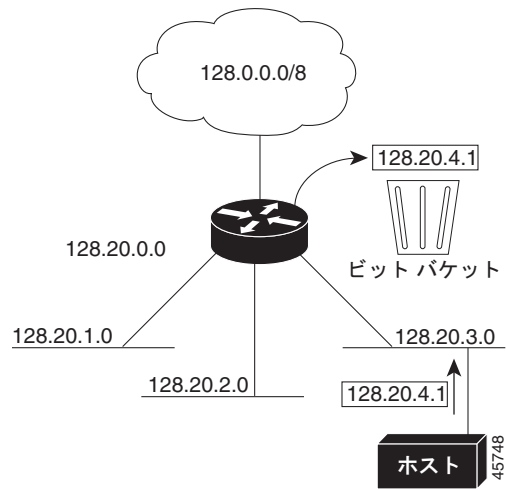


図 36-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、および 128.20.3.0 に接続されています。ホストから 128.20.4.1 へパケットが送信された場合、ネットワークにはデフォルト ルートが存在しないため、ルータはそのパケットを廃棄します。

図 36-3 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 <code>configure terminal</code>	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 <code>no ip classless</code>	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 <code>end</code>	特権 EXEC モードに戻ります。
ステップ4 <code>show running-config</code>	設定を確認します。
ステップ5 <code>copy running-config startup-config</code>	(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、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最適なスーパーネットワーク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、そのデバイスが属しているネットワークを表すネットワーク アドレスが割り当てられます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの 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 アドレスを学習するプロセスを、「アドレス解決」と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、「逆アドレス解決」と呼びます。

スイッチでは、次の形式のアドレス解決を行えます。

- **ARP** : IP アドレスを基に対応する MAC アドレスを取得する場合に使用します。ARP は、入力として IP アドレスを受け取ると、それに対応する MAC アドレスを学習します。また、以降の取得を高速化できるように、IP アドレスと MAC アドレスの対応が ARP キャッシュに格納されます。そのあと、IP データグラムはリンクレイヤ 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** : 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、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そのルータに格納されていれば、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、ルータはそれらのパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能 (ローカル MAC アドレスでなく IP アドレスを要求する点を除く) を持つ Reverse Address Resolution Protocol (RARP; 逆アドレス解決プロトコル) 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。サーバを特定する必要がある場合は、**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。

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.36-8)
- 「[ARP カプセル化の設定](#)」 (P.36-10)
- 「[プロキシ ARP のイネーブル化](#)」 (P.36-10)

スタティック ARP キャッシュの定義

ARP など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な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永続的なエントリを ARP キャッシュに設定できます。また、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、その ARP エントリに対して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。 <ul style="list-style-type: none"> • arpa : ARP カプセル化 (イーサネット インターフェイス用) • snap : SNAP カプセル化 (トークンリングおよび FDDI の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 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 6 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 7 end	特権 EXEC モードに戻ります。
ステップ 8 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 9 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 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。

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（キーワード **arpa** 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	no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	arp {arpa snap}	ARP カプセル化方法を指定します。 <ul style="list-style-type: none"> • arpa : ARP • snap : SNAP
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	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 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。

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

デフォルトの場合、スイッチでは、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のプロトコルとして、プロキシ ARP が使用されます。

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	no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	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 5	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ6	<code>show ip interface [interface-id]</code>	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7	<code>copy running-config startup-config</code>	(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

IP ルーティングがイネーブルでないスイッチでは、次のメカニズムを使用することで、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.36-11)
- 「デフォルト ゲートウェイ」(P.36-11)
- 「IRDP」(P.36-12)

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。ルーティング情報を持たないホストは、すべてのホストが同じローカルイーサネット上にあり、かつそれらが ARP を使用して MAC アドレスを学習するという仮定の下で動作します。送信元と異なるネットワーク上のホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを調べます。最適ルートがある場合、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。要求の送信元ホストはパケットをスイッチに送信し、スイッチはそのパケットを目的のホストに転送します。プロキシ ARP では、すべてのネットワークがローカルにある場合と同様に処理され、IP アドレスごとに ARP 要求が実行されます。

デフォルトでは、プロキシ ARP は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方法については、「[プロキシ ARP のイネーブル化](#)」(P.36-10) 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れば有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法として、デフォルト ルータ (デフォルト ゲートウェイ) を定義するという方法があります。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、適切にルーティングを行うか、または IP 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ことでホストが使用するローカル ルータを指定します。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や使用できなくなった場合に、そのことを検出できないという短所があります。

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。

■ IP アドレス指定の設定

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

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

IRDP

スイッチでは、ルータ ディスカバリを使用することにより、IRDP を介して他のネットワークへのルートをダイナミックに学習できます。ホストは、IRDP を使用して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 RIP ルーティングの更新を受信し、この情報からルータの場所を推測することもできます。ただし、実際のところ、スイッチには、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 テーブルが格納されるわけではなく、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 には、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思なされるまでの期間を、ルータごとに指定できるという利点があります。

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。プライオリティがより高いルータが検出された場合、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、または再転送が多すぎるために TCP 接続がタイムアウトに近づいている場合には、最も高いプライオリティを持つルータが新たに選択されます。

インターフェイスで IRDP ルーティングを行うには、そのインターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータは、必要に応じて変更することもできます。

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	no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	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。

コマンド	目的
ステップ5 <code>ip irdp multicast</code>	(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6 <code>ip irdp holdtime seconds</code>	(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 <code>maxadvertinterval</code> 値の 3 倍です。 <code>maxadvertinterval</code> 値よりも大きな値 (9000 秒以下) を指定する必要があります。 <code>maxadvertinterval</code> 値を変更すると、この値も変更されます。
ステップ7 <code>ip irdp maxadvertinterval seconds</code>	(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8 <code>ip irdp minadvertinterval seconds</code>	(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 <code>maxadvertinterval</code> 値の 0.75 倍です。 <code>maxadvertinterval</code> を変更すると、この値も新しいデフォルト値 (<code>maxadvertinterval</code> の 0.75 倍) に変更されます。
ステップ9 <code>ip irdp preference number</code>	(任意) デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は $-2^{31} \sim 2^{31}$ です。デフォルト値は 0 です。この値を大きくするにつれて、ルータのプリファレンス レベルは高くなります。
ステップ10 <code>ip irdp address address [number]</code>	(任意) プロキシアドバタイズを行うために必要な IRDP アドレスおよびプリファレンスを指定します。
ステップ11 <code>end</code>	特権 EXEC モードに戻ります。
ステップ12 <code>show ip irdp</code>	IRDP 値を表示し、設定を確認します。
ステップ13 <code>copy running-config startup-config</code>	(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` 値および `minadvertinterval` 値も変更されます。そのため、`holdtime` 値または `minadvertinterval` 値のいずれかを手動で変更するには、最初に `maxadvertinterval` 値を変更しておくことが重要です。

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

- **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 フィールドまたはサブネット フィールドが含まれます。
- **フラ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することによっても、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャストの各トラフィックを制限できます。詳細については、第 23 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。

ルータでは、ブロードキャスト ストームを防ぐため、ローカル ケーブル長が制限されています。ブリッジ（インテリジェントブリッジを含む）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 ストームが伝播します。ブロードキャスト ストーム問題を解決するには、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のが最善の方法です。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。スイッチでは、ブロードキャスト メッセージの転送用として複数のアドレス指定スキームがサポートされています。

- 「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.36-14)
- 「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.36-15)
- 「IP ブロードキャスト アドレスの確立」(P.36-16)
- 「IP ブロードキャストのフラッディング」(P.36-17)

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

サービス拒絶攻撃からルータを極力保護するため、デフォルトでは、IP ダイレクトブロードキャストは転送されず廃棄されます。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。転送できるのは、**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したプロトコルだけです。

アクセス リストを指定すると、転送するブロードキャストを制御できます。アクセス リストで許可されている IP パケットに限り、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るようになります。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 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4 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。アクセス リストを指定すると、転送するブロードキャストを制御できます。アクセス リストを指定した場合、そのアクセス リストで許可されている IP パケットだけが変換可能となります。
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。

コマンド	目的
ステップ6 <code>ip forward-protocol {udp [port] nd sdns}</code>	ブロードキャスト パケットを転送する際に、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。 <ul style="list-style-type: none"> • udp : UDP データグラムを転送します。 <i>port</i> : (任意) 転送される UDP サービスを制御する宛先ポートを指定します。 • 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7 <code>end</code>	特権 EXEC モードに戻ります。
ステップ8 <code>show ip interface [interface-id]</code> または <code>show running-config</code>	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9 <code>copy running-config startup-config</code>	(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

User Datagram Protocol (UDP; ユーザ データグラム プロトコル) は、2つのエンドシステム間でオーバーヘッドの少ないコネクションレス型セッションを実現する IP ホストツーホスト レイヤ プロトコルです。UDP では、受信したデータグラムの確認応答は行われません。ネットワーク ホストでは、UDP ブロードキャストを使用して、アドレス、設定、名前などの情報の検索が行われる場合もあります。このようなホストが、サーバの存在しないネットワーク セグメントに属する場合は、通常 UDP ブロードキャストは転送されません。ルータ上では、特定のクラスのブロードキャストがヘルパー アドレスへ転送されるように、インターフェイスを設定できます。それぞれのインターフェイスに対して、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定すると、転送される UDP サービスを制御できます。UDP プロトコルは複数指定することもできます。また、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; ネットワーク ディスク) 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。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については、『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 コマンドに関する説明箇所に記載されているリストを参照してください。

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) 情報を搬送します。

■ IP アドレス指定の設定

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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip helper-address address</code>	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 5	<code>exit</code>	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	<code>ip forward-protocol {udp [port] nd sdns}</code>	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 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show ip interface [interface-id]</code> または <code>show running-config</code>	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 9	<code>copy running-config startup-config</code>	(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

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 で構成されたアドレスです (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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip broadcast-address ip-address</code>	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 5	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ6	<code>show ip interface [interface-id]</code>	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7	<code>copy running-config startup-config</code>	(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 ブロードキャストアドレスをデフォルトに戻すには、**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、フラッディングに関与す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では、ブロードキャストを受信できますが、受信したブロードキャストは転送できません。また同じルータのある別のインターフェイス上で受信されたブロードキャストが、そのインターフェイスを介して送信されることもありません。

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はフラッディング可能です。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。フラッディングを行う場合、パケットは次の条件を満たす必要があります (これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです)。

- MAC レベルのブロードキャストであること。
- IP レベルのブロードキャストであること。
- 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 であること。
- Time To Live (TTL) 値が 2 以上であること。

フラッディングされた UDP データグラムには、出カインターフェイス上で **ip broadcast-address** インターフェイス コンフィギュレーション コマンドにより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るため、データグラムがネットワーク上を伝播していくのに伴って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 ずつ減少します。

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)、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。そのため、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	<code>configure terminal</code>	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	<code>ip forward-protocol spanning-tree</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(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 アドレス指定の設定

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て、スパニング ツリー ベースの UDP フラッディングを約 4～5 倍高速化できます。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

スパニング ツリー ベースのフラッディングを高速化させるには、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 アドレス指定のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になる、またはその可能性がある場合は、**clear** 特権 EXEC コマンドを使用して、すべての内容を消去できます。

表 36-2 キャッシュ、テーブル、およびデータベースを消去するためのコマンド

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 1 つまたはすべてのエントリを削除します。
clear ip route {network [mask] *}	IP ルーティング テーブルから 1 つまたは複数のルート削除します。

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経路など）のような特定の統計情報を表示できます。

表 36-3 キャッシュ、テーブル、およびデータベースを表示するためのコマンド

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、サーバ ホスト名、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。

表 36-3 キャッシュ、テーブル、およびデータベースを表示するためのコマンド (続き)

コマンド	目的
<code>show ip irdp</code>	IRDP 値を表示します。
<code>show ip masks address</code>	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の数を表示します。
<code>show ip redirects</code>	デフォルト ゲートウェイのアドレスを表示します。
<code>show ip route [address [mask]] [protocol]</code>	ルーティング テーブルの現在の状態を表示します。
<code>show ip route summary</code>	ルーティング テーブルの現在の状態をサマリー形式で表示します。

IPv4 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 ルーティングは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	<code>configure terminal</code>	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	<code>ip routing</code>	IP ルーティングをイネーブルにします
ステップ 3	<code>router ip_routing_protocol</code>	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 コマンドを使用して、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。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 を使用した IP ルーティングをイネーブルにする例を示します。

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

この時点で、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。手順については次の各セクションで説明します。

- 「RIP の設定」 (P.36-20)
- 「OSPF の設定」 (P.36-25)
- 「EIGRP の設定」 (P.36-38)

- 「BGP の設定」 (P.36-45)
- 「ISO CLNS ルーティングの設定」 (P.36-67)
- 「OSFP に対する BFD の設定」 (P.36-82)
- 「プロトコルに依存しない機能の設定」 (P.36-101) (任意)

RIP の設定

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

RIP を使用している場合、スイッチからはルーティング情報アップデート (アドバタイズメント) が 30 秒間隔で送信します。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、アップデートを行わないルータに関するルーティング テーブル エントリはすべて削除されます。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由するルータ数です。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。また、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。このように到達可能範囲 (0 ~ 15) が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP では、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がアドバタイズされます。0.0.0.0 は、実在するネットワークではありませんが、RIP では、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扱われます。デフォルト ネットワークが RIP によって学習された場合、またはルータが最終ゲートウェイで、RIP にデフォルト メトリックが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 では、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が送信されます。インターフェイスのネットワークは、指定されていないければ、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」 (P.36-20)
- 「基本的な RIP パラメータの設定」 (P.36-21)
- 「RIP 認証の設定」 (P.36-23)
- 「スプリット ホライズンの設定」 (P.36-23)

RIP のデフォルト設定

表 36-4 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。
デフォルト情報の送信	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)。

表 36-4 RIP のデフォルト設定 (続き)

機能	デフォルト設定
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。
Neighbor	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	<ul style="list-style-type: none"> • アップデート：30 秒。 • 無効：180 秒。 • ホールドダウン：180 秒。 • フラッシュ：240 秒。
アップデート送信元の検証	イネーブル。
バージョン	RIP バージョン 1 パケットおよびバージョン 2 パケットを受信し、バージョン 1 パケットを送信。

基本的な RIP パラメータの設定

RIP を設定する場合は、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。Cisco ME 3400E スイッチに対して RIP コンフィギュレーション 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。

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に限り必須です)。
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を行うためには、これらのネットワークのインターフェイスを経由することが必要です。 (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隣接ルータを定義します。これにより、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。

RIP の設定

コマンド	目的
ステップ 6 offset list [<i>access-list number</i> <i>name</i>] { <i>in</i> <i>out</i> } <i>offset</i> [<i>type number</i>]	(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 を通じて学習したルートへの着信メトリックおよび発信メトリックを増やします。オフセット リストは、アクセス リストまたはインターフェイスを使用して制限できます。
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。 <ul style="list-style-type: none"> • <i>update</i> : ルーティング アップデートの送信間隔を指定します。デフォルトは 30 秒です。 • <i>invalid</i> : ルートが無効と宣言されるまでの制限時間を指定します。デフォルトは 180 秒です。 • <i>holddown</i> : 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を指定します。デフォルトは 180 秒です。 • <i>flush</i> : ルーティング アップデートが延期される時間を指定します。デフォルトは 240 秒です。
ステップ 8 version { <i>1</i> <i>2</i> }	(任意) RIP バージョン 1 または RIP バージョン 2 のパケットだけが送受信されるようにスイッチを設定します。デフォルトの場合、スイッチはバージョン 1 およびバージョン 2 を受信し、バージョン 1 だけを送信します。インターフェイス上での送受信に使用されるバージョンを制御するには、インターフェイス コマンド ip rip {send receive} version 1 2 1 2 を使用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 に限る)、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の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。デフォルトの場合、スイッチでは着信 RIP ルーティング アップデートの送信元 IP アドレスの検証が行われます。送信元アドレスが無効な場合、アップデートは廃棄されます。通常的环境下で使用するときは、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 11 output-delay <i>delay</i>	(任意) 送信する RIP アップデートの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 アップデートにパケット間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状態を表示するには、**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、認証は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には、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鍵は、キーチェーンによって決まります。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。そのため、「[認証鍵の管理](#)」(P.36-116)に記載されている作業も実行する必要があります。

スイッチでは、RIP 認証がイネーブルであるインターフェイスに対して、プレーンテキストと MD5 の 2 種類のモードでの認証がサポートされています。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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip rip authentication key-chain name-of-chain</code>	RIP 認証をイネーブルにします。
ステップ 5	<code>ip rip authentication mode [text md5]</code>	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 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config interface [interface-id]</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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。認証を実行しない場合は、`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。

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 ループの発生を回避するために、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 ホライズンを適用した場合、ルータでは、ルートに関する情報がその送信元インターフェイスからアドバタイズされなくなります。この機能を使用すると、リンクが壊れている場合に複数のルータ間通信が最適化されます。



(注)

ルートが適切にアドバタイズされるよう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ことが必要である場合を除いて、通常は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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip address ip-address subnet-mask</code>	IP アドレスおよび IP サブネットを設定します。
ステップ 5	<code>no ip split-horizon</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip interface interface-id</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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。

サマリー アドレスの設定

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 プールがアドバタイズされるように、RIP が実行されているインターフェイスを設定するには、`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 アドレスとインターフェイス 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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip address ip-address subnet-mask</code>	IP アドレスおよび IP サブネットを設定します。
ステップ 5	<code>ip summary-address rip ip address ip-network mask</code>	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 6	<code>no ip split horizon</code>	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。

	コマンド	目的
ステップ7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ8	<code>show ip interface interface-id</code>	設定を確認します。
ステップ9	<code>copy running-config startup-config</code>	(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 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。インターフェイスがレイヤ 2 モード (デフォルト) の場合は、**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 アドレス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)# no switchport
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
```

OSPF の設定

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

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



(注)

OSPF では、各メディアがブロードキャスト ネットワーク、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、またはポイントツーポイント ネットワークに分類されます。ブロードキャスト ネットワークおよび非ブロードキャスト ネットワークは、ポイントツーマルチポイント ネットワークとしても設定できます。スイッチでは、これらすべてのネットワーク タイプがサポートされています。

シスコの実装機能は、OSPF バージョン 2 仕様に準拠しています。主な特徴は次のとおりです。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって学習したルートは、別の IP ルーティング プロトコルに再配布できます。つまり OSPF では、ドメイン内レベルで、EIGRP および RIP によって学習したルートを取り込むことができます。OSPF ルートを RIP にエクスポートすることもできます。
- エリア内の隣接ルータ間におけるプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータの dead インターバルおよび hello インターバル、認証鍵などがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area (NSSA) がサポートされています。

通常、OSPF を使用するためには、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) の間で調整を行う必要があります。最低限の設定では、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。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.36-27)
- 「NSF 認識」(P.36-28)
- 「OSPF インターフェイスの設定」(P.36-29)
- 「OSPF のネットワーク タイプの設定」(P.36-30)
- 「OSPF エリア パラメータの設定」(P.36-33)
- 「その他の OSPF パラメータの設定」(P.36-34)
- 「LSA グループ ペーシングの変更」(P.36-36)
- 「ループバック インターフェイスの設定」(P.36-36)
- 「OSPF のモニタリング」(P.36-37)

OSPF のデフォルト設定

表 36-5 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。 再送信インターバル：5 秒。 送信遅延：1 秒。 プライオリティ：1。 hello インターバル：10 秒。 dead インターバル：hello インターバルの 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 エリアの定義なし。 NSSA：NSSA の定義なし。
自動コスト	100 Mbps。
デフォルト情報の送信	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、デフォルトの外部ルート タイプはタイプ 2。
デフォルト メトリック	各ルーティング プロトコルに適した組み込みの自動メトリック変換。
距離 OSPF	dist1（エリア内部のすべてのルート）：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 LSA がインターフェイスにフラッディング。
IP OSPF 名検索	ディセーブル。
隣接関係変更ログ	イネーブル。
Neighbor	指定なし。
近接データベース フィルタ	ディセーブル。発信 LSA はすべてネイバーにフラッディング。
ネットワーク エリア	ディセーブル。
NSF ¹ 認識	イネーブル ² 。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
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 遅延：5 秒。 SPF ホールドタイム：10 秒。

表 36-5 OSPF のデフォルト設定 (続き)

機能	デフォルト設定
仮想リンク	<p>エリア ID またはルータ ID は未定義</p> <p>hello インターバル : 10 秒。</p> <p>再送信インターバル : 5 秒。</p> <p>送信遅延 : 1 秒。</p> <p>dead インターバル : 40 秒。</p> <p>認証鍵 : 鍵は未定義。</p> <p>メッセージダイジェスト鍵 (MD5) : 鍵は未定義。</p>

1. NSF = Nonstop Forwarding (ノンストップフォワーディング)
2. OSPF NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、OSPF NSF 認識機能がサポートされています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ Route Processor (RP; ルート プロセッサ) がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア 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、隣接ルータからのパケットが転送され続けます。

この機能は、ディセーブルにできません。この機能の詳細については、次の URL にある『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://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 プロセスを作成して、そのルーティング プロセスに関連付ける IP アドレスの範囲を指定し、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	<code>configure terminal</code>	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	<code>router ospf process-id</code>	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、内部で使用するためにローカルに割り当てられる識別パラメータです。プロセス ID には、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割り当てられます。
ステップ 3	<code>network address wildcard-mask area area-id</code>	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。wildcard-mask を指定すると、1 つのコマンドを使用するだけで、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 進数または IP アドレスを指定できます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show ip protocols</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、OSPF ルーティング プロセスを設定し、それにプロセス番号 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は変更する必要はありませんが、一部のインターフェイス パラメータ (hello インターバル、dead インターバル、認証鍵など) については、接続されたネットワーク内のすべてのルータで値を統一する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。



(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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip ospf cost</code>	(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 5	<code>ip ospf retransmit-interval seconds</code>	(任意) Link State Advertisement (LSA; リンク ステート アドバタイズメント) の送信間隔を秒単位で指定します。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は 5 秒です。
ステップ 6	<code>ip ospf transmit-delay seconds</code>	(任意) リンク ステート アップデート パケットを送信するまでの予測待機時間を秒単位で設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は 1 秒です。
ステップ 7	<code>ip ospf priority number</code>	(任意) ネットワークに対して、OSPF で指定されたルータを検索する際の手掛かりとなる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 8	<code>ip ospf hello-interval seconds</code>	(任意) OSPF インターフェイスにおける hello パケットの送信間隔を秒単位で設定します。この値は、ネットワークのすべてのノードで同じであることが必要です。指定できる範囲は 1 ~ 65535 秒です。デフォルトは 10 秒です。

コマンド	目的
ステップ 9 <code>ip ospf dead-interval seconds</code>	(任意) 最後のデバイスの hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒単位で設定します。この値は、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 インターバルの 4 倍です。
ステップ 10 <code>ip ospf authentication-key key</code>	(任意) 隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列 (最大 8 バイト長) を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換できるように、同じパスワードを設定する必要があります。
ステップ 11 <code>ip ospf message-digest-key keyid md5 key</code>	(任意) MDS 認証をイネーブルにします。 <ul style="list-style-type: none"> • <i>keyid</i> : ID を 1 ~ 255 の範囲で指定します。 • <i>key</i> : 英数字パスワードを指定します (最大 16 バイト)。
ステップ 12 <code>ip ospf database-filter all out</code>	(任意) インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトの場合、OSPF では、LSA が到達するインターフェイスを除く、同じエリア内のすべてのインターフェイスに新しい LSA がフラッディングされます。
ステップ 13 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 14 <code>show ip ospf interface [interface-name]</code>	OSPF に関連するインターフェイス情報を表示します。
ステップ 15 <code>show ip ospf neighbor detail</code>	近接スイッチの 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。 <ul style="list-style-type: none"> • <i>Options is 0x52</i> <i>LLS Options is 0x1 (LR)</i> この 2 つの行が表示されれば、近接スイッチは NSF 認識です。 • <i>Options is 0x42</i> : 近接スイッチが NSF 認識でないことを表します。
ステップ 16 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

OSPF のネットワーク タイプの設定

OSPF では、デフォルトで各メディアが次の 3 タイプのネットワークに分類されます。

- ブロードキャスト ネットワーク (イーサネット、トークンリング、および FDDI)
- NBMA ネットワーク (Switched Multimegabit Data Service [SMDS; スイッチド マルチメガビット データ サービス]、フレーム リレー、および X.25)
- ポイントツーポイント ネットワーク (High-Level Data Link Control [HDLC; ハイレベル データリンク制御]、PPP [ポイントツーポイントプロトコル])

また、ネットワーク インターフェイスは、デフォルトのメディア タイプに関係なく、ブロードキャスト ネットワークまたは NBMA ネットワークのいずれかに設定できるほか、ポイントツーポイントまたはポイントツーマルチポイントのいずれかに設定することもできます。

非ブロードキャスト ネットワークに対する OSPF の設定

OSPF ネットワークには多数のルータが付加される可能性があるため、ネットワークに対して代表ルータを選択します。ネットワーク内でブロードキャスト機能が設定されていない場合に、代表ルータを選択するには、特別なコンフィギュレーションパラメータが必要となります。これらのパラメータを設定する必要があるのは、代表ルータまたはバックアップの代表ルータになることが許可されている（つまりルータ プライオリティ値が 0 でない）デバイスに対してだけです。

非ブロードキャスト ネットワークと相互接続する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	<code>configure terminal</code>	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	<code>router ospf process-id</code>	OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>neighbor ip-address [priority number] [poll-interval seconds]</code>	必要に応じて、ネイバー パラメータにより OSPF ネイバーを指定します。 <ul style="list-style-type: none"> <code>ip-address</code> : OSPF ネイバーのインターフェイス IP アドレスを入力します。 (任意) <code>priority number</code> : IP アドレスに関連付けられた非ブロードキャスト ネイバーのルータ プライオリティ値を指定します。指定できる範囲は 0 ~ 255 で、デフォルト値は 0 です。 (任意) <code>poll-interval seconds</code> : ポーリング インターバル (秒単位) を表す数値を指定します。ただし、<code>hello</code> インターバルに比べて十分大きな値を指定することを推奨します。指定できる範囲は 0 ~ 4294967295 で、デフォルトは 120 秒 (2 分) です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip ospf [process-id]</code>	OSPF に関連する情報を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

ポイントツーマルチポイントの非ブロードキャスト ネットワークでは、さらに `neighbor` ルータ コンフィギュレーション コマンドを使用してネイバーを指定します。ネイバーにコストを割り当てるかどうかは任意です。

OSPF インターフェイスに対するネットワーク タイプの設定

ネットワーク インターフェイスは、デフォルトのメディア タイプに関係なく、ブロードキャストまたは NBMA のいずれかに設定できるほか、ポイントツーポイントまたはポイントツーマルチポイントのいずれかに設定することもできます。

OSPF ポイントツーマルチポイント インターフェイスは、1 つまたは複数のネイバーを持つ番号付けされたポイントツーポイント インターフェイスとして定義されます。ポイントツーマルチポイントブロードキャスト ネットワークでは、ネイバーを指定するかどうかは任意です。メディアがブロードキャストをサポートしていない場合にインターフェイスをポイントツーマルチポイントとして設定するには、`neighbor` コマンドを使用してネイバーを指定する必要があります。

■ OSPF の設定

インターフェイスに OSPF ネットワーク タイプを設定するには、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	<code>ip ospf network {broadcast non-broadcast {point-to-multipoint [non-broadcast] point-to-point}}</code>	<p>指定されたインターフェイスに対する OSPF ネットワーク タイプを設定します。次のいずれかのネットワーク タイプを選択します。</p> <ul style="list-style-type: none"> • broadcast : OSPF ブロードキャスト マルチアクセス ネットワークを指定します。 • non-broadcast : OSPF NBMA ネットワークを指定します。 • point-to-multipoint : OSPF ポイントツーマルチポイント ネットワークを指定します。別のキーワードを入力しない場合、インターフェイスはブロードキャスト メディアでポイントツーマルチポイントとなります。 • point-to-multipoint non-broadcast : OSPF 非ブロードキャスト ポイントツーマルチポイント ネットワークを指定します。 • point-to-point : OSPF ポイントツーポイント ネットワークを指定します。
ステップ 5	<code>exit</code>	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	<code>router ospf process-id</code>	(ポイントツーマルチポイントの場合は任意、ポイントツーマルチポイント非ブロードキャストの場合は必須) OSPF 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 7	<code>neighbor ip-address cost number</code>	<p>(ポイントツーマルチポイントの場合は任意、ポイントツーマルチポイント非ブロードキャストの場合は必須) 設定済みの OSPF ネイバーを指定し、そのネイバーにコストを割り当てます。</p> <ul style="list-style-type: none"> • ip-address : OSPF ネイバーのインターフェイス IP アドレスを入力します。 • cost number : ネイバーのコストを 1 ~ 65535 の整数で指定します。 <p>(注) ポイントツーマルチポイントブロードキャスト ネットワークでは、ネイバーを指定するかどうかは任意ですが、ネイバーを指定する場合は、必ずネイバーにコストを指定する必要があります。</p> <p>ポイントツーマルチポイント非ブロードキャスト ネットワークでは、ネイバーを指定する必要がありますが、ネイバーにコストを割り当てるかどうかは任意です。割り当てない場合は、ip ospf cost インターフェイス コンフィギュレーション コマンドに基づいてインターフェイスのコストがネイバーのコストと見なされます。</p>
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	<code>show ip ospf interface [interface-id]</code>	OSPF に関連するインターフェイス情報を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(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。

メディアのネットワーク タイプをデフォルトに戻すには、`ip ospf network` 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

OSPF エリア パラメータは、必要に応じて複数設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への不正アクセスをパスワードによって阻止する認証用パラメータも含まれます。スタブ エリアは、外部ルートに関する情報が送信されないエリアです。ただし、Autonomous System (AS; 自律システム) 外の宛先に対しては、エリア境界ルータ (ABR) によってスタブ エリアへのデフォルトの外部ルートが生成されます。NSSA では、コアからそのエリアへ向かう LSA がすべてフラッドされるわけではありませんが、再配布すればエリア内の AS 外部ルートをインポートできます。

経路集約とは、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 の `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	<code>configure terminal</code>	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	<code>router ospf process-id</code>	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	<code>area area-id authentication</code>	(任意) 指定したエリアに対して、パスワードによる不正アクセスの防止機能を有効にします。ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	<code>area area-id authentication message-digest</code>	(任意) エリアに対して MD5 認証をイネーブルにします。
ステップ 5	<code>area area-id stub [no-summary]</code>	(任意) エリアをスタブ エリアとして定義します。 <code>no-summary</code> キーワードを指定すると、ABR はサマリーリンクアドバタイズメントをスタブ エリアに送信できなくなります。

コマンド	目的
ステップ 6 <code>area area-id nssa [no-redistribution] [default-information-originate] [no-summary]</code>	(任意) エリアを NSSA として定義します。同じエリア内の各ルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 <ul style="list-style-type: none"> • no-redistribution : ルータが NSSA ABR であり、かつ redistribute コマンドを使用してルートを (NSSA ではなく) 通常のエリアへインポートする場合に選択します。 • default-information-originate : NSSA にタイプ 7 LSA をインポートできるようにする場合に ABR で選択します。 • no-redistribution : サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7 <code>area area-id range address mask</code>	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 9 <code>show ip ospf [process-id] show ip ospf [process-id [area-id]] database</code>	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。 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 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

その他の OSPF パラメータの設定

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

- 経路集約：他のプロトコルからのルートを再配布すると（「[ルート マップによるルーティング情報の再配布](#)」(P.36-105) を参照)、各ルータは外部 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、再配布されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID や、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）などが含まれます。仮想リンクは、スタブ エリアを介しては設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配布を設定すると、ルータは自動的に ASBR になります。ASBR は、OSPF ルーティング ドメインへのデフォルト ルートが強制的に生成されるよう設定できます。
- 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、ルータを簡単に特定できます。

- デフォルト メトリック : OSPF では、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 メトリックが計算されます。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。ただし、*ref* のデフォルト値は 10、帯域幅 (*bw*) は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定すると、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、ルーティング情報送信元の信頼性を表す数値です。0 ~ 255 の整数を指定でき、値が大きいほど信頼性は低下します。管理ディスタンスが 255 の場合は、ルーティング情報送信元をまったく信頼できないため、その値は無視してください。OSPF では、エリア内のルート (エリア内)、別のエリアへのルート (エリア間)、および再配布によって学習した別のルーティング ドメインからのルート (外部) という 3 種類の管理ディスタンスが使用されます。これらいずれの管理ディスタンスも値を変更できます。
- 受動インターフェイス : イーサネット上の 2 つのデバイス間に位置するインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに hello パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。この 2 つのデバイスは、受信側インターフェイス宛の hello パケットを介して、相互を認識します。
- ルート計算タイマー : OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールドタイムを設定できます。
- 隣接関係変更ログ : OSPF 近接状態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。

これらの 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、再配布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、その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.36-29)、仮想リンクのデフォルト設定については表 36-5 (P.36-27) 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) OSPF ルーティング ドメインへのデフォルト ルートが強制的に生成されるよう ASBR を設定します。パラメータはすべて任意です。
ステップ 6	ip ospf name-lookup	(任意) DNS 名検索を設定します。デフォルトはディセーブルです。
ステップ 7	ip auto-cost reference-bandwidth ref-bw	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	distance ospf {[inter-area dist1] [inter-area dist2] [external dist3]}	(任意) OSPF 距離の値を変更します。各ルート タイプに対するデフォルトの距離は 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からの hello パケットの送信を抑制します。

	コマンド	目的
ステップ 10	<code>timers throttle spf spf-delay spf-holdtime spf-wait</code>	(任意) ルート計算タイマーを設定します。 <ul style="list-style-type: none"> <code>spf-delay</code> : SPF 計算の変更を受信する間の遅延を指定します。指定できる範囲は 1 ~ 600000 ミリ秒です。 <code>spf-holdtime</code> : 最初と 2 番目の SPF 計算の間の遅延を指定します。指定できる範囲は 1 ~ 600000 ミリ秒です。 <code>spf-wait</code> : SPF 計算の最大待機時間をミリ秒単位で指定します。指定できる範囲は 1 ~ 600000 ミリ秒です。
ステップ 11	<code>ospf log-adj-changes</code>	(任意) 近接状態の変更時に Syslog メッセージを送信します。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip ospf [process-id [area-id]] database</code>	特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「 OSPF のモニタリング 」(P.36-37) を参照してください。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

LSA グループ ペーシングの変更

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用することが可能となります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常、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 インターバルは、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、データベース内に約 10000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース (40 ~ 100 LSA) を使用する場合は、ペーシング インターバルを 10 ~ 20 分と長め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	<code>configure terminal</code>	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	<code>router ospf process-id</code>	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	<code>timers lsa-group-pacing seconds</code>	LSA のグループ ペーシングを変更します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

ループバック インターフェイスの設定

OSPF では、インターフェイス上に設定されている中で最大の IP アドレスが、ルータ ID として使用されます。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は、OSPF プロセスによって新しいルータ ID が再計算され、そのインターフェイスからすべてのルーティング情報が再送信されます。

す。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、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 ではこの IP アドレスがルータ ID として使用されます。ループバック インターフェイスには障害が発生しないため、ループバック インターフェイスを使用することで安定性は増大します。OSPF では、ループバック インターフェイスが他のインターフェイスよりも自動的に優先され、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 アドレスが選択されます。

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

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

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

OSPF のモニタリング

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

表 36-6 は、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たものです。**show ip ospf database** 特権 EXEC コマンドのオプションおよび表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。

表 36-6 IP OSPF 統計情報の表示コマンド

コマンド	目的
show ip ospf [<i>process-id</i>]	OSPF ルーティング プロセスに関する一般的な情報を表示します。
show ip ospf [<i>process-id</i>] database [router] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [router] [self-originate] show ip ospf [<i>process-id</i>] database [router] [adv-router [<i>ip-address</i>]] show ip ospf [<i>process-id</i>] database [network] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [summary] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [asbr-summary] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [external] [<i>link-state-id</i>] show ip ospf [<i>process-id area-id</i>] database [database-summary]	OSPF データベースに関連する情報を表示します。
show ip ospf border-routes	内部 OSPF ルーティングの ABR テーブル エントリおよび ASBR テーブル エントリを表示します。
show ip ospf interface [<i>interface-name</i>]	OSPF に関連するインターフェイス情報を表示します。

表 36-6 IP OSPF 統計情報の表示コマンド

コマンド	目的
<code>show ip ospf neighbor [interface-name] [neighbor-id] detail</code>	OSPF インターフェイスのネイバー情報を表示します。
<code>show ip ospf virtual-links</code>	OSPF に関連する仮想リンク情報を表示します。

EIGRP の設定

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は、使用されるディスタンス ベクトル アルゴリズムおよび距離情報は IGRP と同じですが、コンバージェンス特性および動作効率が大幅に改善されています。

コンバージェンス技術には、Diffusing Update Algorithm (DUAL; Diffusing アップデート アルゴリズム) 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デバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算から除外されます。

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。EIGRP において転送制御フィールドの値が増加するのは、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に限りです。

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- 近隣探索および回復**: 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る場合、または動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。近隣探索および回復は、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実現されます。ネイバーは、hello パケットを受信している限り、動作していると判断されます。動作していると判断されると、隣接ルータはルーティング情報を交換します。
- 信頼できるトランスポート プロトコル**: EIGRP パケットがすべてのネイバーに順序どおり、確実に配信されます。マルチキャスト パケットおよびユニキャスト 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 ネットワークでは、すべてのネイバーそれぞれに対して hello パケットを確実に送信する必要はありません。そのため EIGRP では、マルチキャスト hello を送信する際には、確認応答が不要であることを受信者に知らせるための情報がそのパケット内に格納されます。他のタイプのパケット (アップデートなど) の場合は、確認応答 (ACK パケット) が要求されます。コンバージェンス時間を短縮するため、確認応答のない保留中パケットがある場合には、信頼性の高い転送によってマルチキャスト パケットが迅速に送信されます。
- DUAL 有限状態マシン**: すべてのルート計算に関する決定プロセスが処理されます。DUAL 有限状態マシンでは、すべてのネイバーによりアドバタイズされた全ルートが追跡され、距離情報 (メトリック) に基づいて、ループのない効率的なパスが選択されます。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 パスを持った (ルーティング ループに含まれないことが保証されている)、パケット転送用の隣接ルータです。

適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は、再計算を行って新たな後継ルータを決定する必要があります。ルートの再計算に要する時間によって、コンバージェンス時間は変わります。トポロジが変更された場合、DUAL では、不要な再計算を省略するために、適切な後継ルータが存在するかどうかのテストが行われます。

- **プロトコル依存モジュール**: ネットワーク レイヤ プロトコル固有の作業を行います。たとえば、IP でカプセル化された EIGRP パケットの送受信を行う IP EIGRP モジュールは、プロトコル依存モジュールの 1 つです。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 に通知する作業を行います。ルーティングの決定結果は IP ルーティング テーブルに格納されます。また EIGRP では、他の IP ルーティング プロトコルにより学習されたルートが再配布されます。

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」(P.36-39)
- 「基本的な EIGRP パラメータの設定」(P.36-40)
- 「EIGRP インターフェイスの設定」(P.36-41)
- 「EIGRP ルート認証の設定」(P.36-42)
- 「EIGRP スタブ ルーティングの設定」(P.36-43)
- 「EIGRP のモニタリングおよびメンテナンス」(P.36-45)

EIGRP のデフォルト設定

表 36-7、パート 1 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、この境界にサブプレフィクスが集約される。
デフォルト情報	再配布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の受け渡しが行われる。
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布できるのは、接続されたルートおよびインターフェイスのスタティック ルートに限る。デフォルト メトリックは次のとおり。 <ul style="list-style-type: none"> • 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数。 • 信頼性: 0 ~ 255 の任意の数値 (255 の場合は信頼性が 100%)。 • 負荷: 0 ~ 255 の数値で表される有効帯域幅 (255 の場合は 100% の負荷)。 • MTU: バイトで表されたルートの MTU サイズ (0 または任意の正の整数)。
距離	内部距離: 90。 外部距離: 170。
EIGRP の隣接関係変更ログ	ディセーブル。隣接関係変更はロギングされない。
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 インターバル	低速 NBMA ネットワーク: 60 秒。それ以外のネットワーク: 5 秒。
IP ホールドタイム	低速 NBMA ネットワーク: 180 秒。それ以外のネットワーク: 15 秒。
IP スプリット ホライズン	イネーブル。
IP サマリー アドレス	サマリー集約アドレスは未定義。
メトリックの重み	tos: 0、k1 および k3: 1、k2、k4、および k5: 0。

表 36-7、パート 1 EIGRP のデフォルト設定 (続き)

機能	デフォルト設定
ネットワーク	指定なし。
NSF ¹ 認識	イネーブル ² 。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
オフセットリスト	ディセーブル。
ルータ EIGRP	ディセーブル。
メトリック設定	ルート マップにはメトリック設定なし。
トラフィック共有	メトリックの比率に応じて配分。
分散	1 (等価コストロード バランシング)。

1. NSF = Nonstop Forwarding (ノンストップフォワーディング)

2. EIGRP NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP では、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が送信されます。インターフェイス ネットワークを指定しない場合は、どの EIGRP アップデートでもアドバタイズされません。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、EIGRP NSF 認識機能がサポートされています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア 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、隣接ルータからのパケットが転送され続けます。


この機能は、ディセーブルにできません。この機能に関する詳細については、次の URL にある『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_guide09186a0080160010.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	<code>configure terminal</code>	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	<code>router eigrp autonomous-system</code>	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 番号は、他の EIGRP ルータへのルートを識別するためのもので、ルーティング情報のタグ付けに使用されます。
ステップ 3	<code>network network-number</code>	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 では、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が送信されます。

コマンド	目的
ステップ4 <code>eigrp log-neighbor-changes</code>	(任意) EIGRP 隣接関係変更のログをイネーブルにし、ルーティングシステムの安定性をモニタします。
ステップ5 <code>metric weights tos k1 k2 k3 k4 k5</code>	(任意) EIGRP メトリックを調整します。デフォルト値は、多くのネットワークが適切に動作するように配慮して設定されていますが、必要であれば調整することも可能です。  注意 メトリックの設定は複雑な作業です。メトリックの設定は熟練したネットワーク設計者の指導のもとで行ってください。
ステップ6 <code>offset list [access-list number name] {in out} offset [type number]</code>	(任意) オフセットリストをルーティングメトリックに適用し、EIGRP によって学習したルートへの着信メトリックおよび発信メトリックの値を増やします。オフセットリストは、アクセスリストまたはインターフェイスを使用して制限できます。
ステップ7 <code>no auto-summary</code>	(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 <code>ip summary-address eigrp autonomous-system-number address mask</code>	(任意) サマリー集約を設定します。
ステップ9 <code>end</code>	特権 EXEC モードに戻ります。
ステップ10 <code>show ip protocols</code>	設定を確認します。 NSF 認識の場合、出力には次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ11 <code>copy running-config startup-config</code>	(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、または設定をデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。


EIGRP インターフェイスの設定

他の任意の EIGRP パラメータは、インターフェイスごとに設定できます。

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 <code>configure terminal</code>	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 <code>interface interface-id</code>	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 <code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ4 <code>ip bandwidth-percent eigrp percent</code>	(任意) インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。

EIGRP の設定

コマンド	目的
ステップ 5 ip summary-address eigrp <i>autonomous-system-number address mask</i>	(任意) 指定されたインターフェイスのサマリー集約アドレスを設定します (auto-summary がイネーブルの場合は、通常設定する必要はありません)。
ステップ 6 ip hello-interval eigrp <i>autonomous-system-number seconds</i>	(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。デフォルトは、低速 NBMA ネットワークでは 60 秒、その他すべてのネットワークでは 5 秒です。
ステップ 7 ip hold-time eigrp <i>autonomous-system-number seconds</i>	(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。デフォルトは、低速 NBMA ネットワークでは 180 秒、その他すべてのネットワークでは 15 秒です。  注意 ホールドタイムを調整する場合は、事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 8 no ip split-horizon eigrp <i>autonomous-system-number</i>	(任意) スプリット ホライズンをディセーブルにし、ルート情報がその送信元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 9 end	特権 EXEC モードに戻ります。
ステップ 10 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 11 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

EIGRP ルート認証の設定

EIGRP ルート認証を設定すると、EIGRP ルーティング プロトコルからのルーティング アップデートに対して MD5 認証が実行されます。これにより、承認されていない送信元からの不正なルーティング メッセージや問題のあるルーティング メッセージの受信を回避できます。

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 <i>interface-id</i>	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 shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

コマンド	目的
ステップ 4 <code>ip authentication mode eigrp autonomous-system md5</code>	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 5 <code>ip authentication key-chain eigrp autonomous-system key-chain</code>	IP EIGRP パケットの認証をイネーブルにします。
ステップ 6 <code>exit</code>	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 <code>key chain name-of-chain</code>	キーチェーンを指定し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定したものと同名を指定します。
ステップ 8 <code>key number</code>	キーチェーン コンフィギュレーション モードで、鍵番号を指定します。
ステップ 9 <code>key-string text</code>	キーチェーン コンフィギュレーション モードで、キー字符串を指定します。
ステップ 10 <code>accept-lifetime start-time {infinite end-time duration seconds}</code>	(任意) 鍵を受信できる期間を指定します。 <i>start-time</i> および <i>end-time</i> の構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。 <i>end-time</i> および duration のデフォルトは infinite です。
ステップ 11 <code>send-lifetime start-time {infinite end-time duration seconds}</code>	(任意) 鍵を送信できる期間を指定します。 <i>start-time</i> および <i>end-time</i> の構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。 <i>end-time</i> および duration のデフォルトは infinite です。
ステップ 12 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 13 <code>show key chain</code>	認証鍵情報を表示します。
ステップ 14 <code>copy running-config startup-config</code>	(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場合、または設定をデフォルト値に戻すには、上記コマンドの **no** 形式を使用します。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能を使用すると、ルーテッドトラフィックをエンドユーザの近くへ移動することで、リソースの使用量を軽減できます。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 トラフィックに対して許可されたルートだけが、EIGRP スタブ ルーティングが設定されたスイッチを通過できます。スイッチでは、ユーザのインターフェイスとして設定された、または他のデバイスに接続されたインターフェイスへ、ルーテッドトラフィックが送信されます。

EIGRP スタブ ルーティングを使用する場合は、EIGRP が使用されるように配信ルータおよびリモートルータを設定し、スイッチだけをスタブとして設定する必要があります。スイッチからは、指定したルートだけが伝播されます。スイッチは、サマリー、接続されたルート、およびルーティングアップデートに関するすべてのクエリーに応答します。



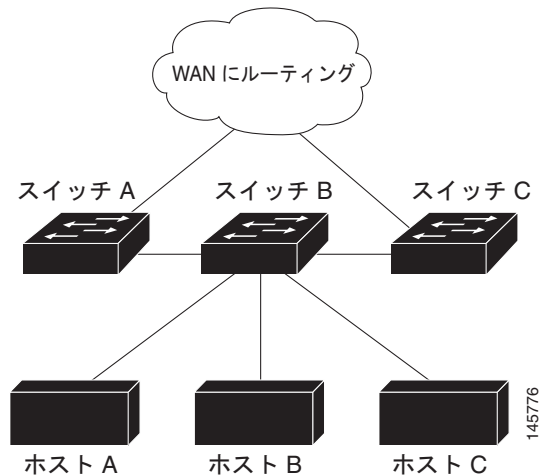
(注)

EIGRP タブ ルーティングでは、接続されたルートまたはサマリー ルートに限り、ルーティング テーブルからネットワーク内の別のスイッチへアドバタイズされます。スイッチでは、アクセス レイヤでの EIGRP スタブ ルーティングにより、その他のタイプのルーティング アドバタイズメントが不要になります。マルチ VRF-CE と EIGRP スタブ ルーティングは、同時には設定できません。

スタブ ステータスを知らせるパケットを受信したネイバーは、スタブ ルータに対してルートに関するクエリーを送信しません。また、スタブ ピアを持つルータが、そのピアに対してクエリーを送信することはありません。スタブ ルータからすべてのピアへ適切なアップデートが送信される場合、その処理は配信ルータが行います。

図 36-4 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 およびスイッチ C は、外部の WAN に接続されています。スイッチ B からは、接続されたスタティックルート、再配布ルート、およびサマリー ルートがスイッチ A およびスイッチ C へアドバタイズされます。スイッチ B では、スイッチ A から学習したルートはアドバタイズされません（同様にスイッチ A でも、スイッチ B から学習されたルートはアドバタイズされません）。

図 36-4 EIGRP スタブ ルータの設定



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

EIGRP スタブ ルーティング用のリモート 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 <code>configure terminal</code>	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 <code>router eigrp 1</code>	EIGRP プロセスが実行されるようにリモート ルータまたは配信ルータを設定し、ルータ コンフィギュレーション モードを開始します。

コマンド	目的
ステップ3 <code>network network-number</code>	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。
ステップ4 <code>eigrp stub [receive-only connected static summary]</code>	リモート ルータを EIGRP スタブ ルータとして設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • receive-only : ルータを受信専用ネイバーとして設定する場合に入力します。 • connected : 接続されたルートをアドバタイズする場合に入力します。 • static : スタティック ルートをアドバタイズする場合に入力します。 • summary : サマリー ルートをアドバタイズする場合に入力します。
ステップ5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ6 <code>show ip eigrp neighbor detail</code>	リモート ルータが EIGRP スタブ ルータとして設定されたことを確認します。出力の最後の行には、リモート ルータまたはスポーク ルータのスタブ ステータスが表示されます。
ステップ7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定を確認するには、配信ルータから `show ip eigrp neighbor detail` 特権 EXEC コマンドを入力します。

EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。また、EIGRP ルーティングに関するさまざまな統計情報を表示できます。表 36-8 は、ネイバーの削除および統計情報の表示に使用できる特権 EXEC コマンドをまとめたものです。表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2 を参照してください。

表 36-8 IP EIGRP の clear コマンドおよび show コマンド

コマンド	目的
<code>clear ip eigrp neighbors [if-address interface]</code>	ネイバー テーブルからネイバーを削除します。
<code>show ip eigrp interface [interface] [as number]</code>	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。
<code>show ip eigrp neighbors [type-number]</code>	EIGRP によって検出されたネイバーを表示します。
<code>show ip eigrp topology [autonomous-system-number] [[ip-address] mask]</code>	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。
<code>show ip eigrp traffic [autonomous-system-number]</code>	すべてまたは特定の EIGRP プロセスの送受信パケット数を表示します。

BGP の設定

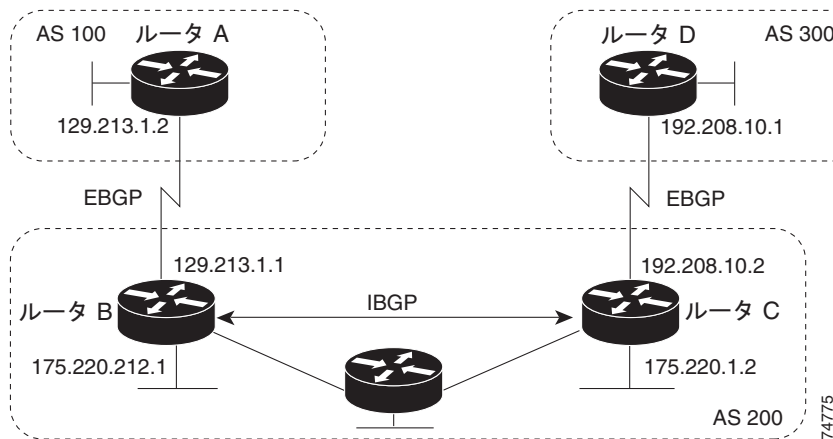
BGP は、Exterior Gateway Protocol (EGP; 外部ゲートウェイ プロトコル) です。AS 間で、ループの発生しないルーティング情報交換を行うためのドメイン間ルーティング システムを設定する際に使用されます。AS は、共通の管理の下で動作する複数のルータにより構成されます。EGP を介して相互に接続されたこれらのルータによって、RIP や OSPF などの IGP が境界内で実行されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。

BGP に関する詳細については、『Internet Routing Architectures』(Cisco Press 刊)、および『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring BGP」を参照してください。

BGP 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 の「IP Routing Protocols」を参照してください。表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C 「Cisco IOS リリース 12.2(52)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 AS に属するルータは *Internal BGP* (IBGP; 内部 BGP) を実行し、異なる AS に属するルータは *External BGP* (EBGP; 外部 BGP) を実行します。コンフィギュレーション コマンドの機能は、EBGP を設定する場合と IBGP を設定する場合ではほぼ同じです。異なるのは、ルーティング アップデートが AS 間で交換されるか (EBGP)、AS 内で交換されるか (IBGP) という点です。図 36-5 は、EBGP と IBGP がともに稼動しているネットワークを示したものです。

図 36-5 EBGP、IBGP、および複数の AS



外部 AS と情報を交換する前に、BGP では、AS 内のネットワークに必ず到達できるように、AS 内のルータ間で内部 BGP ピアリングが定義され、IGRP や OSPF など AS 内で稼動する IGP に BGP ルーティング情報が再配布されます。

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 では、トランスポート プロトコルとして TCP (特にポート 179) が使用されます。ルーティング情報を交換するため相互に 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 36-5 では、ルータ A とルータ B、ルータ B とルータ C、ルータ C とルータ D がそれぞれ BGP ピアを構成しています。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 では、この情報を基にしてループのない AS マップが作成されます。

このネットワークの特徴は次のとおりです。

- ルータ A およびルータ B では EBGP が、ルータ B およびルータ 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できるのであれば、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、論理的には完全メッシュ型に接続する必要があります。BGP4 により実現される *連合* および *ルート リフレクタ* という 2 つの技術を使用すると、論理的な完全メッシュ型を構成するための要件を緩和できます。
- 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。また BGP ピアは、キープアライブ メッセージ (接続が有効であることを確認)、および通知メッセージ (エラーまたは特殊条件に応答) 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 AS のリスト (AS パス)、および他のパス アトリビュート 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、ネットワークの到達可能性情報を他の BGP システムと交換することにあります。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 ポリシー判断を行ったりする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には、ネクスト ホップ ルータで使用可能なルートがあり、かつ IGP から同期信号を受信している (IGP 同期がディセーブルの場合は除く) 場合です。複数のルートが使用可能な場合、BGP ではアトリビュート値に基づいてパスが選択されます。BGP アトリビュートの詳細については、「[BGP 判断アトリビュートの設定](#)」(P.36-54) を参照してください。

BGP バージョン 4 では Classless Interdomain Routing (CIDR; クラスレス ドメイン間ルーティング) がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。CIDR により、BGP 内部のネットワーク クラスという概念は不要になり、IP プレフィックスのアドバタイズがサポートされます。

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.36-48)
- 「[BGP ルーティングのイネーブル化](#)」(P.36-50)
- 「[ルーティング ポリシー変更の管理](#)」(P.36-52)
- 「[BGP 判断アトリビュートの設定](#)」(P.36-54)
- 「[ルート マップによる BGP フィルタリングの設定](#)」(P.36-56)
- 「[ネイバー単位での BGP フィルタリングの設定](#)」(P.36-57)
- 「[BGP フィルタリング用のプレフィックス リストの設定](#)」(P.36-58)
- 「[BGP コミュニティ フィルタリングの設定](#)」(P.36-59)
- 「[BGP ネイバーおよびピア グループの設定](#)」(P.36-61)
- 「[集約アドレスの設定](#)」(P.36-63)
- 「[ルーティング ドメイン連合の設定](#)」(P.36-63)
- 「[BGP ルート リフレクタの設定](#)」(P.36-64)
- 「[ルート ダンプニングの設定](#)」(P.36-65)
- 「[BGP のモニタリングおよびメンテナンス](#)」(P.36-66)

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」を参照してください。特定のコマンドに関する詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。また、表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C 「Cisco IOS リリース 12.2(52)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 36-9 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	<ul style="list-style-type: none"> ルータはルートを選択する場合に AS パスを考慮するが、外部 BGP ピアからの類似ルートは比較されない。 ルータ ID の比較：ディセーブル。
BGP コミュニティ リスト	<ul style="list-style-type: none"> 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、暗黙的に拒否されるようデフォルト設定される。 フォーマット：シスコ デフォルト フォーマット (32 ビット番号)
BGP 連合 ID/ピア	<ul style="list-style-type: none"> ID：設定なし。 ピア：指定なし。
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 (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	デフォルトでディセーブル。イネーブルの場合は、次のとおり。 <ul style="list-style-type: none"> 半減期は 15 分。 再使用は 750 (10 秒増分)。 抑制は 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 (設定されている場合)、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。
デフォルト情報の送信 (プロトコルまたはネットワーク再配布)	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)。
距離	<ul style="list-style-type: none"> 外部ルートの管理ディスタンス：20 (指定できる範囲は 1 ~ 255) 内部ルートの管理ディスタンス：200 (指定できる範囲は 1 ~ 255) ローカル ルートの管理ディスタンス：200 (指定できる範囲は 1 ~ 255)
配布リスト	<ul style="list-style-type: none"> 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。
内部ルート再配布	ディセーブル。
IP プレフィクス リスト	定義なし。

表 36-9 BGP のデフォルト設定 (続き)

機能	デフォルト設定
Multi Exit Discriminator (MED)	<ul style="list-style-type: none"> 常に比較：ディセーブル。異なる AS 内のネイバーからのパスについては MED を比較しない。 最適パスの比較：ディセーブル。 最悪パスである MED の除外：ディセーブル。 決定的な MED 比較：ディセーブル。
Neighbor	<ul style="list-style-type: none"> アドバタイズメント インターバル：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒。 変更ロギング：イネーブル。 条件付きアドバタイズメント：ディセーブル。 デフォルトの送信：ネイバーにデフォルト ルートは送信されない。 説明：なし。 配布リスト：定義なし。 外部 BGP マルチホップ：直接接続されたネイバーに限り許可。 フィルタ リスト：使用しない。 受信されるプレフィックスの最大数：制限なし。
Neighbor	<ul style="list-style-type: none"> 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。割り当てられたメンバーなし。 プレフィックス リスト：指定なし。 リモート AS (ネイバーの BGP テーブルにエントリを追加)：定義されたピアなし。 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 アトリビュートの送信：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：イネーブルでない。 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 バージョン 4。 重み：BGP ピアを介して学習したルートの場合は 0、ローカル ルータからのルートの場合は 32768。
NSF ¹ 認識	ディセーブル ² 。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
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 = Nonstop Forwarding (ノンストップ フォワーディング)

2. メトロ IP アクセス イメージが実行されているスイッチ上の IPv4 に対しては、グレースフル リスタートをイネーブルにすることにより、BGP NSF 認識をイネーブルにできます。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、BGP NSF 認識機能がサポートされています。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。隣接ルータが NSF 対応である場合、この機能をイネーブルにすると、レイヤ 3 スイッチでは、ルータ内で障害が発生したプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断することなくソフトウェア 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、隣接ルータからのパケットが転送され続けます。

詳細については、次の URL にある『*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ためには、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する必要があります。BGP はネイバーとの関係を完全に認識するため、BGP ネイバーについても指定する必要があります。

BGP では、内部ネイバーおよび外部ネイバーという 2 種類のネイバーがサポートされています。内部ネイバーは同じ AS 内にあるネイバー、外部ネイバーは異なる AS 内にあるネイバーのことです。通常、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ 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 番号は、64512 ~ 65535 の範囲で指定できます。neighbor remove-private-as ルータ コンフィギュレーション コマンドを使用すると、AS パスからプライベート AS 番号が削除されるように外部ネイバーを設定できます。これにより、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、これらの番号が削除されます。

AS が別の AS から受け取ったトラフィックをさらに別の AS に渡す場合は、アドバタイズ対象のルートに矛盾がないことが重要です。BGP によりルートがアドバタイズされてから、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、IGP により AS に情報が伝播され BGP が IGP と同期化されるまで、BGP は待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が別の AS から受け取ったトラフィックをその他の AS へ渡さない場合、または AS 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て、IGP 内で伝送されるルート数を少なくし、BGP のコンバージェンス時間を短縮します。

BGP ルーティングをイネーブルにし、BGP ルーティング プロセスを確立して、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	<code>configure terminal</code>	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	<code>ip routing</code>	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須)。
ステップ 3	<code>router bgp autonomous-system</code>	BGP ルーティング プロセスをイネーブルにして、それに 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 AS 番号専用です。

	コマンド	目的
ステップ 4	network <i>network-number</i> [mask <i>network-mask</i>] [route-map <i>route-map-name</i>]	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、そのネットワークを BGP テーブルに格納します。
ステップ 5	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i>	BGP ネイバー テーブルにエントリを追加し、IP アドレスで指定したネイバーが、指定された AS に属するようにします。 EBGP では、通常ネイバーは直接接続されており、IP アドレスは接続の他端に位置するインターフェイスのアドレスです。 IBGP では、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6	neighbor { <i>ip-address</i> <i>peer-group-name</i> } 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 の同期化をディセーブルにします。
ステップ 8	no auto-summary	(任意) 自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配布された場合、ネットワーク ルートだけが BGP テーブルに追加されます。
ステップ 9	bgp fast-external-falover	(任意) 外部ネイバー間のリンクが切断された場合、BGP セッションが自動的にリセットされるようにします。デフォルトの場合、セッションは即座にはリセットされません。
ステップ 10	bgp graceful-restart	(任意) スイッチ上の NSF 認識をイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show ip bgp network <i>network-number</i> or 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であることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised and received</i> NSF 認識がスイッチではイネーブル、ネイバーではディセーブルの場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised</i>
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP 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。同期化を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 36-5 の各ルータ上で 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 にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors

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

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、ルータ上の最大の IP アドレス（または最大のループバック インターフェイス）です。テーブルは、新規情報によりアップデートされるたびに、そのバージョン番号が増加します。継続的にテーブルバージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生していると判断できます。

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

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide*』 Release 12.2 の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』 Release 12.2 を参照してください。表示されるにもかかわらずスイッチでサポートされていない BGP コマンドについては、付録 C「Cisco IOS リリース 12.2(52)SE でサポートされていないコマンド」を参照してください。

ルーティング ポリシー変更の管理

ピアのルーティング ポリシーには、着信ルーティング テーブル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のある設定がすべて含まれています。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。そのあとで BGP 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には、BGP セッションをリセットし、設定の変更内容を有効にする必要があります。

リセットには、ハードリセットとソフトリセットの 2 つのタイプがあります。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場合、スイッチでは事前に設定を行うことなくソフトリセットを使用できます。ソフトルート リフレッシュ機能は、ピアによって TCP セッションが確

立されたときに送信される OPEN メッセージによりアドバタイズされます。ソフト リセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報を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、このリセットを *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、このリセットを *発信ソフト リセット* といいます。

ソフト着信リセットを実行すると、新規着信ポリシーが有効になります。ソフト発信リセットを実行すると、BGP セッションがリセットされることなく、新規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アップデートが新たに送信されると、新しい着信ポリシーが有効になる場合があります。

表 36-10 ハード リセットとソフト リセットの長所および短所

リセットタイプ	長所	短所
ハード リセット	メモリ オーバーヘッドが発生しません。	ネイバーから取得した BGP テーブル、IP テーブル、および Forwarding Information Base (FIB; 転送情報ベース) テーブル内のプレフィクスが失われます。推奨されません。
発信ソフト リセット	ルーティング テーブル アップデートが設定、保存されません。	着信ルーティング テーブル アップデートがリセットされません。
ダイナミック着信ソフト リセット	BGP セッションおよびキャッシュが消去されません。 ルーティング テーブル アップデートを保存する必要がなく、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 リフレッシュ機能がサポートされている必要があります。

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を確認し、BGP セッションをリセットするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>show ip bgp neighbors</code>	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。 <i>Received route refresh capability from peer</i>
ステップ2 <code>clear ip bgp {* address peer-group-name}</code>	指定された接続上でルーティング テーブルをリセットします。 <ul style="list-style-type: none"> • すべての接続をリセットするには、アスタリスク (*) を入力します。 • 特定の接続をリセットするには、IP アドレスを入力します。 • ピア グループをリセットするには、そのピア グループ名を入力します。

コマンド	目的
ステップ3 <code>clear ip bgp {* address peer-group-name} soft out</code>	<p>(任意) 発信ソフトリセットを実行して、指定された接続上で着信ルーティングテーブルをリセットします。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。</p> <ul style="list-style-type: none"> すべての接続をリセットするには、アスタリスク (*) を入力します。 特定の接続をリセットするには、IP アドレスを入力します。 ピアグループをリセットするには、そのピアグループ名を入力します。
ステップ4 <code>show ip bgp</code> <code>show ip bgp neighbors</code>	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 判断アトリビュートの設定

BGP スピーカーが複数の AS から受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。この判断は、アップデートに格納されているアトリビュート値、および BGP で設定可能なその他の基準に基づいて行われます。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。

BGP ピアは、プレフィクスに対する 2 つの EBGp パスをネイバー AS から学習する際、最適パスを選択し、それを 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の場合、同じネイバー AS から複数の EBGp パスを学習すると、IP ルーティングテーブルには複数のパスが格納されます。さらに、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で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 コマンドを使用すると、許可されるパス数を制御できます。

これらの要因により、BGP が最適パスを選択するためにアトリビュートを評価する際の基準と評価する順序が決定されます。

1. パスで指定されているネクストホップが到達不能な場合、このアップデートは廃棄されます。BGP のネクストホップアトリビュート (ソフトウェアによって自動判別される) は、宛先へ到達するために使用されるネクストホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルートマップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 重み (シスコ独自のパラメータ) が最大であるパスを優先します。重みアトリビュートはルータに対して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関する重みアトリビュートは 32768 で、それ以外のパスの重みアトリビュートは 0 です。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であるルートを優先します。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アトリビュートのデフォルト値は 100 です。ローカルプリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルートマップを使用します。
4. ローカルルータ上で稼働する BGP から送信されたルートを優先します。
5. AS パスが最短のルートを優先します。
6. 送信元タイプが最小のルートを優先します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP によって学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。

7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック アトリビュートが最小のルートを優先します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部 (IBGP) パスより、外部 (EBGP) パスを優先します。
9. 最も近い IGP ネイバー (最小の IGP メトリック) を通って到達できるルートを優先します。この場合、ルータは、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) を使用して宛先に到達します。
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 テーブルに挿入します。
 - 最適ルートと目的のルートがともに外部ルートである
 - 最適ルートと目的のルートの両方が、同じネイバー AS からのルートである
 - **maximum-paths** がイネーブルである
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを優先します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック (仮想) アドレスですが、場合によっては実装に依存します。

判断アトリビュ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	router bgp <i>autonomous-system</i>	BGP ルーティング プロセスをイネーブルにして、それに 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) ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	neighbor {<i>ip-address</i> <i>peer-group-name</i>} next-hop-self	(任意) ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	neighbor {<i>ip-address</i> <i>peer-group-name</i>} weight <i>weight</i>	(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。重み最大のルートが優先されるルートです。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	default-metric <i>number</i>	(任意) 優先されるパスが外部ネイバーに設定されるように MED メトリックを設定します。MED を持たないルータもすべて、この値に設定されます。指定できる範囲は 1 ~ 4294967295 です。この値が最小であるパスが最優先されます。
ステップ 7	bgp bestpath med missing-as-worst	(任意) MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	bgp always-compare med	(任意) 異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間に限って比較されます。

■ BGP の設定

	コマンド	目的
ステップ 9	<code>bgp bestpath med confed</code>	(任意) 連合内の異なるサブ AS によってアドバタイズされたパスの中から特定のパスを選択する場合に、MED を考慮するようスイッチを設定します。
ステップ 10	<code>bgp deterministic med</code>	(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の中から選択する場合に、MED 変数を考慮するようスイッチを設定します。
ステップ 11	<code>bgp default local-preference value</code>	(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、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を持つパスが優先されます。
ステップ 12	<code>maximum-paths number</code>	(任意) IP ルーティングテーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティングテーブルに追加されます。指定できる範囲は 1 ~ 8 です。複数のパスが追加されると、パス間のロードバランシングが可能になります。
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show ip bgp</code> <code>show ip bgp neighbors</code>	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	<code>copy running-config startup-config</code>	(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。

デフォルト状態に戻すには、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、ルーティング情報を制御、変更したり、ルーティング ドメイン間でルートを再配布する条件を定義したりできます。ルート マップの詳細については、「[ルート マップによるルーティング情報の再配布](#)」(P.36-105) を参照してください。各ルート マップには、ルート マップを識別する名前 (マップ タグ) およびオプションのシーケンス番号が付いています。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>route-map map-tag [[permit deny] sequence-number]]</code>	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 3	<code>set ip next-hop ip-address [...ip-address] [peer-address]</code>	(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。 <ul style="list-style-type: none"> 着信ルート マップの場合は、一致するルートのネクストホップをネイバー ピア アドレスに設定し、サードパーティのネクストホップを上書きします。 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 アドレスに設定して、ネクストホップ計算をディセーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ5 <code>show route-map [map-name]</code>	設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

ネイバー単位での BGP フィルタリングの設定

BGP アドバタイズメントをフィルタリングするには、`as-path access-list` グローバル コンフィギュレーション コマンドや `neighbor filter-list` ルータ コンフィギュレーション コマンドなどの 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.36-114) を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、各アトリビュートを変更したりできます。ルート マップは、着信アップデートまたは発信アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデートで送信または許可されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づく照合がサポートされています。AS パスの照合には `match as-path access-list` ルート マップ コマンド、コミュニティに基づく照合には `match community-list` ルート マップ コマンド、ネットワークに基づく照合には `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 <code>configure terminal</code>	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 <code>router bgp autonomous-system</code>	BGP ルーティング プロセスをイネーブルにして、それに 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 <code>neighbor {ip-address peer-group name} distribute-list {access-list-number name} {in out}</code>	(任意) アクセス リストの指定に従って、ネイバーとの間で送受信される 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) <code>neighbor prefix-list</code> 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も同じ BGP ピアを設定できません。
ステップ4 <code>neighbor {ip-address peer-group name} route-map map-tag {in out}</code>	(任意) ルート マップを適用し、着信ルートまたは発信ルートをフィルタリングします。
ステップ5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ6 <code>show ip bgp neighbors</code>	設定を確認します。
ステップ7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

BGP 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する必要があります。

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	<code>configure terminal</code>	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	<code>ip as-path access-list access-list-number {permit deny} as-regular-expressions</code>	BGP 関連アクセス リストを定義します。
ステップ 3	<code>router bgp autonomous-system</code>	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	<code>neighbor {ip-address peer-group name} filter-list {access-list-number name} {in out weight weight}</code>	アクセス リストに基づいて、BGP フィルタを作成します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp neighbors [paths regular-expression]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィクス リストの設定

neighbor distribute-list ルータ コンフィギュレーション コマンドなどの多数の 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 リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィクス 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。一致するルートが存在する場合は、そのルートが使用されます。プレフィクスが許可されるか、または拒否されるかは、次に示す規則に基づいて決定されます。

- プレフィクス リストが空の場合は、すべてのプレフィクスが許可されます。
- 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트리とも一致しない場合は、暗黙的に拒否されたと見なされます。
- 指定されたプレフィクスと一致するエントリがプレフィクス リスト内に複数存在する場合は、シーケンス番号が最小であるプレフィクス リスト エントリが特定されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合、そのリストには追加エントリを挿入できません。また、増分値として大きな値を選択すると、値が不足する可能性があります。

コンフィギュレーション エントリを削除するときは、シーケンス番号を指定する必要はありません。

show コマンドの出力にも、シーケンス番号が表示されます。

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 リストを作成する、またはプレフィクス リストにエントリを追加するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip prefix-list list-name [seq seq-value] deny permit network/len [ge ge-value] [le le-value]	照合する条件に合わせて、アクセスを拒否 (deny) または許可 (permit) するプレフィクス リストを作成します。シーケンス番号を指定することもできます。 permit 句または deny 句を少なくとも 1 つ入力する必要があります。 <ul style="list-style-type: none"> network/len には、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) を指定します。 (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表します。ge-value および le-value に指定する値は、$len < ge-value < le-value < 32$ という条件を満たしていることが必要です。
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) コンフィギュレーション ファイルに設定を保存します。

プレフィクス リストまたはそのエントリをすべて削除するには、**no ip prefix-list list-name** グローバル コンフィギュレーション コマンドを使用します。プレフィクス リストから特定の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場合は **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消去するには、**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 アトリビュートの値を基に BGP でルーティング情報の配布を制御する方法の 1 つです。コミュニティは、共通するいくつかのアトリビュート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もあります。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、推移的でグローバルな、オプションの COMMUNITIES アトリビュート (1 ~ 4294967200) によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

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

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

コミュニティリストを使用すると、ルート マップの `match` 句で使用されるコミュニティ グループを作成できます。さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。文のチェックは、一致が検出されるまで続けられ、いずれか 1 つの文に一致した時点で、テストは終了します。

コミュニティに基づいて COMMUNITIES アトリビュートおよび `match` 句を設定するには、「[ルート マップによるルーティング情報の再配布](#)」(P.36-105) に記載されている `match community-list` ルートマップ コンフィギュレーション コマンドおよび `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、ネイバーに COMMUNITIES アトリビュートは送信されません。COMMUNITIES アトリビュートが特定の IP アドレスのネイバーに送信されるように指定するには、`neighbor send-community` ルータ コンフィギュレーション コマンドを使用します。

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

コマンド	目的
ステップ 1 <code>configure terminal</code>	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 <code>ip community-list community-list-number {permit deny} community-number</code>	コミュニティ リストを作成し、それに番号を割り当てます。 <ul style="list-style-type: none"> <code>community-list-number</code> には 1 ~ 99 の整数を指定します。この値により、1 つまたは複数のコミュニティの許可グループまたは拒否グループが識別されます。 <code>community-number</code> には、<code>set community</code> 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を指定します。
ステップ 3 <code>router bgp autonomous-system</code>	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 <code>neighbor {ip-address peer-group name} send-community</code>	この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 5 <code>set comm-list list-num delete</code>	(任意) ルート マップで指定された標準または拡張のコミュニティ リストと一致する着信アップデートまたは発信アップデートのコミュニティ アトリビュートから、コミュニティを削除します。
ステップ 6 <code>exit</code>	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 <code>ip bgp-community new-format</code>	(任意) AA:NN のフォーマットで BGP コミュニティを表示し、解析を行います。 BGP コミュニティは、2 つの部分からなる 2 バイト長フォーマットで表示されます。シスコのデフォルトのコミュニティ フォーマットは NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN のフォーマットをとります。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 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 9 <code>show ip bgp community</code>	設定を確認します。
ステップ 10 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

通常は、多数の BGP ネイバーに同一のアップデート ポリシー（同じ発信ルート マップ、配布リスト、フィルタ リスト、アップデート送信元など）が設定されます。アップデート ポリシーが同じであるネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加する必要があります。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。また、すべてのピア グループ メンバーが、ピア グループに対する変更を継承します。さらには、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 アドレスを使用して、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て、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、いずれの設定情報も削除することなく、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。 remote-as number を使用してピア グループが設定されていない場合は、このコマンドを使用して、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。
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送信する COMMUNITIES アトリビュートを指定します。
ステップ 9 neighbor {ip-address peer-group-name} update-source interface	(任意) IBGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10 neighbor {ip-address peer-group-name} ebgp-multihop	(任意) ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート (0.0.0.0) の場合、マルチホップ セッションは確立されません。
ステップ 11 neighbor {ip-address peer-group-name} local-as number	(任意) ローカル 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。

■ BGP の設定

	コマンド	目的
ステップ 12	neighbor { <i>ip-address</i> <i>peer-group-name</i> } advertisement-interval <i>seconds</i>	(任意) BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	neighbor { <i>ip-address</i> <i>peer-group-name</i> } maximum-prefix <i>maximum</i> [<i>threshold</i>]	(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。 <i>threshold</i> (任意) は、警告メッセージが生成される基準となる最大値 (パーセント) です。デフォルト値は 75% です。
ステップ 14	neighbor { <i>ip-address</i> <i>peer-group-name</i> } next-hop-self	(任意) ネイバー宛の BGP アップデートに関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 15	neighbor { <i>ip-address</i> <i>peer-group-name</i> } password <i>string</i>	(任意) TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>map-name</i> { in out }	(任意) 着信ルート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 { <i>ip-address</i> <i>peer-group-name</i> } send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 18	neighbor { <i>ip-address</i> <i>peer-group-name</i> } timers <i>keepalive holdtime</i>	(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。 <ul style="list-style-type: none"> • <i>keepalive</i> には、キープアライブ メッセージがピアに送信される時間間隔を指定します。指定できる範囲は 1 ~ 4294967295 秒で、デフォルトは 60 秒です。 • <i>holdtime</i> には、キープアライブ メッセージを受信しなかった場合にピアが非アクティブと宣言されるまでの時間間隔を指定します。指定できる範囲は 1 ~ 4294967295 秒で、デフォルトは 180 秒です。
ステップ 19	neighbor { <i>ip-address</i> <i>peer-group-name</i> } weight <i>weight</i>	(任意) ネイバーからのすべてのルートに対して重みを指定します。
ステップ 20	neighbor { <i>ip-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-number</i> <i>name</i> } { 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 { <i>ip-address</i> <i>peer-group-name</i> } filter-list <i>access-list-number</i> { in out weight <i>weight</i> }	(任意) BGP フィルタを作成します。
ステップ 22	neighbor { <i>ip-address</i> <i>peer-group-name</i> } version <i>value</i>	(任意) ネイバーと通信するとき使用する BGP バージョンを指定します。
ステップ 23	neighbor { <i>ip-address</i> <i>peer-group-name</i> } soft-reconfiguration inbound	(任意) 受信したアップデートの保存を開始するようにソフトウェアを設定します。
ステップ 24	end	特権 EXEC モードに戻ります。
ステップ 25	show ip bgp neighbors	設定を確認します。
ステップ 26	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

集約アドレスの設定

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化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配布するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリが 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	<code>configure terminal</code>	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	<code>router bgp autonomous-system</code>	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	<code>aggregate-address address mask</code>	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、アトミック集約アトリビュートが設定されます。
ステップ 4	<code>aggregate-address address mask as-set</code>	(任意) AS 設定パス情報を生成します。このコマンドを使用すると、その直前にあるコマンドと同じ規則に従う集約エントリを作成できます。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多数のパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、更新されます。
ステップ 5	<code>aggregate-address address-mask summary-only</code>	(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	<code>aggregate-address address mask suppress-map map-name</code>	(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	<code>aggregate-address address mask advertise-map map-name</code>	(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	<code>aggregate-address address mask attribute-map map-name</code>	(任意) ルート マップで指定されたアトリビュートを持つ集約を生成します。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show ip bgp neighbors [advertised-routes]</code>	設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

ルーティング ドメイン連合の設定

IBGP メッシュの単純化は、AS を複数のサブ AS に分割し、単独の AS としてされる 1 つの連合にグループ化することによっても実現できます。各 AS はその内部構造が完全メッシュ型になっており、同じ連合内の他の AS との間には数本の接続があります。異なる AS 内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様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 AS に対して共通の IGP を使用できます。

BGP 連合を設定するには、AS グループの AS 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	<code>configure terminal</code>	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	<code>router bgp autonomous-system</code>	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	<code>bgp confederation identifier autonomous-system</code>	BGP 連合 ID を設定します。
ステップ 4	<code>bgp confederation peers autonomous-system</code> [<code>autonomous-system ...</code>]	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp neighbor</code> <code>show ip bgp network</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

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

ルート リフレクタを使用すると、学習されたルートをネイバーへ渡す際に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ型に接続する必要はありません。IBGP ピアをルート リフレクタとして設定すると、その IBGP ピアでは IBGP によって学習されたルートが一連の IBGP ネイバーに送信されるようになります。ルート リフレクタの内部ピアは、クライアント ピアおよび非クライアント ピア (AS システム内に存在するその他すべてのルータ) という 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させます。ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。非クライアント ピアは完全メッシュ型に相互接続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、そのクラスタ外部の IBGP スピーカーとは通信しません。

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

- EBGP スピーカーからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートをすべてのクライアントにアドバタイズします。
- クライアントからのルートをすべてのクライアントおよび非クライアント ピアにアドバタイズします。したがって、クライアントは完全メッシュ型に接続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、各クラスタはルート リフレクタのルート ID によって識別されます。冗長性を高め、シングル ポイント障害を回避するには、クラスタに複数のルート リフレクタを設定する必要があります。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。1 つのクラスタ内にあるルート リフレクタ全体は、完全メッシュ型に接続したうえで、一連のクライアント ピアおよび非クライアント ピアを共有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	<code>configure terminal</code>	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	<code>router bgp <i>autonomous-system</i></code>	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	<code>neighbor <i>ip-address</i> <i>peer-group-name</i> route-reflector-client</code>	ローカル ルータを BGP ルート リフレクタとして設定し、指定されたネイバーをクライアントとして設定します。
ステップ 4	<code>bgp cluster-id <i>cluster-id</i></code>	(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にクラスタ ID を設定します。
ステップ 5	<code>no bgp client-to-client reflection</code>	(任意) クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、それらのクライアントが完全メッシュ型に接続されている場合、ルート リフレクタはルートをクライアントに反映させる必要はありません。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip bgp</code>	設定を確認します。送信元の ID およびクラスタリスト アトリビュートを表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニングの設定

ルート フラップ ダンプニングを使用すると、インターネットワーク全体におけるフラッピング ルートの伝播を最小限に抑制できます。ルートがフラッピングと見なされるのは、そのルートの状態が、使用可能状態と使用不可能状態との間で繰り返し変化する場合です。ルート ダンプニングがイネーブルの場合は、フラッピングしているルートに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、設定された制限値に達すると、ルートが稼動している場合であっても、BGP によりルートのアドバタイズが抑制されます。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、アップ状態のまま抑制されているルートのアドバタイズが再開されます。

IBGP によって学習されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが 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	<code>configure terminal</code>	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	<code>router bgp <i>autonomous-system</i></code>	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	<code>bgp dampening</code>	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	<code>bgp dampening <i>half-life</i> <i>reuse suppress</i> <i>max-suppress</i> [<i>route-map map</i>]</code>	(任意) ルート ダンプニング係数のデフォルト値を変更します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp flap-statistics [{<i>regexp regexp</i>} {<i>filter-list list</i>} {<i>address mask</i> [<i>longer-prefix</i>]}]</code>	(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、統計情報は削除されます。
ステップ 7	<code>show ip bgp dampened-paths</code>	(任意) 抑制されるまでの時間を含めて、ダンプニングされたルートを表示します。

■ BGP の設定

	コマンド	目的
ステップ 8	<code>clear ip bgp flap-statistics</code> [{ <i>regex</i> <i>regex</i> } { <i>filter-list</i> <i>list</i> } { <i>address mask</i> [<i>longer-prefix</i>]}]	(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	<code>clear ip bgp dampening</code>	(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	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造を持つ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することもできます。また、リソースの利用率を取得したり、ネットワークの問題点を解消するための情報を使用したりすることも可能です。さらには、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティングパスを検出することもできます。

表 36-8 は、BGP を消去および表示するために使用する特権 EXEC コマンドをまとめたものです。表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2 を参照してください。

表 36-11 IP BGP の clear コマンドおよび show コマンド

コマンド	目的
<code>clear ip bgp address</code>	特定の BGP 接続をリセットします。
<code>clear ip bgp *</code>	すべての BGP 接続をリセットします。
<code>clear ip bgp peer-group tag</code>	BGP ピア グループのすべてのメンバーを削除します。
<code>show ip bgp prefix</code>	プレフィクスがアドバタイズされたピア グループ、またはピア グループに含まれないピアを表示します。ネクストホップやローカルプレフィクスなどのプレフィクス アトリビュートも表示されます。
<code>show ip bgp cidr-only</code>	サブネット マスクおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
<code>show ip bgp community [community-number] [exact]</code>	指定されたコミュニティに属するルートを表示します。
<code>show ip bgp community-list community-list-number [exact-match]</code>	コミュニティ リストで許可されたルートを表示します。
<code>show ip bgp filter-list access-list-number</code>	指定された AS パス アクセス リストで一致したルートを表示します。
<code>show ip bgp inconsistent-as</code>	送信元の AS と整合しないルートを表示します。
<code>show ip bgp regexp regular-expression</code>	コマンドラインに入力された特定の正規表現と一致する AS パスを持ったルートを表示します。
<code>show ip bgp</code>	BGP ルーティング テーブルの内容を表示します。
<code>show ip bgp neighbors [address]</code>	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。

表 36-11 IP BGP の clear コマンドおよび show コマンド (続き)

コマンド	目的
<code>show ip bgp neighbors [address] [advertised-routes dampened-routes flap-statistics paths regular-expression received-routes routes]</code>	特定の BGP ネイバーから学習されたルートを表示します。
<code>show ip bgp paths</code>	データベース内のすべての BGP パスを表示します。
<code>show ip bgp peer-group [tag] [summary]</code>	BGP ピア グループに関する情報を表示します。
<code>show ip bgp summary</code>	すべての BGP 接続のステータスを表示します。

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 ネイバーをリセット、起動、またはダウンさせるときに生成されるメッセージのロ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 Systems Interconnection (OSI; 開放型システム間相互接続) モデルにおけるネットワーク レイヤの標準です。ISO ネットワーク アーキテクチャのアドレスは、Network Service Access Point (NSAP; ネットワーク サービス アクセス ポイント) アドレスおよび Network Entity Title (NET) と呼ばれます。OSI ネットワークの各ノードには、1 つまたは複数の NET が設定されています。さらに、各ノードには NSAP アドレスが多数存在します。

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コネクションレス型ルーティングをスイッチ上でイネーブルにすると、そのスイッチは転送の判断だけを行い、ルーティング関連の機能は使用しません。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。スイッチは、ISO CLNS ネットワークの 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。このルーティング プロトコルでは、エリアという概念が使用されます。エリア内では、すべてのルータがすべてのシステム ID の到達方法を認識しています。エリア間でも、いくつかのルータが適切なエリアに到達する方法を認識しています。IS-IS では、ステーションルーティング (エリア内部) およびエリアルーティング (エリア間) という 2 つのレベルのルーティングがサポートされています。

ISO IGRP と IS-IS NSAP のアドレス指定方式の重要な違いは、エリア アドレスの定義にあります。どちらも、レベル 1 ルーティング (エリア内ルーティング) のシステム ID を使用しますが、アドレスをエリアルーティング用に指定する方式が異なります。ISO IGRP NSAP アドレスには、ドメイン、エリア、システム ID という、互いに独立した 3 つのルーティング用フィールドが含まれています。一方、IS-IS アドレスには、エリア、システム ID という 2 つのフィールドが含まれていますが、このうちエリアフィールドは、ドメイン フィールドとエリア フィールドを連結して 1 つにしたフィールドです。



(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。このセクションで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS 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 インデックスやオンライン検索を使用して情報を取得してください。

IS-IS ダイナミック ルーティングの設定

IS-IS は、ISO のダイナミック ルーティング プロトコルです。IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成したうえで、それをネットワークではなく、特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することにより、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロセスを指定できます。次に、IS-IS ルーティング プロセスの各インスタンス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、すべてのルータがネットワーク内に含まれる単独のエリアとして確立されます。IS-IS ネットワークは通常、規模が拡大するにつれて、すべてのエリアから接続された（次にローカル エリアに接続される）複数のレベル 2 ルータで構成されるバックボーン エリアに再構成されます。ローカル エリア内では、ルータはすべてのシステム ID への到達方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を、バックボーン ルータはその他のエリアへの到達方法をそれぞれ認識しています。

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）を実行するのに、レベル 1 の隣接関係を確立します。ルータは、レベル 1 エリア間のルーティング（エリアルーティング）を実行するのに、レベル 2 の隣接関係を確立します。

各シスコ ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。通常、各ルーティング プロセスは 1 つのエリアに対応付けられます。デフォルトでは、設定済みのルーティング プロセスの最初のインスタンスはレベル 1 およびレベル 2 の両方のルーティングを実行します。これ以外にもルータ インスタンスを設定できますが、このインスタンスは自動的にレベル 1 エリアとして処理されます。IS-IS ルーティング プロセスの各インスタンスには、個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングの場合、各シスコ ユニットには最大 29 のレベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するよう設定できるのは 1 つのプロセスに限られます。いずれかのプロセスに対してレベル 2 ルーティングを設定した場合、追加されたプロセスはすべて自動的にレベル 1 として設定されます。このプロセスは、同時にレベル 1 ルーティングを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 インスタンスとして望ましくない場合は、**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。また、レベル 2 ルータとして異なるルータ インスタンスを設定する場合にも、**is-type** コマンドを使用します。



(注)

IS-IS の詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Routing Protocols」を参照してください。このセクションで説明するコマンドの構文および使用方法の詳細については、『Cisco IOS IP Command Reference』 Release 12.2 を参照してください。

ここでは、IS-IS ルーティングの設定方法の概要を説明します。内容は次のとおりです。

- 「IS-IS のデフォルト設定」 (P.36-69)
- 「NSF 認識」 (P.36-69)
- 「IS-IS グローバル パラメータの設定」 (P.36-72)
- 「IS-IS インターフェイス パラメータの設定」 (P.36-74)

IS-IS のデフォルト設定

表 36-12 IS-IS のデフォルト設定

機能	デフォルト設定
Link-State PDU (LSP) エラーを無視	イネーブル。
IS-IS タイプ	従来型 IS-IS : ルータはレベル 1 (ステーション) とレベル 2 (エリア) の両方のルータとして動作。 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 とレベル 2 の両方のルータとして動作。その他のインスタンスは、レベル 1 ルータ。
デフォルト情報の送信	ディセーブル。
IS-IS 隣接状態変更のログ	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 最大ライフタイム (リフレッシュなし)	LSP パケットが削除されるまで 1200 秒 (20 分)。
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒 (15 分) ごとに送信。
最大 LSP パケット サイズ	1497 バイト。
NSF ¹ 認識	イネーブル ² 。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中、隣接する NSF 対応ルータからのパケットを転送し続けることが可能。
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 RPC 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 パスワードまたはドメイン パスワードの定義なし。認証はディセーブル。
set-overload-bit	ディセーブル。イネーブルの場合に引数が入力されなければ、過負荷ビットが即座に設定され、 no set-overload-bit コマンドを入力するまで設定されたままになる。
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 計算遅延 : 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 = Nonstop Forwarding (ノンストップ フォワーディング)

2. IS-IS NSF 認識は、メトロ IP アクセス イメージを実行しているスイッチ上の IPv4 に対してイネーブルになっています。

NSF 認識

メトロ IP アクセス イメージの IPv4 に対しては、統合型 IS-IS NSF 認識機能がサポートされています。この機能により、NSF 認識 Customer-Premises Equipment (CPE; 顧客宅内機器) ルータが、NSF 対応のルータにパケットの NSF を実行させることができます。ローカル ルータは NSF を必ずしも実行す

る必要はありませんが、その NSF 認識により、スイッチオーバー プロセスの間、隣接する NSF 対応ルータ上のルーティング データベースおよびリンクステート データベースの整合性と信頼性を維持できます。

この機能は自動的にイネーブルになるため、設定は必要ありません。この機能に関する詳細については、次の URL にある『*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際は、まず各ルーティング プロセスの名前および 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て、ルーティング プロセスの各インスタンスにエリアを指定します。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>clns routing</code>	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	<code>router isis [area tag]</code>	指定されたルーティング プロセスに対し 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) 引数 <i>area tag</i> を使用して、IS-IS ルータが割り当てられるエリアを指定します。複数の IS-IS エリアを設定するときは、値を入力する必要があります。 設定された最初の IS-IS インスタンスは、デフォルトでレベル 1 とレベル 2 です。それ以降のインスタンスは、自動的にレベル 1 となります。 is-type グローバル コンフィギュレーション コマンドを使用すると、ルーティングのレベルを変更できます。
ステップ 4	<code>net network-entity-title</code>	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 およびアドレスの名前を指定できます。
ステップ 5	<code>is-type {level-1 level-1-2 level-2-only}</code>	(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。 <ul style="list-style-type: none"> • 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 ルータの両方として機能します。 • level-2 : エリア ルータとしてだけ機能します。
ステップ 6	<code>exit</code>	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	<code>interface interface-id</code>	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 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、インターフェイスをレイヤ 3 モードにします。
ステップ 8	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

コマンド	目的
ステップ9 ip router isis [area tag]	インターフェイスの ISO CLNS に IS-IS ルーティング プロセスを設定し、そのルーティング プロセスにエリア指定子を関連付けます。
ステップ10 clns router isis [area tag]	インターフェイスの ISO CLNS をイネーブルにします。
ステップ11 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、IS-IS 対応エリアのすべてのインターフェイスに IP アドレスが必要となります。
ステップ12 end	特権 EXEC モードに戻ります。
ステップ13 show isis [area tag] database detail	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。

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型 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。従来型 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 gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
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 gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
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 gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
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、任意で設定可能な一部の IS-IS グローバルパラメータについて説明します。

- ルートマップにより制御されるデフォルトルートを設定することで、IS-IS ルーティングドメイン内にデフォルトルートを一時的に設定できます。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も指定できます。
- ルータに対しては、内部チェックサムエラーとともに受信した IS-IS LSP を無視するよう設定できるほか、破損した LSP を消去するよう設定することもできます。消去された LSP は、その発信側で再生成されます。
- エリアおよびドメインには、パスワードを割り当てることができます。
- サマリーアドレス（経路集約）によりルーティングテーブルで表示される集約アドレスを作成できます。他のルーティングプロトコルから学習されたルートも集約できます。サマリーのアドバタイズには、対象となる全ルートのメトリックの中で最小のメトリックが使用されます。
- 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なしで 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、SPF 計算、および PRC 計算のスロットリングタイマーを設定できます。
- IS-IS 隣接状態が変更（アップまたはダウン）した場合に、ログメッセージが生成されるようスイッチを設定できます。
- ネットワーク内のリンクの MTU サイズが 1500 バイト未満である場合は、ルーティングが引き続き実行されるように LSP MTU を小さくできます。
- `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/レベル 2 境界ルータ、隣接するレベル 1 ルータ、またはエンドホストの間ですべての回線が切断された場合にエリアが分割されないようにできます。

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 <code>configure terminal</code>	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 <code>clns routing</code>	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 <code>router isis</code>	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。
ステップ 4 <code>default-information originate</code> [<code>route-map map-name</code>]	(任意) IS-IS ルーティングドメイン内にデフォルトルートを一時的に設定します。 <code>route-map map-name</code> を入力した場合に、ルートマップが満たされていると、ルーティングプロセスではデフォルトルートが生成されます。
ステップ 5 <code>ignore-lsp-errors</code>	(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ルータを設定します。このコマンドはデフォルトでイネーブルです（破損した LSP は廃棄されます）。破損した LSP を消去するには、 <code>no ignore-lsp-errors</code> 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 <code>area-password password</code>	(任意) レベル 1（ステーションルータ レベル）の LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7 <code>domain-password password</code>	(任意) レベル 2（エリアルータ レベル）の LSP に挿入されるルーティングドメイン認証パスワードを設定します。

コマンド	目的
ステップ 8 summary-address <i>address mask</i> [<i>level-1</i> <i>level-1-2</i> <i>level-2</i>]	(任意) 所定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 { <i>seconds</i> wait-for-bgp }]	(任意) ルータに問題がある場合、他のルータが SFP 計算の際にこのルータを無視するように、過負荷ビット (hippity ビット) を設定します。 <ul style="list-style-type: none"> • (任意) on-startup : 起動時にだけ、過負荷ビットを設定します。on-startup が指定されない場合、過負荷ビットが即座に設定され、no set-overload-bit コマンドを入力するまで設定されたままになります。on-startup が指定された場合は、秒数または wait-for-bgp を入力する必要があります。 • <i>seconds</i> : キーワード on-startup 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 : キーワード on-startup 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 がコンバージするまで設定されたままになります。BGP がコンバージしたことが IS-IS に通知されない場合、過負荷ビットは 10 分後に無効となります。
ステップ 10 lsp-refresh-interval <i>seconds</i>	(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 リフレッシュは 900 秒 (15 分) ごとに送信されます。
ステップ 11 max-lsp-lifetime <i>seconds</i>	(任意) LSP パケットがリフレッシュされないままルータ 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 [<i>level-1</i> <i>level-2</i>] <i>lsp-max-wait</i> [<i>lsp-initial-wait</i> <i>lsp-second-wait</i>]	(任意) IS-IS LSP 生成スロットリング タイマーを設定します。 <ul style="list-style-type: none"> • <i>lsp-max-wait</i> : LSP が生成されてから次の LSP が生成されるまでの最大時間間隔 (秒) を指定します。指定できる範囲は 1 ~ 120 で、デフォルトは 5 です。 • <i>lsp-initial-wait</i> : 最初の LSP 生成遅延 (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルト値は 50 です。 • <i>lsp-second-wait</i> : LSP が最初に生成されてからその次に生成されるまでのホールドタイム (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルト値は 5000 です。
ステップ 13 spf-interval [<i>level-1</i> <i>level-2</i>] <i>spf-max-wait</i> [<i>spf-initial-wait</i> <i>spf-second-wait</i>]	(任意) IS-IS SPF スロットリング タイマーを設定します。 <ul style="list-style-type: none"> • <i>spf-max-wait</i> : 連続する SFP 間 (秒) の最大時間間隔を指定します。指定できる範囲は 1 ~ 120 で、デフォルトは 10 です。 • <i>spf-initial-wait</i> : トポロジが変更されてから最初の SFP 計算が行われるまでの時間 (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルト値は 5500 です。 • <i>spf-second-wait</i> : SFP 計算が最初に行われてからその次に行われるまでのホールドタイム (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルト値は 5500 です。

	コマンド	目的
ステップ 14	prc-interval <i>prc-max-wait</i> [<i>prc-initial-wait prc-second-wait</i>]	(任意) IS-IS PRC スロットリング タイマーを設定します。 <ul style="list-style-type: none"> • <i>prc-max-wait</i> : PRC 計算が行われてから次の PRC 計算が行われるまでの最大時間間隔 (秒) を指定します。指定できる範囲は 1 ~ 120 で、デフォルトは 5 です。 • <i>prc-initial-wait</i> : トポロジが変更されてから最初の SFP 計算が行われるまでの時間 (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルトは 2000 です。 • <i>prc-second-wait</i> : PRC 計算が最初に行われてからその次に行われるまでのホールド タイム (ミリ秒) を指定します。指定できる範囲は 1 ~ 10000 で、デフォルトは 5000 です。
ステップ 15	log-adjacency-changes [all]	(任意) IS-IS 隣接状態変更をログに記録するようルータを設定します。End System-to-Intermediate System PDU および Link State Packet (LSP) など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに記録するには、 all を入力します。
ステップ 16	lsp-mtu <i>size</i>	(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 バイトで、デフォルトは 1497 バイトです。 (注) ネットワーク内の任意のリンクで MTU サイズが縮小された場合は、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、すべての隣接レベル 1 ルータ、およびエンド ホストの間で、フル接続が切断された場合、IS-IS レベル 1/レベル 2 境界ルータがレベル 1 エリア プレフィクスをレベル 2 バックボーンにアダプタイズしないようにします。
ステップ 18	end	特権 EXEC モードに戻ります。
ステップ 19	show clns	設定を確認します。
ステップ 20	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ルート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** ルータ コンフィギュレーション コマンドまたは **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場合は、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレス割り当て、LSP リフレッシュ インターバル、LSP ライフタイム、LSP タイマー、SFP 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、これらのコマンドの **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

必要に応じて、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値 (乗数および時間間隔など) をデフォルトから変更するには、複数のルータおよびインターフェイス上でもこれらの値を変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック。IS-IS メトリックの値として使用され、QoS ルーティングが実行されない場合に割り当てられます。

- hello インターバル (インターフェイスから送信される hello パケットの間隔) またはデフォルトの hello パケット乗数。インターフェイスにおいて、IS-IS hello パケットにより送信されるホールドタイムを決定する際に使用されます。このホールドタイムにより、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間が決まります。これにより、障害があるリンクまたはネイバーの検出速度も決定されるため、ルートを再計算できるようになります。hello パケットの消失や、IS-IS 隣接関係の障害が頻発する場合は、hello 乗数を変更します。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害の検出に要する時間を増やすことなく、hello プロトコルの信頼性を高めることができます。
- その他の時間間隔。
 - Complete Sequence Number PDU (CSNP) インターバル : CSNP は、データベースの同期を維持するため、指定ルータにより送信されます。
 - 再送信インターバル : ポイントツーポイント リンクの IS-IS LSP の再送信間隔です。
 - IS-IS LSP 再送信スロットル インターバル : IS-IS LSP がポイントツーポイント リンクで再送信される最大レート (パケット間のミリ秒数) です。このインターバルは、連続して同じ LSP が再送信される場合の送信間隔を表す再送信インターバルとは異なります。
- 代表ルータの選択プライオリティ。マルチアクセス ネットワークで必要な隣接数を減らし、ひいてはルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを軽減できます。
- インターフェイス回線タイプ。指定されたインターフェイス上のネイバーに必要な隣接関係のタイプです。
- 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、インターフェイスをレイヤ 3 モードにします。
ステップ3 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ4 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 (またはコスト) を設定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 10 です。レベルが入力されない場合は、レベル 1 ルータおよびレベル 2 ルータの両方にデフォルト値が適用されます。
ステップ5 isis hello-interval {seconds minimal} [level-1 level-2]	(任意) スイッチが hello パケットを送信する時間間隔を指定します。デフォルトでは、hello インターバル <i>seconds</i> の 3 倍の値が、送信される hello パケットの <i>holdtime</i> としてアドバタイズされます。hello インターバルが短くなると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。 <ul style="list-style-type: none"> • minimal : ホールドタイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。 • seconds : 指定できる範囲は 1 ~ 65535 です。デフォルトは 10 秒です。

コマンド	目的
ステップ 6 isis hello-multiplier <i>multiplier</i> [level-1 level-2]	(任意) ルータが隣接装置のダウンを宣言するためにネイバーで消失すべき IS-IS hello パケット数を指定します。指定できる範囲は 3 ~ 1000 です。デフォルト値は 3 です。使用する hello 乗数が比較的小さいと、コンバージェンス時間は短縮されますが、ルーティングがより不安定になる可能性があります。
ステップ 7 isis csnp-interval <i>seconds</i> [level-1 level-2]	(任意) インターフェイスに IS-IS CSNP インターバルを設定します。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 8 isis retransmit-interval <i>seconds</i>	(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。指定する値は、ネットワーク上にある任意の 2 つのルータ間における予測ラウンドトリップ遅延よりも大きい整数であることが必要です。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 9 isis retransmit-throttle-interval <i>milliseconds</i>	(任意) IS-IS LSP 再送信スロットル インターバルを設定します。これは、IS-IS LSP がポイントツーポイントリンク上で再送信される最大レート (パケット間のミリ秒数) です。指定できる範囲は 0 ~ 65535 です。デフォルト値は、 isis lsp-interval コマンドにより指定されます。
ステップ 10 isis priority <i>value</i> [level-1 level-2]	(任意) 代表ルータの選択に使用するプライオリティを設定します。指定できる範囲は 0 ~ 127 です。デフォルト値は 64 です。
ステップ 11 isis circuit-type {level-1 level-1-2 level-2-only}	(任意) 指定されたインターフェイス上のネイバーに必要な隣接関係のタイプを設定します (インターフェイスの回線タイプを指定します)。 <ul style="list-style-type: none"> • level-1: このノードとネイバーに共通のエリア アドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • 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おり、かつ共通のエリアが少なくとも 1 つ存在する場合、レベル 1 およびレベル 2 の隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルト設定です。 • level 2: レベル 2 隣接関係が確立されます。ネイバー ルータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 12 isis password <i>password</i> [level-1 level-2]	(任意) インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 ルーティング用またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合のデフォルトはレベル 1 およびレベル 2 です。
ステップ 13 end	特権 EXEC モードに戻ります。
ステップ 14 show clns interface <i>interface-id</i>	設定を確認します。
ステップ 15 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

IS-IS のモニタリングおよびメンテナンス

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

表 36-13 は、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 コマンドをまとめたものです。出力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、IOS コマンドリファレンス マスター インデックスやオンライン検索を使用して情報を取得してください。

表 36-13 ISO CLNS および IS-IS の clear コマンドおよび show コマンド

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

BFD の設定

BFD プロトコルを使用すると、さまざまなメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルに合わせて、フォワーディング パスの障害を瞬時に検出できます。BFD プロトコルは、2 つのシステム間で転送されるすべてのデータ プロトコルの上位においてユニキャスト（ポイントツーポイント）モードで動作し、直接接続されたネイバー間の IPv4 接続を追跡する役割を持ちます。BFD パケットは、宛先のポート番号 3784 または 3785 とともに UDP パケットでカプセル化されます。

EIGRP、IS-IS、および OSPF の導入下では、BFD の次善手段として、改良された障害検出メカニズムを使用できます。この場合、EIGRP タイマー、IS-IS タイマー、および OSPF タイマーの値を小さくすることで 1 ～ 2 秒間隔での障害検出が可能ですが、BFD を使用すれば障害検出の間隔は 1 秒未満です。BFD は、これらのタイマーの値を小さくした場合に比べて CPU への負荷が小さいほか、特定のルーティング プロトコルとは連動していないため、さまざまなルーティング プロトコルに対応できる汎用的で一貫性のある障害検出メカニズムとして使用できます。

BFD セッションを作成するには、ピアとなる両方のシステム（BFD ピア）上に BFD を設定する必要があります。BFD ピア上において、インターフェイス レベルおよびルーティング プロトコル レベルで BFD をイネーブルにすると、BFD セッションを作成できます。BFD タイマーがネゴシエートされると、BFD ピアでは、そのネゴシエートされた間隔で制御パケットが相互に送信されます。ネイバーが直接接続されていないと、BFD ネイバー登録は拒否されます。

図 36-6 は、OSPF および BFD が稼動する 2 つのルータで構成された単純なネットワークを表したものです。OSPF によりネイバーが検出されると (1)、OSPF 隣接ルータとの BFD ネイバー セッションが開始されるよう BFD プロセスに要求が送信され (2)、BFD ネイバー セッションが確立されます (3)。

図 36-6 BFD セッションの確立

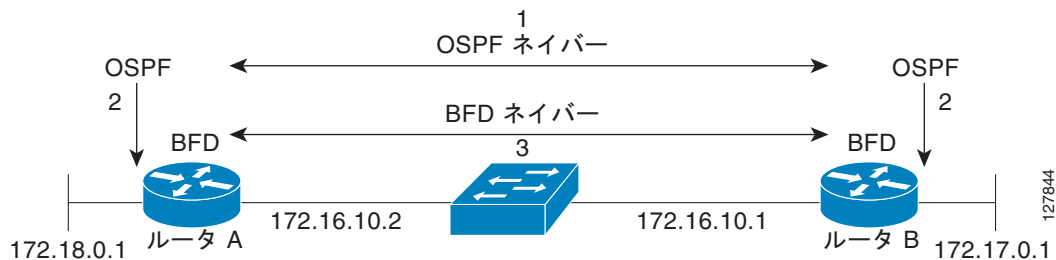
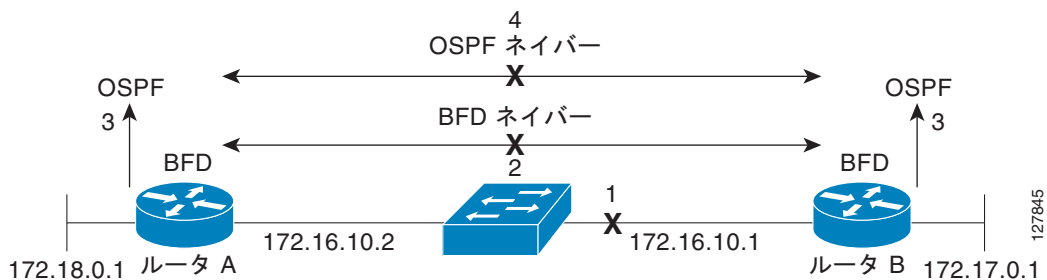


図 36-7 は、ネットワーク内で障害が発生した場合 (1) の動作を示したものです。この場合、OSPF ネイバーとの BFD ネイバー セッションは終了します (2)。BFD から OSPF プロセスへは、その BFD ネイバーが到達不能になったことが通知され、OSPF プロセスによって OSPF ネイバー関係が解消されます (4)。代替パスが使用できる場合は、ルータによりそのパス上でコンバージェンスが開始されます (3)。

図 36-7 OSPF ネイバー関係の解消



BFD クライアントでは、ネイバーを BFD に登録するためのルーティング プロトコルが実行されます。スイッチでは、ISIS、OSPF v1 および v2、BGP、EIGRP、および HSRP の各クライアントがサポートされており、複数のクライアント プロトコルに対して、1 つの BFD セッションを共用できます。たとえば、同一ピアへの同一リンク上で OSPF と EIGRP が稼働しているネットワークでは、BFD セッションを 1 つだけ作成すれば、情報は 2 つのルーティング プロトコルで共有されます。

スイッチでは、BFD バージョン 0 およびバージョン 1 がサポートされています。BFD ネイバーではバージョンのネゴシエーションが自動的に行われ、プロトコルは常に新しい方のバージョンで実行されます。デフォルトのバージョンはバージョン 1 です。

デフォルトの場合、BFD ネイバーは、制御パケットとエコー パケットの両方を交換することで、フォワーディングの障害検出を行います。スイッチでは、設定された BFD インターバル (50 ~ 999 ミリ秒) でエコー パケットが送信されます。また制御パケットは、BFD のスロータイマー レート (1000 ~ 3000 ミリ秒) で送信されます。

障害発生率の検出は、BFD エコー モードを使用することでより高速化できます。BFD エコー モードは、BFD セッションを設定すればデフォルトでイネーブルになります。このモードの場合、スイッチは BFD ソフトウェア レイヤからエコー パケットを送信し、BFD ネイバーは、高速スイッチング レイヤを介してそのエコー パケットに応答します。エコー パケットは、BFD ネイバーのソフトウェア レイヤには到達せず、障害検出を行うフォワーディング パスを介して戻されます。bfd interval 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、BFD インターフェイスから BFD エコー パケットが送信される頻度を設定できます。

帯域幅の使用量を抑える場合は、no bfd echo 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、エコー パケットの送信をディセーブルにします。エコー モードがディセーブルの場合、フォワーディングの障害検出には制御パケットが使用されます。制御パケットは、設定されたスロータイマー レートで交換されます。そのため、障害検出に要する時間が長くなる場合があります。スロータイマー レートの設定は、bfd slow-timer グローバル コンフィギュレーション コマンドで行います。設定できる範囲は 1000 ~ 3000 ミリ秒で、デフォルトは 1000 ミリ秒です。

エコー処理は、BFD ネイバーの設定とは独立したスイッチ インターフェイスで、イネーブルとディセーブルを切り替えられます。エコー モードをディセーブルにしても、インターフェイスからのエコー パケット送信がディセーブルになるだけです。エコー パケットを受信する高速スイッチング レイヤでは常に、エコー パケットが送信者へ返送されます。

スイッチ上で BFD を稼働させるためには、BFD インターフェイス上で基本的な BFD インターバル パラメータを設定し、スイッチ上でルーティングをイネーブルにしたあと、BFD のルーティング プロトコル クライアントを少なくとも 1 つイネーブルにする必要があります。また、参加するスイッチ上で Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) がイネーブル (デフォルト) になっていることを確認する必要があります。

設定の詳細については、次の URL にある『Bidirectional Forwarding Detection』フィーチャ モジュールを参照してください。

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

コマンドの詳細については、次の URL にある『Master Index to the Cisco IOS Command List for Release 12.4』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

ここでは、BFD の設定について説明します。

- 「BFD のデフォルト設定」 (P.36-80)
- 「BFD のデフォルト設定に関する注意事項」 (P.36-80)
- 「インターフェイスに対する BFD セッション パラメータの設定」 (P.36-80)
- 「BFD ルーティング プロトコル クライアントのイネーブル化」 (P.36-82)

BFD のデフォルト設定

BFD セッションは設定されていません。BFD はすべてのインターフェイス上でディセーブルです。

BFD が設定されている場合、デフォルトはバージョン 1 です。ただし、バージョンはスイッチによりネゴシエートされます。バージョン 0 もサポートされています。

スタンバイ BFD (HSRP 用) はデフォルトでイネーブルに設定されています。

BFD セッションの設定時には非同期 BFD エコー モードがイネーブルになります。

BFD のデフォルト設定に関する注意事項

スイッチで同時に使用できる BFD セッションの数は最大で 28 です。

スイッチ上で BFD を実行する手順は次のとおりです。

- BFD セッションを実行する各インターフェイス上で、基本的な BFD インターバル パラメータを設定します。
- スイッチ上でルーティングをイネーブルにします。BFD を設定する際は必ずしもルーティングをイネーブルにする必要はありませんが、BFD セッションをアクティブにするには、スイッチおよび BFD インターフェイスにおいてルーティングがイネーブルになっている必要があります。
- BFD のルーティング プロトコル クライアントを少なくとも 1 つイネーブルにします。使用するルーティング プロトコルに対しては、高速コンバージェンスを実装することを推奨します。高速コンバージェンスの詳細については、この章または『Cisco IOS IP Configuration Guide』Release 12.2 の IP ルーティングに関する項を参照してください。



(注)

ルーティング プロトコル コマンドを設定する前に、インターフェイス上で BFD インターバル パラメータを設定することを推奨します (特に EIGRP を使用する場合)。

参加するスイッチ上で、IP ルーティングのほかに CEF もイネーブル (デフォルト) になっていることを確認します。

BFD は、ルーティング インターフェイスとして設定された物理インターフェイス上でサポートされます。レイヤ 2 インターフェイス、疑似回線、スタティック ルート、SVI インターフェイス、およびポート チャネルではサポートされていません。

レイヤ 2 ポート上に BFD インターフェイス コマンドを設定できますが、そのインターフェイス上で BFD セッションが動作するためには、それをレイヤ 3 インターフェイスとして設定し (no switchport)、さらに IP アドレスを割り当てる必要があります。

HSRP BFD ではデフォルトで、スタンバイ BFD がすべてのインターフェイス上でグローバルにイネーブル化されています。いずれかのインターフェイス上でスタンバイ BFD をディセーブルにした場合、BFD セッションをアクティブにするには、スタンバイ BFD をいったんグローバルにディセーブル化したあと、再度グローバルにイネーブル化する必要があります。

BFD エコー モード (デフォルト) を使用するには、BFD インターフェイス上で **no ip redirects** 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、ICMP リダイレクト メッセージの送信をディセーブルにすることを推奨します。

インターフェイスに対する BFD セッション パラメータの設定

インターフェイス上で BFD セッションを開始するには、事前にそのインターフェイスをレイヤ 3 モードにしたうえで、ベースライン BFD パラメータを設定する必要があります。



(注)

レイヤ 2 インターフェイス上で BFD を設定できますが、BFD セッションを開始するためには、双方のインターフェイスをレイヤ 3 モードにし、スイッチ上でルーティングをイネーブルにする必要があります。

BFD セッションに参加するインターフェイス上で BFD 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	BFD セッションに使用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。BFD がサポートされるのは物理インターフェイスだけです。
ステップ 3 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface (UNI; ユーザ ネットワーク インターフェイス) および Enhanced Network Interface (ENI; 拡張ネットワーク インターフェイス) はディセーブル、Network Node Interface (NNI; ネットワーク ノード インターフェイス) はイネーブルです。
ステップ 4 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。
ステップ 5 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 6 bfd interval milliseconds min_rx milliseconds multiplier value	<p>インターフェイス上でエコー パケットごとに BFD パラメータを設定します。</p> <ul style="list-style-type: none"> interval : BFD エコー パケットを BFD ピアに送信する時間間隔を指定します。指定できる範囲は 50 ~ 999 ミリ秒 (ms) です。 min_rx : BFD ピアから返送された BFD エコー パケットを受信する時間間隔を指定します。指定できる範囲は 50 ~ 999 ミリ秒です。 multiplier : BFD ピアが使用不能になったことを宣言し、障害の発生を他の BFD に通知するための基準として、その BFD ピアにおける BFD エコー パケットの連続消失数を指定します。指定できる範囲は 3 ~ 50 です。 <p>(注) ベースライン BFD パラメータにはデフォルト値はありません。</p>
ステップ 7 end	特権 EXEC モードに戻ります。
ステップ 8 show running-config	設定を確認します。
ステップ 9 show bfd neighbor detail	(任意) ネイバーによるセッション作成時に、最終的に設定された値またはネゴシエートされた値を表示します。
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。

BFD パラメータの設定を削除するには、**no bfd interval** 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。

BFD ルーティング プロトコル クライアントのイネーブル化

インターフェイス上で BFD パラメータの設定が完了すると、1 つまたは複数のルーティング プロトコルに対して BFD セッションを開始できます。最初にスイッチ上で **ip routing** グローバル コンフィギュレーション コマンドを入力して、ルーティングをイネーブルにする必要があります。ただし、インターフェイス上で BFD セッションを開始する方法は複数あり、どの方法を使用するかはルーティング プロトコルによって異なります。

- 「OSFP に対する BFD の設定」 (P.36-82)
- 「IS-IS に対する BFD の設定」 (P.36-83)
- 「BGP に対する BFD の設定」 (P.36-85)
- 「EIGRP に対する BFD の設定」 (P.36-86)
- 「HSRP に対する BFD の設定」 (P.36-86)

OSFP に対する BFD の設定

OSPF 用の BFD セッションを開始するには、参加するすべてのデバイス上で OSPF が稼動している必要があります。BFD の OSPF サポートをイネーブルにする場合は、それをすべての OSPF インターフェイス上、またはいずれか 1 つ以上の OSPF インターフェイス上でイネーブルにします。

OSFP BFD のグローバルな設定

OSFP BFD をグローバルに設定し、必要に応じてそれを特定のインターフェイス上で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	<code>configure terminal</code>	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	<code>router ospf process- id</code>	OSPF プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bfd all-interfaces</code>	OSPF ルーティング プロセスに対応付けられているすべてのインターフェイス上で BFD をグローバルにイネーブル化します。
ステップ 4	<code>exit</code>	(任意) 1 つまたは複数の OSPF インターフェイス上で BFD をディセーブルにする場合は、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	<code>interface interface-id</code>	(任意) 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 6	<code>ip ospf bfd disable</code>	(任意) 指定した OSPF インターフェイス上で BFD をディセーブルにします。BFD セッションを実行しないすべての OSPF インターフェイスに対して、ステップ 5 および 6 を繰り返し実行します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show bfd neighbors [detail]</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(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。

すべてのインターフェイス上で OSPF BFD をディセーブルにするには、**no bfd all-interfaces** ルータ コンフィギュレーション コマンドを使用します。いずれかのインターフェイス上で OSPF BFD をディセーブルにする場合は、そのインターフェイス上で **no ip ospf bfd** インターフェイス コンフィギュレーション コマンドまたは **ip ospf bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

一部のインターフェイス上でだけ OSPF BFD を稼働させる場合は、OSPF BFD をグローバルにイネーブル化する代わりに、それらのインターフェイス上で **ip ospf bfd** インターフェイス コンフィギュレーション コマンドを実行することもできます。詳細については、次に説明する手順を参照してください。



(注) レイヤ 2 インターフェイス上で OSPF BFD を設定しても、その設定は認識されません。

次に、すべての OSPF インターフェイス上で OSPF BFD を設定する例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

インターフェイス上での OSPF BFD 設定

個々のインターフェイス上で OSPF BFD 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 プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	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 4	interface interface-id	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 5	ip ospf bfd	指定された OSPF インターフェイス上で BFD をイネーブルにします。BFD セッションを実行するすべての OSPF インターフェイスに対して、ステップ 3 および 4 を繰り返し実行します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show bfd neighbors [detail]	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。

いずれかのインターフェイス上で OSPF BFD をディセーブルにするには、そのインターフェイス上で **no ip ospf bfd** インターフェイス コンフィギュレーション コマンドまたは **ip ospf bfd disable** インターフェイス コンフィギュレーション コマンドを実行します。

次に、単独のインターフェイス上で OSPF BFD を設定する例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip ospf bfd
```

IS-IS に対する BFD の設定

IS-IS 用の BFD セッションを開始する場合は、BFD に参加するすべてのデバイス上で、IS-IS が稼働している必要があります。BFD の IS-IS サポートをグローバルにイネーブルにする場合は、それをすべての IS-IS インターフェイス上、またはいずれか 1 つ以上の IS-IS インターフェイス上でイネーブルにします。

IS-IS BFD のグローバルな設定

IS-IS BFD をグローバルに設定し、必要に応じてそれを特定のインターフェイス上で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	<code>configure terminal</code>	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	<code>router is-is area-tag</code>	IS-IS プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bfd all-interfaces</code>	OSPF ルーティング プロセスに対応付けられているすべてのインターフェイス上で IS-IS をグローバルにイネーブル化します。
ステップ 4	<code>exit</code>	(任意) 1 つまたは複数の IS-IS インターフェイス上で BFD をディセーブルにする場合は、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	<code>interface interface-id</code>	(任意) 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 6	<code>ip router isis</code>	(任意) インターフェイス上で IPv4 IS-IS ルーティングをイネーブルにします。
ステップ 7	<code>isis bfd disable</code>	(任意) IS-IS インターフェイス上で BFD をディセーブルにします。BFD セッションを実行しないすべての IS-IS インターフェイスに対して、ステップ 5 ~ 7 を繰り返し実行します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show bfd neighbors [detail]</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(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。

すべてのインターフェイス上で IS-IS BFD をディセーブルにするには、`no bfd all-interfaces` ルータ コンフィギュレーション コマンドを使用します。指定されたインターフェイス上で IS-IS BFD をディセーブルにするには、そのインターフェイス上で `no isis bfd` インターフェイス コンフィギュレーション コマンドまたは `isis bfd disable` インターフェイス コンフィギュレーション コマンドを実行します。

一部のインターフェイス上でだけ IS-IS BFD を稼働させる場合は、IS-IS BFD をグローバルにイネーブル化する代わりに、それらのインターフェイス上で `isis bfd` インターフェイス コンフィギュレーション コマンドを実行することもできます。詳細については、次に説明する手順を参照してください。



(注)

IS-IS BFD が稼働するのはレイヤ 3 インターフェイス上ですが、IS-IS BFD はレイヤ 2 モードのインターフェイス上でもレイヤ 3 モードのインターフェイス上でも設定できます。IS-IS BFD をイネーブルにすると、次のようなメッセージが表示されます。

```
%ISIS BFD is reverting to router mode configuration, and remains disabled.
```

次に、高速コンバージェンスを設定したうえで、すべての IS-IS インターフェイス上に IS-IS BFD を設定する例を示します。

```
Switch(config)# router is-is tag1
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

インターフェイス上での IS-IS BFD の設定

個々のインターフェイス上で IS-IS BFD 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	<code>configure terminal</code>	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	<code>router is-is area-tag</code>	IS-IS プロセスを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>exit</code>	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 4	<code>interface interface-id</code>	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 5	<code>isis bfd</code>	指定された IS-IS インターフェイス上で BFD をイネーブルにします。BFD セッションを実行するすべての IS-IS インターフェイスに対して、ステップ 3 および 4 を繰り返し実行します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show bfd neighbors [detail]</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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。

いずれかのインターフェイス上で IS-IS BFD をディセーブルにするには、そのインターフェイス上で `no isis bfd` インターフェイス コンフィギュレーション コマンドまたは `isis bfd disable` インターフェイス コンフィギュレーション コマンドを実行します。

次に、単独のインターフェイス上で IS-IS BFD を設定する例を示します。

```
Switch(config)# router is-is tag1
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# isis bfd
```

BGP に対する BFD の設定

BGP 用の BFD セッションを開始するときは、参加するすべてのデバイス上で BGP が稼動している必要があります。BGP BFD をイネーブルにするには、BFD ネイバーの IP アドレスを入力します。

BGP BFD 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	<code>configure terminal</code>	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	<code>router bgp as-tag</code>	BGP AS を指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>neighbor ip-address fall-over bfd</code>	BFD ネイバー上で、BFD のフォールオーバー サポートをイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show bfd neighbors [detail]</code> > <code>show ip bgp neighbor</code>	設定を確認します。 ネイバーへの BGP 接続に関する情報を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP BFD をディセーブルにするには、`no neighbor ip-address fall-over bfd` ルータ コンフィギュレーション コマンドを使用します。

EIGRP に対する BFD の設定

EIGRP 用の BFD セッションを開始する場合は、参加するすべてのデバイス上で EIGRP が稼動している必要があります。BFD の EIGRP サポートをグローバルにイネーブルにする場合は、それをすべての EIGRP インターフェイス上、またはいずれか 1 つ以上の EIGRP インターフェイス上でイネーブルにします。

EIGRP BFD 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	<code>configure terminal</code>	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	<code>router eigrp as-number</code>	EIGRP AS 番号を指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>log-adjacency changes [detail]</code>	EIGRP ネイバーがアップまたはダウンした際、システム ロギング メッセージが送信されるようにスイッチを設定します。
ステップ 4	<code>bfd {all-interfaces interface interface-id}</code>	EIGRP BFD をイネーブルにします。 <ul style="list-style-type: none"> EIGRP ルーティング プロセスに対応付けられたすべてのインターフェイス上で、BFD をグローバルにイネーブル化する場合は all-interfaces を入力します。 EIGRP ルーティング プロセスに対応付けられた 1 つまたは複数のインターフェイスに対して BFD を個別にイネーブル化するには、interface interface-id を入力します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show bfd neighbors [detail]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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。

すべてのインターフェイス上で EIGRP BFD をディセーブルにするには、**no bfd all-interfaces** ルータ コンフィギュレーション コマンドを使用します。いずれかのインターフェイス上で OSPF BFD をディセーブルにするには、そのインターフェイス上で **no bfd interface interface-id** ルータ コンフィギュレーション コマンドを実行します。

HSRP に対する BFD の設定

HSRP ではデフォルトで BFD がサポートされています。BFD はすべてのインターフェイス上でグローバルにイネーブル化されています。HSRP サポートが手動でディセーブル化されている場合は、インターフェイス コンフィギュレーション モードまたはグローバル コンフィギュレーション モードで再度イネーブル化できます。参加するすべてのデバイスで、HSRP および CEF がイネーブルになっている必要があります (CEF はデフォルトでイネーブル)。

HSRP BFD を再度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	<code>configure terminal</code>	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	<code>interface interface-id</code>	BFD セッションに使用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。BFD がサポートされるのは物理インターフェイスだけです。
ステップ 3	<code>ip address ip-address subnet-mask</code>	インターフェイスの IP アドレスおよび IP サブネット マスクを設定します。

	コマンド	目的
ステップ 4	<code>standby [group-number] ip [ip-address] [secondary]</code>	HSRP をアクティブにします。
ステップ 5	<code>standby bfd</code>	(任意) インターフェイス上で BFD の HSRP サポートをイネーブルにします。
ステップ 6	<code>exit</code>	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	<code>standby bfd all-interfaces</code>	(任意) すべてのインターフェイス上で BFD の HSRP サポートをイネーブルにします。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show standby neighbors</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(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。

すべてのインターフェイス上で BFD の HSRP サポートをディセーブルにするには、**no standby bfd all-interfaces** 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。いずれかのインターフェイス上で BFD の HSRP サポートをディセーブルにするには、**no standby bfd** 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) **no standby bfd** 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インターフェイス上のスタンバイ BFD をディセーブルにした場合、その他のインターフェイス上で BFD セッションをアクティブにするためには、**no standby bfd all-interfaces** グローバル コンフィギュレーション コマンドと **standby bfd all-interfaces** グローバル コンフィギュレーション コマンドをこの順に入力して、スタンバイ BFD をいったんグローバルにディセーブル化したあと、再度グローバルにイネーブル化する必要があります。

BFD エコー モードのディセーブル化

BFD セッションを設定すると、BFD インターフェイスでは BFD エコー モードがデフォルトでイネーブルになります。インターフェイス上でエコー モードをディセーブルにすると、そのインターフェイスでは、エコー パケットは送信されず、ネイバーから受信したエコー パケットに限り返送されます。エコー モードがディセーブルの場合、フォワーディングの障害検出には制御パケットが使用されます。BFD 制御パケットの送信頻度を低くする場合は、スロー タイマーを設定します。

BFD デバイス上でエコー モードをディセーブルにし、スロータイマー レ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	<code>configure terminal</code>	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	<code>interface interface-id</code>	BFD インターフェイスを入力し、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	<code>no bfd echo</code>	インターフェイス上で BFD エコー モードをディセーブルにします。BFD エコー モードは、デフォルトでイネーブルに設定されていますが、BFD ネイバー上では個別にディセーブル化できます。
ステップ 4	<code>exit</code>	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	<code>bfd slow-timer [milliseconds]</code>	(任意) BFD のスロータイマーの値を設定します。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルト値は 1000 ミリ秒です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ7	<code>show bfd neighbors detail</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(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。

スイッチ上でエコー モードをディセーブルにしたあと、再度イネーブルにするには、`bfd echo` グローバル コンフィギュレーション モードを使用します。

マルチ VRF CE の設定

Virtual Private Network (VPN; バーチャルプライベート ネットワーク) を使用すると、ISP バックボーン ネットワーク上で帯域幅をセキュアな方法で共有できます。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーでは、VPN Routing/Forwarding (VRF; VPN ルーティングおよび転送) テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスが関連付けられます。

スイッチは、Customer Edge (CE; カスタマー エッジ) デバイスの複数の VRF (マルチ VRF) インスタンスをサポートしています (マルチ VRF CE)。サービス プロバイダーは、マルチ 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 のサポートに、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 IOS Switching Services Configuration Guide』 Release 12.2 を参照してください。

- 「マルチ VRF CE の概要」 (P.36-88)
- 「マルチ VRF CE のデフォルト設定」 (P.36-90)
- 「マルチ VRF CE の設定時の注意事項」 (P.36-91)
- 「VRF の設定」 (P.36-91)
- 「VRF 認識サービスの設定」 (P.36-92)
- 「VPN ルーティング セッションの設定」 (P.36-95)
- 「BGP PE/CE ルーティング セッションの設定」 (P.36-96)
- 「マルチ VRF CE の設定例」 (P.36-97)
- 「マルチ VRF CE ステータスの表示」 (P.36-101)

マルチ VRF CE の概要

マルチ VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。マルチ VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF には所属させられません。



(注)

マルチ 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ことが必要です。

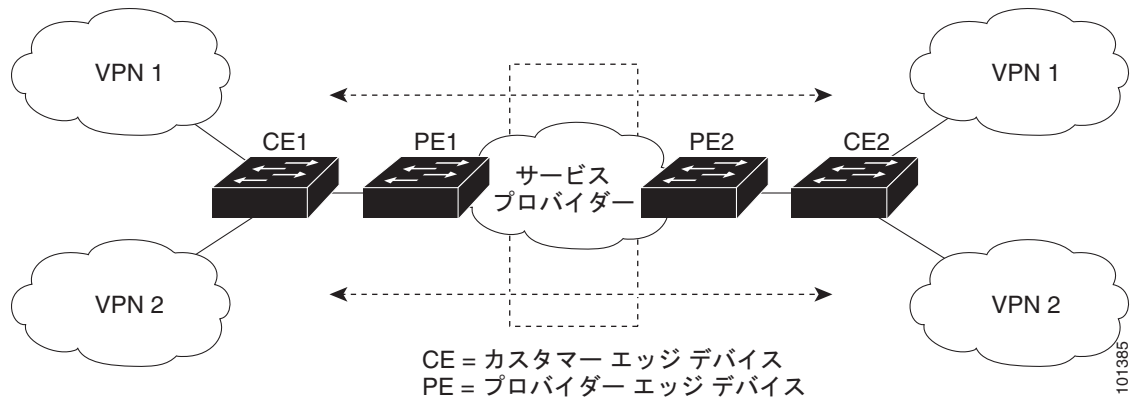
マルチ VRF CE には、次のようなデバイスがあります。

- **Customer edge (CE; カスタマー エッジ)** : カスタマーは、CE デバイスにより、1 つまたは複数の Provider Edge (PE; プロバイダー エッジ) ルータへのデータ リnk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 デバイスは、サイトのローカル ルートをルータにアドバタイズし、そこからリモート VPN ルートを学習します。Cisco ME 3400 スイッチは、CE として使用できます。
- **Provider edge (PE; プロバイダー エッジ)** : PE 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 デバイス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 ルートだけを維持すればよく、すべてのサービス プロバイダー 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 に参加する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

マルチ 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 の間ではただ 1 つの物理リンクが使用されます。共有 CE は、カスタマーごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、カスタマーごとにパケットをスイッチングまたはルーティングします。マルチ VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシーおよびセキュリティを支店に拡張します。

図 36-8 は、Cisco ME スイッチを使用した複数の仮想 CE による構成を示したものです。このシナリオは、中小企業など、VPN サービスの帯域幅要件が低いカスタマーに適しています。このような場合、Cisco ME スイッチではマルチ VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能であるため、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスであることが必要です。

図 36-8 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、マルチ VRF CE 関連のデータ構造で 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。

マルチ VRF CE を設定すると、レイヤ 3 転送テーブルは、概念的に次の 2 つのセクションに分割されます。

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

各 VRF の VLAN ID は別々のポリシー ラベルにマッピングされます。処理を行う際はこれを使用して VRF が区別されます。レイヤ 3 転送テーブルのマルチ VRF CE セクションでルートが検出されない場合は、グローバルルーティング セクションを使用してフォワーディング パスを決定します。レイヤ 3 設定機能では、学習された新しい VPN ルートごとに、入力ポートの VLAN ID を使用してポリシー ラベルが取得され、マルチ VRF CE ルーティング セクションにポリシー ラベルおよび新しいルートが挿入されます。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。

マルチ VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力ポリシー 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。ルートが見つかり、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。ルートが見つかり、ルータは対応する MPLS ラベルをパケットに追加し、それを MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去し、そのラベルに基づいて正しい VPN ルーティング テーブルを特定します。次に、通常のルート検索を実行します。ルートが見つかり、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。ルートが見つかり、パケットを VPN 内で転送します。

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

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

マルチ VRF CE のデフォルト設定

表 36-14 は、VRF のデフォルト設定をまとめたものです。

表 36-14 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 は定義されていない。
マップ	インポート マップ、エクスポート マップ、およびルート マップは定義されていない。
VRF 最大ルート数	5000
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。

マルチ VRF CE の設定時の注意事項

ネットワークに VRF を設定する場合は、次の事項に注意してください。

- マルチ VRF CE を含むスイッチは複数のカスタマーで共有しますが、一方で各カスタマーには独自のルーティング テーブルがあります。
- カスタマーは、別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN であれば IP アドレスの重複が許可されます。
- マルチ VRF CE では、複数のカスタマーが、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、カスタマー間でパケットが区別されます。それぞれのカスタマーには独自の VLAN があります。
- マルチ VRF CE には、サポートしていない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、マルチ VRF CE の使用と複数の CE の使用に違いはありません。図 36-8 では、複数の仮想レイヤ 3 インターフェイスがマルチ VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF 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できます。
- カスタマーは、別のカスタマーと重複しないかぎり、複数の VLAN を使用できます。カスタマーの VLAN は、スイッチに保存されている適切なルーティング テーブルを識別するために使用される特定のルーティング テーブル ID にマッピングされます。
- スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートしています。
- 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、EIGRP およびスタティック ルーティング) を使用できます。ただし、次の理由から (EBGP; 外部 BGP) を使用することを推奨します。
 - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
 - BGP は、さまざまな管理者により運用されるシステム間でルーティング情報を受け渡しできるように設計されています。
 - BGP では、ルートのアトリビュートを CE へ簡単に渡すことができます。
- マルチ VRF CE は、パケットのスイッチング レートに影響しません。
- VRF を設定しない場合は、最大 105 のポリシーを設定できます。
- VRF を 1 つでも設定した場合、設定できるポリシーの数は 41 となります。
- 設定されているポリシーの数が 41 を超えている場合は、VRF を設定できません。
- VRF とプライベート VLAN は相互に排他的です。プライベート VLAN では VRF をイネーブルにできません。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 をイネーブルにはできません。
- VRF と Policy-Based Routing (PBR; ポリシーベース ルーティング) は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっている場合、VRF をイネーブルにはできません。VRF がインターフェイスでイネーブルになっている場合、PBR をイネーブルにはできません。

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。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip routing</code>	IP ルーティングをイネーブルにします
ステップ 3	<code>ip vrf vrf-name</code>	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	<code>rd route-distinguisher</code>	ルート識別子を指定し、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	<code>route-target {export import both} route-target-ext-community</code>	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (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。 <code>route-target-ext-community</code> は、ステップ 4 で入力した <code>route-distinguisher</code> と同じであることが必要です。
ステップ 6	<code>import map route-map</code>	(任意) ルート マップを VRF に関連付けます。
ステップ 7	<code>interface interface-id</code>	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、ルーテッド ポートまたは SVI を指定できます。
ステップ 8	<code>no shutdown</code>	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 9	<code>ip vrf forwarding vrf-name</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show ip vrf [brief detail interfaces] [vrf-name]</code>	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 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VRF と、そのインターフェイスすべてを削除するには、`no ip vrf vrf-name` グローバル コンフィギュレーション コマンドを使用します。VRF からいずれかの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。

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で設定できます。これらのサービスは、グローバル ルーティング インスタンス内で実行されます。IP サービスは、複数のルーティング インスタンスで実行されるように拡張されています。これが VRF 認識です。システム内に設定された 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、プラットフォームから独立したモジュールに実装されています。VRF とは、Cisco IOS における複数のルーティング インスタンスのことです。各プラットフォームでは、サポートされる VRF 数に独自の制限があります

VRF 認識サービスには次のような特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに対して PING を実行できます。
- ARP エントリは、それぞれの VRF 内で個別に学習されます。ユーザは、特定の VRF に関する ARP エントリを表示できます。

次のサービスはすべて VRF 認識です。

- ARP
- 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)
- syslog
- traceroute
- FTP および TFTP



(注) Unicast Reverse Path Forwarding (uRPF; ユニキャスト RPF) に対しては、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。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』 Release 12.2 を参照してください。

コマンド	目的
<code>show ip arp vrf vrf-name</code>	指定した VRF の ARP テーブルを表示します。

PING のユーザ インターフェイス

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

コマンド	目的
<code>ping vrf vrf-name ip-host</code>	指定した VRF の ARP テーブルを表示します。

SNMP のユーザ インターフェイス

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server trap authentication vrf</code>	VRF 上のパケットに対して SNMP トラップをイネーブルにします。
ステップ 3	<code>snmp-server engineID remote <host> vrf <vpn instance> <engine-id string></code>	スイッチ上のリモート SNMP エンジンに名前を設定します。
ステップ 4	<code>snmp-server host <host> vrf <vpn instance> traps <community></code>	SNMP トラップ動作の受信側を指定し、SNMP トラップの送信に使用する VRF テーブルを指定します。

■ マルチ VRF CE の設定

	コマンド	目的
ステップ 5	<code>snmp-server host <host> vrf <vpn instance> informs <community></code>	SNMP インフォーム動作の受信側を指定し、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。
ステップ 6	<code>snmp-server user <user> <group> remote <host> vrf <vpn instance> <security model></code>	SNMP アクセス用に、VRF 上にあるリモートホストの SNMP グループにユーザを追加します。
ステップ 7	<code>end</code>	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 アドレスが正しい IP ルーティング テーブルへ追加されることが保証されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no switchport</code>	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	<code>ip vrf forwarding <vrf-name></code>	インターフェイス上で VRF を設定します。
ステップ 5	<code>ip address ip address</code>	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	<code>standby 1 ip ip address</code>	HSRP をイネーブルにし、仮想 IP アドレスを設定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。

syslog のユーザ インターフェイス

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>logging on</code>	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、または一時的にディセーブルにします。
ステップ 3	<code>logging host ip address vrf vrf name</code>	ロギング メッセージが送信される syslog サーバのホストアドレスを指定します。
ステップ 4	<code>logging buffered logging buffered size debugging</code>	メッセージを内部バッファにログとして記録します。
ステップ 5	<code>logging trap debugging</code>	syslog サーバに送信するロギング メッセージを制限します。
ステップ 6	<code>logging facility facility</code>	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	<code>end</code>	特権 EXEC モードに戻ります。

traceroute のユーザ インターフェイス

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

コマンド	目的
<code>traceroute vrf vrf-name ipaddress</code>	宛先アドレスを検索する 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 が VRF 認識であるためには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイス E1/0 に付随する VRF テーブルを使用する場合であれば、特定のルーティング テーブルを使用することが FTP/TFTP に通知されるよう CLI `ip [t]ftp source-interface E1/0` を設定する必要があります。この例では、宛先 IP アドレスの検索に VRF テーブルが使用されません。これらの変更は、下位互換性があるため、既存の動作には影響しません。つまり、`source-interface` CLI を使用すれば、VRF が設定されていないインターフェイスに対してもパケットを送信できます。

FTP 接続の送信元 IP アドレスを指定するには、`ip ftp source-interface` 表示モード コマンドを使用します。接続が行われ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	<code>configure terminal</code>	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	<code>ip ftp source-interface interface-type interface-number</code>	FTP 接続の送信元 IP アドレスを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

インターフェイスの IP アドレスを TFTP 接続の送信元アドレスとして指定するには、`ip tftp source-interface` 表示モード コマンドを使用します。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。

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

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、その他のプロトコルでも手順は同じです。



(注) EIGRP ルーティング プロセスが VRF インスタンス内部で実行されるよう設定するには、**autonomous-system autonomous-system-number address-family** コンフィギュレーション モード コマンドを使用して、AS 番号を設定する必要があります。

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

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 router ospf process-id vrf vrf-name	OSPF ルーティングをイネーブルにし、VPN 転送テーブルを指定して、ルータ コンフィギュレーション モードを開始します。
ステップ3 log-adjacency-changes	(任意) 隣接状態の変更をログに記録します。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布するようにスイッチを設定します。
ステップ5 network network-number area area-id	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ6 end	特権 EXEC モードに戻ります。
ステップ7 show ip ospf process-id	OSPF ネットワークの設定を確認します。
ステップ8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

BGP PE/CE ルーティング セッションの設定

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

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 router bgp autonomous-system-number	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ3 network network-number mask network-mask	ネットワークとマスクを指定し、BGP の使用を通知します。
ステップ4 redistribute ospf process-id match internal	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ5 network network-number area area-id	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ6 address-family ipv4 vrf vrf-name	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレスファミリー モードを開始します。
ステップ7 neighbor address remote-as as-number	PE ルータと CE ルータの間の BGP セッションを定義します。
ステップ8 neighbor address activate	IPv4 アドレスファミリーのアドパイズメントをアクティブにします。
ステップ9 end	特権 EXEC モードに戻ります。

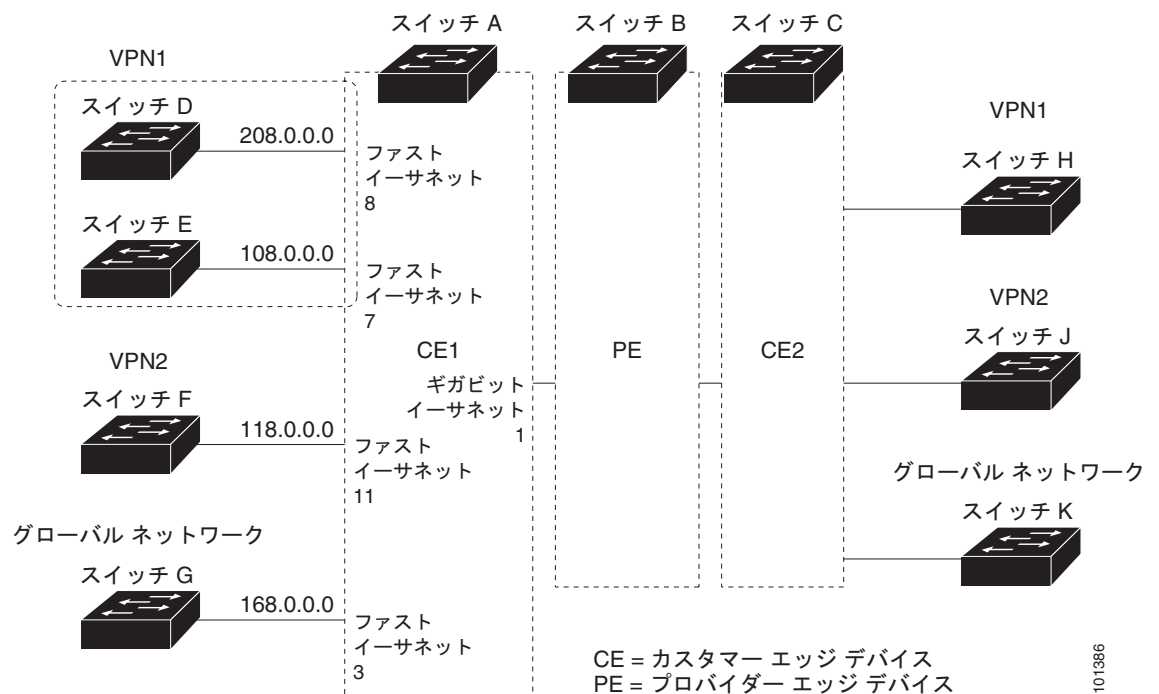
	コマンド	目的
ステップ 10	<code>show ip bgp [ipv4] [neighbors]</code>	BGP 設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

マルチ VRF CE の設定例

図 36-9 は、図 36-8 と同様のネットワークにおける物理的な接続を単純化した例です。VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。この図のあとに記載されている例は、Cisco ME 3400 スイッチを CE Switch A として設定する方法、およびカスタマー スイッチ D および F の VRF 設定です。CE スイッチ C やその他のカスタマー スイッチを設定するためのコマンドは記載されていませんが、この例で使用されているコマンドとほぼ同じです。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 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 36-9 マルチ 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 上で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 と 11 は VPN に接続されます。

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

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

Switch(config)# interface gigabitethernet0/5
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 fastethernet0/8
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config-if)# no shutdown
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 上で使用する VLAN を設定します。VLAN 10 は、CE と PE の間の VRF 11 によって使用されます。VLAN 20 は、CE と PE の間の VRF 12 によって使用されます。VLAN 118 と VLAN 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

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

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

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

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

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

VPN1 と VPN2 で OSPF ルーティングを設定します。

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

CE/PE ルーティングに BGP を設定します。

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

Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D の設定

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
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

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
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
```

■ マルチ VRF CE の設定

```
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

スイッチ B (PE ルータ) では、次のコマンドを使用することにより、CE デバイス、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 gigabitethernet0.10
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 gigabitethernet0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
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
```

マルチ VRF CE ステータスの表示

マルチ VRF CE の設定とステータスに関する情報を表示するには、表 36-15 の特権 EXEC コマンドを使用します。

表 36-15 マルチ VRF CE 情報を表示するコマンド

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

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

プロトコルに依存しない機能の設定

ここでは、IP ルーティング プロトコルに依存しない機能の設定方法について説明します。この章で説明する IP ルーティング プロトコルに依存しない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」を参照してください。

ここでは、次の設定情報について説明します。

- 「CEF の設定」 (P.36-101)
- 「等価コスト ルーティング パスの個数の設定」 (P.36-103)
- 「スタティック ユニキャスト ルートの設定」 (P.36-103)
- 「デフォルトのルートおよびネットワークの指定」 (P.36-105)
- 「ルート マップによるルーティング情報の再配布」 (P.36-105)
- 「PBR の設定」 (P.36-109)
- 「ルーティング情報のフィルタリング」 (P.36-113)
- 「認証鍵の管理」 (P.36-116)

CEF の設定

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に割り振ることができます。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となります。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 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 と分散隣接関係テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラー イメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク 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します。CEF は、隣接関係テーブルを使用して、レイヤ 2 アドレッシング 情報を付加します。隣接関係テーブルには、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、(ASIC; 特定用途向け IC) を使用してギガビット回線レートの IP トラフィックを実現しているため、CEF 転送はソフトウェア フォワーディング パス、つまり CPU が転送す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化されています。何らかの理由で CEF が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 コマンドを使用して、再度イネーブルに設定できます。

デフォルト設定では、CEF はすべてのレイヤ 3 インターフェイス上でイネーブルです。 **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、ソフトウェアにより転送され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 フォワーディング 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デバッグするのに便利です。ソフトウェア フォワーディング パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。



注意

CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、インターフェイス上の CEF をデバッグ 目的以外でディセーブルにすることは避けてください。

CEF をグローバルにイネーブル化したり、ソフトウェア転送トラフィック用のインターフェイス上でディセーブルになった場合にそのインターフェイス上で CEF をイネーブルにしたりするには、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。
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 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5 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 6 end	特権 EXEC モードに戻ります。
ステップ 7 show ip cef	すべてのインターフェイスの CEF ステータスを表示します。

	コマンド	目的
ステップ 8	<code>show cef linecard [detail]</code>	CEF に関連するインターフェイス情報を表示します。
ステップ 9	<code>show cef interface [interface-id]</code>	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 10	<code>show adjacency</code>	CEF の隣接関係テーブル情報を表示します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

等価コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティング テーブルに複数の等価コスト ルートが含まれる場合は、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格納されている場合、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、回線に障害が発生した場合に備えて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し、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、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。

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	<code>configure terminal</code>	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	<code>router {bgp rip ospf eigrp}</code>	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	<code>maximum-paths maximum</code>	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 ~ 8 です。ほとんどの IP ルーティング プロトコルではデフォルトは 4 ですが、BGP に限りデフォルトは 1 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip protocols</code>	<i>Maximum path</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを経由して送信元と宛先の間でパケットを転送するユーザ定義のルートです。スタティック ルートは、ルータが特定の宛先へのルートを構築できない場合に重要性を持つことがあり、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	<code>configure terminal</code>	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	<code>ip route prefix mask {address interface} [distance]</code>	スタティック ルートを確立します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip route</code>	設定を確認するため、ルーティング テーブルの現在の状態を表示します。
ステップ 5	<code>copy running-config startup-config</code>	(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。

スタティック ルートは、ユーザによって削除されるまでスイッチに保持されます。ただし、管理ディスタンスの値を割り当てることで、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、デフォルトの管理ディスタンスが設定されています (表 36-16 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 プロトコルの管理ディスタンスよりも大きな値になるように設定します。

表 36-16 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
EIGRP サマリー ルート	5
EBGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IBGP	200
不明	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。`redistribute` スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、ルーティング テーブルでは、インターフェイスを指し示すスタティック ルートが接続され、その結果スタティックな性質を失っ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 ルートを定義する場合は、ダイナミック ルーティング プロトコルに `redistribute` スタティック コマンドを指定しないかぎり、ルートはアドバタイズされません。

インターフェイスがダウンすると、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に対して有効なネクストホップが見つからないスタティック 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

ルータは、他のネットワークすべてへのルートを学習できるわけではありません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルトルートをスマート ルータ宛に指定します（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学習されるか、ルータごとに設定されます。ダイナミックな内部ルーティング プロトコルはそのほとんどが、スマート ルータを使用してデフォルト情報をダイナミックに生成し、それ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、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク **0.0.0.0** がアドバタイズされます。

ネットワークのデフォルト ルートを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータのデフォルト ルートをそのルータ自身で生成できるようにする方法はいくつかありますが、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 ルートを指定するという方法もその 1 つです。

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	選択されたデフォルト ルートを最終ゲートウェイのディスプレイに表示します。
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場合は、これ以上の設定は必要ありません。システムにより、ルーティング テーブルが定期的にはスキャンされ、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。シスコのルータでは、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、管理ディスタンスおよびメトリック情報が使用されます。

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い場合でも、そこへのパスが格納されていれば、そのネットワークは 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布

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て、ルーティング プロトコル間で情報を再配布できます。ルーティング プロトコル間での情報の再配布は、サポートされているすべての IP ベース ルーティング プロトコルで行われます。

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布を条件付きで制御することもできます。**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 **set** ルートマップ コンフィギュレーション コマンドを使用すると、ルートマップの条件部を定義できます。**match** コマンドは条件が一致しなければならないことを示します。**set** コマンドを使用すると、**match** コマンドで定義された条件をルーティングアップデートが満たす場合に実行されるアクションを指定できます。再配布はプロトコルに依存しない機能ですが、**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 **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。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理は一切実行されません。このため、**match** コマンドまたは **set** コマンドを少なくとも 1 つは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 に送信されるため、CPU の使用量が増大する原因となります。

route-map 文は、**permit** が指定されているか **deny** が指定されているかによって、その意味が異なります。この文に **deny** が指定されている場合、一致基準を満たすパケットは通常の転送チャンネルを通じて返送されます (宛先ベース ルーティング)。この文に **permit** が指定されている場合は、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ンネルを介して転送されます。

match 句および **set** 句による入力の実行が完了したら、BGP ルートマップの **continue** 句を使用して、ルートマップに対する追加の入力を実行できます。**continue** 句を使用して、より多くのモジュラポリシー定義を設定して組織化すれば、特定のポリシー設定を同じルートマップ内で繰り返す必要がなくなります。スイッチでは、発信ポリシーに対して **continue** 句がサポートされています。ルートマップの **continue** 句の使用に関する詳細については、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 はいずれも任意ですが、**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 **set** ルートマップ コンフィギュレーション コマンドはそれぞれ、少なくとも 1 つ入力する必要があります。

再配布用のルート 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 <i>map-tag</i> [permit deny] [<i>sequence number</i>]	再配布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。 <i>map-tag</i> : 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 コマンドでは、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布されます。 deny が指定されている場合、ルートは再配布されません。 <i>sequence number</i> (任意) : すでに同じ名前が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 マップの位置を表す番号を指定します。
ステップ 3 match as-path <i>path-list-number</i>	BGP AS パス アクセス リストを一致基準にします。
ステップ 4 match community-list <i>community-list-number</i> [exact]	BGP コミュニティ リストを一致基準にします。
ステップ 5 match ip address { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	名前または番号を指定し、標準アクセス リストを一致基準にします。1 ~ 199 の整数を指定できます。
ステップ 6 match metric <i>metric-value</i>	指定されたルート メトリックを一致基準にします。 <i>metric-value</i> には、0 ~ 4294967295 の範囲で値が指定された EIGRP のメトリックを指定できます。
ステップ 7 match ip next-hop { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	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 アドレスを一致基準にします。
ステップ 8 match tag <i>tag value</i> [... <i>tag-value</i>]	1 つまたは複数のルート タグ値の中から指定されたタグ値を一致基準にします。0 ~ 4294967295 の整数を指定できます。
ステップ 9 match interface <i>type number</i> [... <i>type number</i>]	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 ホップへのルートを一一致基準にします。
ステップ 10 match ip route-source { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	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を一致基準にします。
ステップ 11 match route-type { local internal external [type-1 type-2]}	指定された route-type の値を一致基準にします。 <ul style="list-style-type: none"> local : ローカルに生成された BGP ルート internal : OSPF エリア内ルート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

■ プロトコルに依存しない機能の設定

	コマンド	目的
ステップ 12	<code>set dampening halflife reuse suppress max-suppress-time</code>	BGP ルート ダンプニング係数を設定します。
ステップ 13	<code>set local-preference value</code>	ローカル BGP パスに値を割り当てます。
ステップ 14	<code>set origin {igp egp as incomplete}</code>	BGP の送信元コードを設定します。
ステップ 15	<code>set as-path {tag prepend as-path-string}</code>	BGP AS パスを変更します。
ステップ 16	<code>set level {level-1 level-2 level-1-2 stub-area backbone}</code>	ルーティング ドメインの指定エリアにアダプ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 の NSSA エリアおよびバックボーンエリアです。
ステップ 17	<code>set metric metric value</code>	再配布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)。 <i>metric value</i> には 294967295 ~ 294967295 の整数を指定します。
ステップ 18	<code>set metric bandwidth delay reliability loading mtu</code>	再配布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)。 <ul style="list-style-type: none"> <i>bandwidth</i> : ルートのメトリック値または IGRP 帯域幅 (キロビット/秒単位) を 0 ~ 4294967295 の範囲で指定します。 <i>delay</i> : ルート遅延を 0 ~ 4294967295 の範囲で指定します (10 マイクロ秒単位)。 <i>reliability</i> : パケット伝送の成功可能性を 0 ~ 255 の数値で指定します。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。 <i>loading</i> : ルートの有効帯域幅を 0 ~ 255 の数値で指定します (255 は 100% の負荷)。 <i>mtu</i> : ルートの MTU の最小サイズをバイト単位で指定します。指定できる範囲は 0 ~ 4294967295 です。
ステップ 19	<code>set metric-type {type-1 type-2}</code>	再配布されるルートに OSPF 外部メトリック タイプを設定します。
ステップ 20	<code>set metric-type internal</code>	ネクストホップの IGP メトリックと一致するように、EBGP ネイバーにアダプタイズされるプレフィックスの MED 値を設定します。
ステップ 21	<code>set weight</code>	ルーティング テーブルの BGP の重みを設定します。指定できる値は 1 ~ 65535 です。
ステップ 22	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 23	<code>show route-map</code>	設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 24	<code>copy running-config startup-config</code>	(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、**no match** ルート マップ コンフィギュレーション コマンド、または **no set** ルート マップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを配布したり、ルート再配布を制御したりできます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>router {bgp rip ospf eigrp}</code>	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	<code>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]</code>	ルーティング プロトコル間でルートを再配布します。 <code>route-map</code> を指定しないと、すべてのルートが再配布されます。キーワード <code>route-map</code> に <code>map-tag</code> を指定しないと、ルートは配布されません。
ステップ 4	<code>default-metric number</code>	現在のルーティング プロトコルが、再配布されたすべてのルートに対して同じメトリック値を使用するように設定します (BGP、RIP、OSPF)。
ステップ 5	<code>default-metric bandwidth delay reliability loading mtu</code>	EIGRP ルーティング プロトコルが、EIGRP 以外で再配布されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show route-map</code>	設定を確認するため、設定されたすべてのルートマップ、または指定された単独のルート マップを表示します。
ステップ 8	<code>copy running-config startup-config</code>	(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。

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

異なるルーティング プロトコル間では、必ずしもメトリックは変換されません。このような場合、再配布されたルートには疑似的なメトリックが割り当てられます。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無制御に交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配布メトリックが定義されていない場合は、ルーティング プロトコル間でメトリックが自動的に変換されることもあります。

- RIP では、スタティック ルートの自動的な再配布が可能です。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 モードでは、いずれのプロトコルでも、他のルーティング プロトコルの再配布が可能です。

PBR の設定

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用すると、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下げること、ルーティングをより細かく制御できます。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 ポリシーを設定できます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、双方向対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広帯域で高コストのリンクを短時間使用し、E メールなど日常的に使用するアプリケーションデータは狭帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、Access Control List (ACL; アクセスコントロールリスト) 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パケットはすべて、ルートマップを通過します。ルートマップで定義された基準に基づいて、パケットは適切なネクストホップに転送 (ルーティング) されます。

- パケットがどの route-map 文とも一致しない場合は、すべての set 句が適用されます。
- いずれかの文に permit が指定されている場合、どの route-map 文とも一致しないパケットは、通常の転送チャン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、deny を指定できる route-map 文はサポートされていません。

ルートマップの設定に関する詳細については、「[ルートマップによるルーティング情報の再配布 \(P.36-105\)](#)」を参照してください。

送信元アドレスの一致基準を指定する場合は標準 IP ACL を使用し、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を基にした一致基準を指定する場合は拡張 IP ACL 使用します。ルートマップでは、一致が検出されるまでこのプロセスが行われます。一致が検出されない場合は、通常の宛先ベースルーティングが行われます。match 文のリストの末尾には、暗黙的に拒否されるエントリがあります。

match 句に一致した場合は、set 句を使用して、パス内のネクストホップルータを識別する IP アドレスを指定できます。

PBR 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。表示されるにもかかわらずスイッチでサポートされていない PBR コマンドについては、[付録 C「Cisco IOS リリース 12.2\(52\)SE でサポートされていないコマンド」](#)を参照してください。

PBR 設定時の注意事項

PBR の設定を開始する前に、次の点に注意してください。

- マルチキャストトラフィックについては、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャストトラフィックだけです。
- 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 に対して **route-map deny** 文を使用できません。
- ポリシールートマップは、レイヤ 3 モードの EtherChannel ポートチャンネルには適用できますが、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 のメンバーにはなれません。
- スイッチには最大 246 の IP ポリシールートマップを定義できます。
- スイッチには、PBR 用として最大 512 の Access Control Entry (ACE; アクセスコントロールエントリ) を定義できます。
- ルートマップに一致基準を設定する場合は、次の点に注意してください。
 - ローカルアドレス宛のパケットを許可する ACL は、一致基準にはしないでください。PBR がこれらのパケットを転送すると、ping や Telnet の障害、またはルートプロトコルフラッピングの原因となります。

- 拒否 ACE を含む ACL は、一致基準にはしないでください。拒否 ACE に一致するパケットは CPU に送信されるため、場合によっては CPU の利用率が高くなる原因となります。
- PBR を使用するには、**sdm prefer default** 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 テンプレートをイネーブルにしておく必要があります。PBR では、レイヤ 2 テンプレートは使用できません。SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっている場合、VRF をイネーブルにはできません。VRF がインターフェイスでイネーブルになっている場合、PBR をイネーブルにはできません。
- PBR で使用される Ternary CAM (TCAM) エントリの数は、ルート マップそのもの、使用される ACL、および 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、IP precedence および 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 PBR はサポートされていません。有効な set アクションがないか、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされていません。

PBR のイネーブル化

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準およびすべての match 句と一致した場合の動作を指定したルート マップを作成する必要があります。さらに、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにする必要があります。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 句と一致したものはすべて PBR の対象となります。

PBR の高速スイッチングや実装は、スイッチの速度低下を引き起こさない速度範囲で行われます。高速スイッチングされた PBR では、ほとんどの match コマンドおよび 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 をイネーブルにする必要があります。PBR の高速スイッチングは、デフォルトでディセーブルです。

スイッチで生成されたパケット（ローカル パケット）は通常、ポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルにイネーブル化すると、そのスイッチから送信されるすべてのパケットがローカル PBR の対象となります。ローカル PBR は、デフォルトでディセーブルに設定されています。

■ プロトコルに依存しない機能の設定

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]	<p>パケットの出力場所を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> • 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 コマンドでは、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。 <p>(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 文はサポートされていません。</p> <ul style="list-style-type: none"> • sequence number (任意) :すでに同じ名前が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 マップの位置を表す番号を指定します。
ステップ3 match ip address {access-list-number access-list-name} [...access-list-number ...access-list-name]	<p>1 つまたは複数の標準アクセス リストまたは拡張アクセス リストで許可されている送信元 IP アドレスおよび宛先 IP アドレスを一致基準にします。</p> <p>(注) 拒否 ACE を含む ACL や、ローカル アドレス宛のパケットを許可する ACL は入力しないでください。</p> <p>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。</p>
ステップ4 set ip next-hop ip-address [...ip-address]	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します (ネクスト ホップは隣接していなければなりません)。
ステップ5 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ6 interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ7 no shutdown	必要に応じて、インターフェイスをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ8 ip policy route-map map-tag	<p>レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを指定します。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 エントリを設定できます。これらのエントリは、最初の一致が検出されるまで、シーケンス番号順に評価されます。一致が検出されない場合、パケットは通常どおりにルーティングされます。</p> <p>(注) IP ポリシー ルート マップに deny 文が含まれている場合、設定は失敗します。</p>

コマンド	目的
ステップ 9 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 10 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 11 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 PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 12 end	特権 EXEC モードに戻ります。
ステップ 13 show route-map [map-name]	(任意) 設定を確認するため、設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。
ステップ 14 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 15 show ip local policy	(任意) ローカル PBR がイネーブルであるかどうかを表示します。またイネーブルの場合は、使用されているルート マップも表示します。
ステップ 16 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、**no match** ルート マップ コンフィギュレーション コマンド、または **no set** ルート マップ コンフィギュレーション コマンドを使用します。インターフェイス上で PBR をディセーブルにするには、**no ip policy route-map map-tag** インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されるパケットに対して PBR をディセーブルにするには、**ip local policy route-map map-tag** グローバル コンフィギュレーション コマンドを使用します。

ルーティング情報のフィルタリング

ここでは、ルーティング プロトコル情報をフィルタリングする手順について説明します。



(注) OSPF プロセス間でルートが再配布される場合、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 インターフェイスを経由して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、受動として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 インターフェイスを経由しては送受信されません。

多数のインターフェイスが存在するネットワークで、手動による受動インターフェイスの設定を省くには、**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、すべてのインターフェイスをデフォルトで受動インターフェイスになるように設定します。そのうえで、隣接関係が必要なインターフェイスを手動で設定します。

■ プロトコルに依存しない機能の設定

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	<code>configure terminal</code>	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	<code>router {bgp rip ospf eigrp}</code>	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	<code>passive-interface interface-id</code>	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	<code>passive-interface default</code>	(任意) すべてのインターフェイスを、デフォルトで受動インターフェイスとなるように設定します。
ステップ 5	<code>no passive-interface interface type</code>	(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	<code>network network-address</code>	(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。 <code>network-address</code> には IP アドレスを指定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>copy running-config startup-config</code>	(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。

受動インターフェイス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 モニタリング特権 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場合は、**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。キーワード **default** 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受動インターフェイスに設定されます。このとき、**no passive-interface** ルータ コンフィギュレーション コマンドを使用することで、隣接関係を必要とする各インターフェイスを個別に設定できます。**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で使用するのが有効です。

ルーティング アップデートのアドバタイズおよび処理の制御

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

distribute-list ルータ コンフィギュレーション コマンドを使用して、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 (この機能は OSPF には適用されません)。

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	<code>configure terminal</code>	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	<code>router {bgp rip eigrp}</code>	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	<code>distribute-list {access-list-number access-list-name} out [interface-name routing process autonomous-system-number]</code>	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。

	コマンド	目的
ステップ 4	<code>distribute-list {access-list-number access-list-name} in [type-number]</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	(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取り消すには、**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取り消すには、**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、それぞれの正確性に差があることもあります。そこで、さまざまな送信元から送られる情報には、フィルタリングを使用することによりプライオリティを設定できるようになっています。「管理ディスタンス」は、ルータやルータ グループといったルーティング情報の送信元に対する信頼度を表した数値です。大規模ネットワークでは、各ルーティング プロトコルの信頼度に違いがある場合があります。管理ディスタンスの値を指定すると、ルーティング情報の送信元がルータによって自動的に区別されるようになります。ルータでは常に、ルーティング プロトコルの管理ディスタンスが最短（値が最小）であるルートが選択されます。表 36-16 (P.36-104) は、ルーティング情報のさまざまな送信元に対するデフォルトの管理ディスタンスをまとめたものです。

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	<code>configure terminal</code>	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	<code>router {bgp rip ospf eigrp}</code>	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	<code>distance weight {ip-address {ip-address mask}} [ip access list]</code>	管理ディスタンスを定義します。 <i>weight</i> : 管理ディスタンスを 10 ~ 255 の整数として指定します。 <i>weight</i> を単独で使用すると、デフォルトの管理ディスタンスが指定されます。デフォルトの管理ディスタンスは、ルーティング情報の送信元に対して他の指定事項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) <i>ip access list</i> : 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip protocols</code>	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	<code>copy running-config startup-config</code>	(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。

管理ディスタンスを削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

認証鍵の管理

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 EIGRP および RIP バージョン 2 で使用できます。

認証鍵の管理を行うには、あらかじめ認証をイネーブルにしておく必要があります。各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。認証鍵の管理を行うには、キーチェーンを定義したあと、そのキーチェーンに属する鍵を指定し、それぞれの鍵の有効期間を指定します。それぞれの鍵には、ローカルに保存される独自の鍵 ID があります (**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)。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。

鍵は有効期間とともに複数設定できます。ただし、有効な鍵が複数存在する場合でも、送信される認証パケットは 1 つだけです。鍵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ります。

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	キーチェーンを指定し、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。この文字列には 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、先頭文字には数字を使用できません。
ステップ 5 accept-lifetime start-time {infinite end-time duration seconds}	(任意) 鍵を受信できる期間を指定します。 <i>start-time</i> および <i>end-time</i> の構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。 <i>end-time</i> および duration のデフォルトは infinite です。
ステップ 6 send-lifetime start-time {infinite end-time duration seconds}	(任意) 鍵を送信できる期間を指定します。 <i>start-time</i> および <i>end-time</i> の構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無期限です。指定できる最初の日付は 1993 年 1 月 1 日です。 <i>end-time</i> および duration のデフォルトは 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 ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを消去したり、ステータスを表示したりするには、表 36-17 に示す特権 EXEC コマンドを使用します。

表 36-17 IP ルートの消去またはルート ステータスの表示に使用するコマンド

コマンド	目的
clear ip route { <i>network</i> [<i>mask</i> *]}	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状態を表示します。
show ip route [<i>address</i> [<i>mask</i>] [longer-prefixes]] [<i>protocol</i> [<i>process-id</i>]]	ルーティング テーブルの現在の状態を表示します。
show ip route summary	ルーティング テーブルの現在の状態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 [<i>map-name</i>]	設定されたすべてのルート マップ、または指定された単独のルート マップを表示します。

