IP ルーティング：RIP コンフィギュレーション ガイド

IP Routing: RIP Configuration Guide

Cisco IOS XE Release 3S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

IP ルーティング : RIP コンフィギュレーション ガイド

Routing Information Protocol の設定

Routing Information Protocol（RIP）は小規模から中規模の TCP/IP ネットワークで一般的に使用されるルーティング プロトコルです。また、距離ベクトル アルゴリズムを使用してルートを計算する安定したプロトコルです。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「RIP の設定に関する機能情報」（P.29）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

RIP の設定に関する前提条件

RIP を設定する前に、**ip routing** コマンドを設定する必要があります。**ip routing** コマンドの設定の詳細については、『*Cisco IOS IP Routing: RIP Command Reference*』を参照してください。

RIP の設定に関する制約事項

RIP が異なるルートの価値を評価するときに使用するメトリックは、*ホップ カウント* です。ホップ カウントとは、1 つのルート内で通過する可能性があるルートの数です。直接接続しているネットワークのメトリックはゼロです。到達不能のネットワークのメトリックは 16 です。このようにメトリックの範囲は狭いため、RIP は大規模なネットワークに適さないルーティング プロトコルです。

RIP の設定に関する情報

Routing Information Protocol（RIP）を設定するには、次の概念を理解する必要があります。

RIP の概要

Routing Information Protocol では、ブロードキャストの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データ パケットを使用して、ルーティング情報を交換しています。Cisco IOS XE ソフトウェアからは、ルーティング情報の更新が 30 秒ごとに送信されます。この処理は *アドバタイジング* と呼ばれます。ルータがもう 1 つのルータから更新を 180 秒間受信しない場合、更新されないルータとの間のルートは使用不能とマークされます。240 秒経過しても更新がない場合、その更新されないルータのルーティング テーブル エントリはすべて削除されます。

RIP を実行しているルータは、RIP を実行しているもう 1 つのルータからの更新によってデフォルト ネットワークを受信できます。また、ルータは RIP を使用して独自にデフォルト ネットワークを作成（生成）できます。いずれの場合でも、デフォルト ネットワークは RIP を介して他の RIP ネイバーにアドバタイズされます。

RIP Version 2 のシスコの実装では、プレーン テキスト認証、Message Digest 5（MD5）認証、ルート集約、Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）、および Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）をサポートしています。

RIP のルーティング アップデート

RIP は、定期的に、またネットワーク トポロジに変更があったときに、ルーティング アップデート メッセージを送信します。エントリに対する変更を含む RIP のルーティング アップデートをルータが受信すると、ルータのルーティング テーブルは新しいルートを反映するために更新されます。パスのメトリック値は 1 ずつ増え、送信側はネクスト ホップとして示されます。RIP ルータが保持するのは、宛先への最適なルート（メトリック値が最小のルート）のみです。ルータはルーティング テーブルの更新が終わり次第、RIP ルーティング アップデートの送信を開始して、他のネットワーク ルータに変更を通知します。この更新は、RIP ルータが送信する定期的にスケジュールされた更新とは別に送信されます。

RIP のルーティング メトリック

RIP は単一のルーティング メトリック（ホップ カウント）を使用して、送信元と宛先のネットワーク間の距離を測定します。送信元から宛先までのパスの各ホップには、ホップ数の値（通常は 1）が割り当てられます。新規または変更された宛先ネットワーク エントリを含むルーティング アップデートをルータが受信すると、更新で示されているメトリック値に 1 を追加し、ルーティング テーブルにそのネットワークを入力します。送信側の IP アドレスはネクスト ホップとして使用されます。インターフェイス ネットワークのネットワークが指定されていない場合、どの RIP 更新でもアドバタイズされません。

RIP Version 2 と認証のイネーブル化

RIP Version 2 のシスコの実装では、認証、キー管理、ルート集約、CIDR、および VLSM をサポートしています。認証キーの管理の詳細については、「*Configuring IP Routing Protocol-Independent Features*」モジュールの「Managing Authentication Keys」の項を参照してください。

デフォルトで、ソフトウェアは RIP Version 1 および Version 2 パケットを受信しますが、送信するのは Version 1 パケットのみです。Version 1 パケットのみを送受信するようにソフトウェアを設定できます。または、Version 2 パケットのみを送受信するようにソフトウェアを設定できます。デフォルトの動作を上書きするには、インターフェイスから送信する RIP バージョンを設定します。同様に、インターフェイスから受信したパケットを処理する方法も制御できます。

RIP Version 1 は認証をサポートしていません。RIP Version 2 パケットを送受信している場合、インターフェイスで RIP 認証をイネーブルにできます。

キー チェーンによって、そのインターフェイスで使用できるキー セットが決まります。キー チェーンが設定されていない場合、デフォルトの認証を含め、認証はそのインターフェイスで実行されません。そのため、「*Configuring IP Routing Protocol-Independent Features*」モジュールの「Managing Authentication Keys」のタスクも実行する必要があります。

RIP 認証がイネーブルにされているインターフェイスでは、2 モードの認証がサポートされます。プレーン テキスト認証と MD5 認証です。各 RIP Version 2 パケットのデフォルト認証は、プレーン テキスト認証です。

（注） セキュリティ上の目的から、RIP パケットにはプレーン テキスト認証を使用しないでください。プレーン テキスト認証では、各 RIP Version 2 パケットで暗号化されていない認証キーが送信されます。プレーン テキスト認証を使用するのは、セキュリティが問題にならない場合です。たとえば、誤って設定したホストがルーティングに参加しないようにする場合などです。

ルーティング情報の交換

通常、RIP はブロードキャスト プロトコルです。そのため、RIP 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には、このルーティング情報の交換を許可するように Cisco IOS XE ソフトウェアを設定する必要があります。

ルーティング アップデートを交換するインターフェイス セットを制御するには、**passive-interface** ルータ コンフィギュレーション コマンドを設定して、指定したインターフェイスでルーティング アップデートの送信をディセーブルにします。フィルタの詳細については、「*Configuring IP Routing Protocol-Independent Features*」モジュールの「Filter Routing Information」の項を参照してください。

オフセット リストは、RIP を介して学習されるルートに対する着信および送信のメトリックを増やすためのメカニズムです。オプションとして、アクセス リスト、またはインターフェイスのいずれかを使用して、オフセット リストを制限することができます。ルーティング メトリックの値を増やすには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

ルーティング プロトコルでは、ルーティング アップデートの頻度、ルートが無効になるまでの時間、および他のパラメータなどの変数を決めるいくつかのタイマーを使用します。このタイマーを調整して、固有のインターネットワークのニーズに合わせてルーティング プロトコルのパフォーマンスを変更できます。次のようにタイマーを調整できます。

- ルーティング アップデートを更新する頻度（更新の秒単位の間隔）
- ルートが無効と宣言された後の間隔（秒単位）
- より短いパスに関するルーティング情報が抑制されている間隔（秒単位）
- ルーティング テーブルからルートが削除する前に経過する必要がある時間（秒単位）
- ルーティング アップデートが延期される合計時間

また、ソフトウェアの IP ルーティングのサポートを調整して、多様な IP ルーティング アルゴリズムのコンバージェンスを高速化できます。結果として、冗長ルータへのフォールバックが迅速になります。総体的な効果として、迅速なリカバリが重要な状況で、ネットワークのエンドユーザの作業が中断する問題が最小限に抑えられます。

さらに、アドレス ファミリ（または VRF）にのみ適用される固有のタイマーを指定することもできます。1 つのアドレス ファミリに対して timers basic コマンドを指定する必要があります。そうしないと、RIP ルーティングの設定内容に関係なく、timers basic コマンドのシステム デフォルトが使用されます。VRF は基本の RIP 設定のタイマー値を継承しません。timers basic コマンドを使用して明示的に変更していない場合、VRF は常にシステム デフォルト タイマーを使用します。

アドレス ファミリ（VRF）のタイマーを調整する例については、この章の末尾にある「アドレス ファミリ タイマーの設定：例」の項を参照してください。

RIP のルート集約

RIP Version 2 のルートを集約すると、大規模なネットワークのスケーラビリティと効率が改善されます。IP アドレスの集約とは、RIP ルーティング テーブルに子ルート（サマリー アドレスに含まれる個々の IP アドレスの任意の組み合わせに対して作成されるルート）のエントリがないことを意味します。そのため、テーブルのサイズが削減され、ルータが処理できるルート数が増えます。

サマリー IP アドレスは、次の理由から、個々にアドバタイズされた複数の IP ルートよりも効率的に機能します。

- RIP データベースの集約されたルートが最初に処理されます。
- RIP がルーティング データベースを調べるときに、集約されたルートに含まれる任意の関連付けられた子ルートはスキップされるため、必要な処理時間が短縮されます。

Cisco ルータは次の 2 つの方法でルートを集約できます。

- 自動。クラスフル ネットワーク境界を越えるときに、サブプレフィクスをクラスフル ネットワーク境界に自動的に集約する方法（自動集約）。

（注） デフォルトでは、自動集約がイネーブルになっています。

- アドレス プールをダイヤルアップ クライアントに提供できるように、設定に従って、（ネットワーク アクセス サーバ上の）指定したインターフェイスで、集約したローカル IP アドレス プールをアドバタイズする方法。

RIP が RIP データベースのサマリー アドレスが必要だと判断した場合、サマリー エントリは RIP ルーティング データベースに作成されます。サマリー アドレスに子アドレスがある限り、そのアドレスはルーティング データベースに残ります。最後の子ルートが削除されると、サマリー エントリもデータベースから削除されます。このデータベース エントリの処理方法によって、各子ルートがエントリに列挙されないため、データベースのエントリ数は減ります。また、集約エントリ自体は、有効な子ルートがなくなったときに削除されます。

RIP Version 2 のルート集約では、集約エントリの「最適なルート」の最小のメトリック、または現在の子ルートすべてのうち最小のメトリックをアドバタイズする必要があります。集約されたサマリー ルートの最適なメトリックは、ルートが初期化されたとき、またはアドバタイズ時に特定のルートでメトリックの変更があった場合に計算されます。集約されたルートがアドバタイズされたときではありません。

ip summary-address rip router コンフィギュレーション コマンドを使用すると、RIP Version 2 経由で認識された特定のルート セット、または RIP Version 2 に再配布されたルート セットが集約されます。ホスト ルートは、特に集約に適用できます。

スプリット ホライズンを使用する例については、この章の末尾にある「ルート集約の設定：例」の項を参照してください。

インターフェイスで集約するルートを確認するには、**show ip protocols** EXEC コマンドを使用します。RIP データベースでサマリー アドレス エントリを確認できます。このエントリがデータベースに出現するのは、関連する子ルートが集約されている場合のみです。サマリー アドレスに基づいて集約されている関連ルートがある場合に、RIP ルーティング データベース エントリのサマリー アドレス エントリを表示するには、EXEC モードで **show ip rip database** コマンドを使用します。サマリー アドレスの最後の子ルートが無効になると、そのサマリー アドレスもルーティング テーブルから削除されます。

スプリット ホライズン メカニズム

通常、ブロードキャスト型の IP ネットワークに接続し、ディスタンスベクトル ルーティング プロトコルを使用しているルータは、*スプリット ホライズン* メカニズムを使用して、ルーティングがループする可能性を軽減しています。スプリット ホライズンでは、情報が発生したインターフェイス外部のルータによって、ルートに関する情報がアドバタイズされることが防止されます。通常、この動作は、複数のルータ間の（特にリンクが破損した場合の）通信を最適化します。ただし、非ブロードキャスト ネットワーク（フレーム リレーや Switched Multimegabit Digital System（SMDS）など）では、この動作が適さない状況が発生することがあります。このような状況の場合、RIP でスプリット ホライズンを無効にできます。

セカンダリ IP アドレスを使用してインターフェイスを設定し、スプリット ホライズンがイネーブルの場合、そのセカンダリ アドレスから更新を送信できないことがあります。スプリット ホライズンを無効にしない場合、1 つのルーティング アップデートは、1 つのネットワーク番号ごとに送信されます。

RIP アップデートのパケット間遅延

デフォルトでは、複数パケットの RIP アップデートが送信される場合、パケット間に遅延は追加されません。ハイエンド ルータから低速のルータに送信する場合、このようなパケット間遅延を RIP アップデートに追加できます（範囲は 8 ～ 50 ミリ秒）。

WAN 回路上の RIP の最適化

ルータは、多数の宛先に接続する可能性があるコネクション型ネットワークで使用されます。WAN 上の回路はオンデマンドで確立され、トラフィックが低下したときに放棄されます。アプリケーションによっては、ユーザ データに関する任意の 2 サイト間の接続が短く、比較的まれな場合があります。

送信元 IP アドレス

デフォルトで、着信 RIP ルーティング アップデートの送信元 IP アドレスは確認されます。その送信元アドレスが無効な場合、ルーティング アップデートは廃棄されます。「ネットワーク外」のルータがあり、その更新を受信する場合、この機能をディセーブルにできます。ただし、通常の状況では、この機能をディセーブルにしないことをお勧めします。

ネイバー ルータ認証

ネイバー ルータ認証を設定すると、ルータが不正なルート更新情報を受け取るのを防ぐことができます。設定すると、ネイバー ルータ間でルーティング アップデートが交換されるたびに、ネイバー認証が発生します。この認証により、信頼できるソースから信頼できるルーティング情報をルータが受け取ることができるようになります。

ネイバー認証を使用しない場合は、不正または悪意があるルーティング更新情報によってネットワーク トラフィックのセキュリティが侵害されることがあります。セキュリティの侵害は、誰かがネットワーク トラフィックを迂回または分析する場合に発生することがあります。たとえば、許可されていないルータは偽のルーティング更新情報を送信して他のルータを騙し、そのルータにトラフィックを正しくない送信先に送信させることができます。迂回されたトラフィックを分析して、組織に関する機密情報を得たり、単にそのトラフィックを使用して組織のネットワークの通信能力を破壊したりできます。ネイバー認証によって、このような不正なルーティング アップデートの受信を回避できます。

ネイバー認証をルータで設定すると、ルータは受信する各ルーティング アップデート パケットの送信元を認証します。この処理は、送信側と受信側のルータの両方が知っている認証キー（パスワードと呼ばれることもあります）の交換で達成されます。

使用されるネイバー認証には、プレーン テキスト認証と Message Digest Algorithm Version 5（MD5）の 2 種類があります。いずれの形式も同様の機能ですが、MD5 は認証キーではなくメッセージ ダイジェスト（「ハッシュ」とも呼ばれます）を送信するという例外があります。メッセージ ダイジェストはキーとメッセージを使用して作成されますが、キー自体は送信されないため、送信中のキーの読み取りを回避できます。プレーン テキスト認証はネットワークで認証キーを送信します。

（注） セキュリティ戦略の一部として使用する場合、プレーン テキスト認証は推奨されません。プレーン テキスト認証の主な用途は、ルーティング インフラストラクチャを誤って変更する処理を回避する場合です。一方、MD5 認証は、推奨されるセキュリティ方法です。

プレーン テキスト認証では、参加している各ネイバー ルータが認証キーを共有する必要があります。このキーは、設定中に各ルータで指定されます。一部のプロトコルでは、複数のキーを指定できます。そのため、各キーはキー番号で識別する必要があります。

一般的に、ルーティング アップデートが送信されると、次の認証シーケンスが発生します。

1. ルータは、キーおよび対応するキー番号とともにルーティング更新情報をネイバー ルータに送信します。1 つのキーしか使用できないプロトコルでは、キー番号は常にゼロになります。

   受信側（ネイバー）ルータは、そのルータのメモリに格納された同じキーと受け取ったキーを照合します。

2. 2 つのキーが一致すると、受信側ルータはルーティング更新パケットを受け取ります。2 つのキーが一致しない場合、ルーティング アップデート パケットは拒否されます。

ネイバー ルータ認証のもう 1 つの形式は、キー チェーンを使用してキー管理を設定する方法です。キー チェーンを設定する場合は、一連のキーにライフタイムを指定します。Cisco IOS XE ソフトウェアはこれらの各キーを順番に使用します。この処理で、キーが危険にさらされる可能性が軽減されます。キー チェーンの設定情報の詳細については、『*Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide*』の「Configuring IP Routing Protocol-Independent Features」モジュールにある「Managing Authentication Keys」の項を参照してください。

IP-RIP Delay Start

IP-RIP Delay Start 機能は、ネイバー ルータ間のネットワーク接続が完全に機能するまで、RIPv2 ネイバー セッションの開始を遅延させるために Cisco ルータで使用されます。その結果、ルータがシスコ製以外のネイバー ルータに送信する最初の MD5 パケットのシーケンス番号は常に 0 です。MD5 認証を使用してネイバー ルータとの RIPv2 ネイバー セッションを確立するように設定されたルータのデフォルト動作では、物理インターフェイスの起動時に、MD5 パケットの送信を開始します。

RIP の設定方法

ここでは、次の作業について説明します。

RIP のイネーブル化と RIP パラメータの設定

この作業を実行して、RIP をイネーブルにし、RIP パラメータを設定します。

オフセット リスト

オフセット リストは、RIP を介して学習されるルートに対する着信および送信のメトリックを増やすためのメカニズムです。ルーティング メトリックの値を増やすローカル メカニズムを提供するために実行されます。オプションとして、アクセス リスト、またはインターフェイスのいずれかを使用して、オフセット リストを制限することができます。

タイマー

ルーティング プロトコルでは、ルーティング アップデートの頻度、ルートが無効になるまでの時間、および他のパラメータなどの変数を決めるいくつかのタイマーを使用します。このタイマーを調整して、固有のインターネットワークのニーズに合わせてルーティング プロトコルのパフォーマンスを変更できます。次のようにタイマーを調整できます。

- ルーティング アップデートを更新する頻度（更新の秒単位の間隔）
- ルートが無効と宣言された後の間隔（秒単位）
- より短いパスに関するルーティング情報が抑制されている間隔（秒単位）
- ルーティング テーブルからルートが削除する前に経過する必要がある時間（秒単位）
- ルーティング アップデートが延期される合計時間

また、ソフトウェアの IP ルーティングのサポートを調整して、多様な IP ルーティング アルゴリズムのコンバージェンスを高速化できます。結果として、冗長ルータへのフォールバックが迅速になります。総体的な効果として、迅速なリカバリが重要な状況で、ネットワークのエンドユーザの作業が中断する問題が最小限に抑えられます。

手順の概要

1. **enable**
2. **configure terminal**

3. **router rip**
4. **network** *ip-address*
5. **neighbor** *ip-address*
6. **offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*]
7. **timers basic** *update invalid holddown flush* [*sleeptime*]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**router rip** **例：** `Router(config)# router rip`	RIP ルーティング プロセスをイネーブルにして、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	**network** *ip-address* **例：** `Router(config-router)# network 10.1.1.0`	ネットワークを RIP ルーティング プロセスと関連付けます。
ステップ 5	**neighbor** *ip-address* **例：** `Router(config-router)# neighbor 1.1.1.2`	ルーティング情報を交換するネイバー ルータを定義します。
ステップ 6	**offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*] **例：** `Router(config-router)# offset-list 98 in 1 Ethernet 1/0`	（任意）ルーティング メトリックにオフセットを適用します。
ステップ 7	**timers basic** *update invalid holddown flush* [*sleeptime*] **例：** `Router(config-router)# timers basic 1 2 3 4`	（任意）ルーティング プロトコル タイマーを調整します。
ステップ 8	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

RIP バージョンの指定と認証のイネーブル化

この作業を実行して、RIP バージョンを指定し、認証をイネーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** {**1** | **2**}
5. **exit**
6. **interface** *type number*
7. **ip rip send version** [**1**] [**2**]
8. **ip rip receive version** [**1**] [**2**]
9. **ip rip authentication key-chain** *name-of-chain*
10. **ip rip authentication mode** {**text** | **md5**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**router rip** **例：** `Router(config)# router rip`	ルータ コンフィギュレーション モードを開始します。
ステップ 4	**version** {**1**	**2**} **例：** `Router(config-router)# version 1`	RIP Version 1 パケットのみを送信するようにインターフェイスを設定します。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了して、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。

	コマンドまたはアクション	目的
ステップ 6	**interface** *type number* **例：** `Router(config)# interface gigabitEthernet 0/0/0`	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 7	**ip rip send version** [**1**] [**2**] **例：** `Router(config-if)# ip rip send version 1`	RIP Version 1 パケットのみを送信するようにインターフェイスを設定します。
ステップ 8	**ip rip receive version** [**1**] [**2**] **例：** `Router(config-if)# ip rip receive version 1`	RIP Version 1 パケットのみを受け入れるようにインターフェイスを設定します。
ステップ 9	**ip rip authentication key-chain** *name-of-chain* **例：** `Router(config-if)# ip rip authentication key-chain chainname`	RIP 認証をイネーブルにします。
ステップ 10	**ip rip authentication mode** {**text** | **md5**} **例：** `Router(config-if)# ip rip authentication mode md5`	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（設定しないと、デフォルトでプレーン テキスト認証が使用されます）。
ステップ 11	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP ルートの集約

RIP Version 2 は、デフォルトで自動ルート集約をサポートしています。クラスフル ネットワーク境界を越えるとき、サブプレフィクスはクラスフル ネットワーク境界に集約されます。

サブネットの接続を解除した場合、自動ルート集約をディセーブルにして、そのサブネットをアドバタイズします。ルート集約がディセーブルになると、クラスフル ネットワーク境界間でサブネットとホスト ルーティング情報が送信されます。自動集約をディセーブルにするには、ルータ コンフィギュレーション モードで **no auto-summary** コマンドを使用します。

制約事項

スーパーネット アドバタイズメント（クラスフル メジャー ネットワーク未満の任意のネットワーク プレフィクスのアドバタイズ）は、ルーティング テーブルで認識されたスーパーネットのアドバタイズ以外、RIP ルート集約では許可されていません。設定に従って任意のインターフェイスで認識されるスーパーネットは、この場合も認識されます。

たとえば、次のスーパーネット集約は無効です。

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# ip summary-address rip 10.0.0.0 252.0.0.0
```

.
.
.

サブネット マスクが固有でも、インターフェイス上の各ルート集約には固有のメジャー ネットワークが必要です。たとえば、次の設定は許可されていません。

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip summary-address rip** *ip-address network-mask*
5. **exit**
6. **rip router**
7. **no auto-summary**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface** *type number* **例：** `Router(config)# interface gigabitEthernet 0/0/0`	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 4	**ip summary-address rip** *ip-address network-mask* **例：** `Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0`	集約するルートを識別する IP アドレスとネットワーク マスクを指定します。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**router rip** **例：** `Router(config)# router rip`	ルータ コンフィギュレーション モードを開始します。
ステップ 7	**no auto-summary** **例：** `Router(config-router)# no auto-summary`	ルータ コンフィギュレーション モードで、自動集約をディセーブルにします。
ステップ 8	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

スプリット ホライズンのイネーブル化とディセーブル化

この作業を実行して、スプリット ホライズンをイネーブルまたはディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip split-horizon**
   または
   no ip split-horizon
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface** *type number* **例：** `Router(config)# interface serial 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 4	**ip split-horizon** または **no ip split-horizon** **例：** `Router(config-if)# ip split-horizon`	スプリット ホライズンをイネーブルまたはディセーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

送信元 IP アドレスの確認のディセーブル化

この作業を実行して、着信ルーティング アップデートの送信元 IP アドレスを確認するデフォルト機能をディセーブルにします。

制約事項

フレーム リレーと SMDS のカプセル化の場合、スプリット ホライズンはデフォルトでディセーブルです。任意の X.25 カプセル化を使用するインターフェイスの場合、デフォルトでスプリット ホライズンはディセーブルではありません。その他のカプセル化の場合、デフォルトでスプリット ホライズンはイネーブルです。

（注） 一般的に、ルートを適切にアドバタイズするには変更が必要だと確信がない限り、デフォルトの状態を変更することは推奨されません。シリアル インターフェイスでスプリット ホライズンがディセーブルで、そのインターフェイスがパケット通信網に接続されている場合、そのネットワークの関連マルチキャスト グループ内にあるすべてのルータに対してスプリット ホライズンをディセーブルにする必要があることに注意してください。

（注） スプリット ホライズンがイネーブルの場合、集約されたネットワークはアドバタイズされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip split-horizon**
5. **exit**
6. **router rip**
7. **no validate-update-source**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface** *type number* **例：** `Router(config)# interface serial 0/0/0`	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 4	**ip split-horizon** **例：** `Router(config-if)# ip split-horizon`	スプリット ホライズンをイネーブルにします。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**router rip** **例：** `Router(config)# router rip`	ルータ コンフィギュレーション モードを開始します。
ステップ 7	**no validate-update-source** **例：** `Router(config-router)# no validate-update-source`	着信 RIP ルーティング アップデートの送信元 IP アドレスの確認をディセーブルにします。
ステップ 8	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

パケット間遅延の設定

この作業を実行して、パケット間遅延を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **exit**
5. **router rip**
6. **output-delay** *milliseconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface** *type number* **例：** `Router(config)# interface gigabitEthernet 0/0/0`	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 4	`exit`
	
	例：
	`Router(config-if)# exit`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**router rip** **例：** `Router(config-if)# router rip`	ルータ コンフィギュレーション モードを開始します。
ステップ 6	**output-delay** *milliseconds* **例：** `Router(config-router)# output-delay 8`	発信 RIP アップデートのパケット間遅延を設定します。
ステップ 7	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

WAN 上の RIP の最適化

RIP が最適化されていない場合、2 つの問題があります。

- 一般的に、RIP による定期的なブロードキャストによって、WAN 回路が閉じられなくなります。
- 固定のポイント間リンクでも、30 秒ごとに回線で渡される情報量なので、定期的な RIP 転送のオーバーヘッドによって通常のデータ転送が重度に妨害される可能性があります。

このような制約事項に対処するには、RIP のトリガー拡張機能によって、ルーティング データベースに更新があった場合にのみ、WAN 上で情報を送信するようにします。この機能をイネーブルにしたインターフェイスでは、定期的な更新パケットは抑制されます。ポイント間のシリアル インターフェイスでは、RIP ルーティング トラフィックが減ります。そのため、使用に関して課金されるオンデマンド回路ではコストを節約できます。RIP のトリガー拡張機能は、RFC 2091『*Triggered Extensions to RIP to Support Demand Circuits*』の一部をサポートしています。

この作業を実行して、RIP のトリガー拡張機能をイネーブルにし、RIP プライベート データベースの内容を表示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type** *controller-number*
4. **ip rip triggered**
5. **end**
6. **show ip rip database** [*prefix mask*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface pos** *controller-number* **例：** `Router(config)# interface serial 2/0/0`	シリアル インターフェイスを設定します。
ステップ 4	**ip rip triggered** **例：** `Router(config-if)# ip rip triggered`	RIP のトリガー拡張機能をイネーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip rip database** [*prefix mask*] **例：** `Router# show ip rip database`	RIP プライベート データベースの内容を表示します。

フレーム リレー ネットワークから接続されるルータの IP-RIP Delay Start の設定

この項の作業では、フレーム リレー インターフェイスで IP-RIP Delay Start 機能を使用するようにルータを設定する方法について説明します。

- 「RIPv2 の設定」（P.18）（必須）
- 「シリアル サブインターフェイスでのフレーム リレーの設定」（P.20）（必須）
- 「フレーム リレー サブインターフェイスでの IP、RIPv2 用 MD5 認証、および IP-RIP Delay Start 機能の設定」（P.21）（必須）

多くの場合、IP-RIP Delay Start 機能は、MD5 認証を使用してフレーム リレー ネットワーク上でシスコ製以外のデバイスと RIPv2 ネイバー関係を確立するように Cisco ルータが設定されている場合に使用されます。フレーム リレー上で RIPv2 ネイバーに接続したとき、基礎となるフレーム リレー回路でデータを送受信する準備が整っていない場合でも、フレーム リレー ネットワークに接続されているシリアル インターフェイスが実行されている可能性があります。シリアル インターフェイスが実行中で、フレーム リレー回路がまだ機能していない場合、シリアル インターフェイスでルータが送信しようとした MD5 パケットはドロップされます。パケットの送信に必要なフレーム リレー回路がまだ機能していないために、MD5 パケットがドロップされると、フレーム リレー回路がアクティブになった後にネイバー ルータが受信する最初の MD5 パケットのシーケンス番号は、0 よりも大きくなります。一部の非シスコ製ルータでは、他のルータから受信する最初の MD5 パケットのシーケンス番号が 0 を超える場合、MD5 で認証された RIPv2 ネイバー セッションの開始を許可しません。

RIPv2 に関する MD5 認証の実装方法がベンダーによって異なるのは、おそらくパケット損失に関連する RFC（RFC 2082）があいまいなためです。RFC 2082 では、0 のシーケンス番号、または最後に受信したシーケンス番号よりも大きいシーケンス番号を受け入れる準備をする必要があると提案しています。RIPv2 の MD5 メッセージ受信の詳細については、http://www.ietf.org/rfc/rfc2082.txt の RFC 2082 の 3.2.2 を参照してください。

（注） IP-RIP Delay Start 機能は、ファスト イーサネットやギガビット イーサネットなで、他のインターフェイス タイプでサポートされます。

（注） IP-RIP Delay Start 機能が必要なのは、シスコ製以外のデバイスとの RIPv2 ネイバー関係を確立するように Cisco ルータが設定され、MD5 ネイバー認証を使用する場合のみです。

ワンポイント アドバイス Cisco ルータでは、他のルータから受信する最初の MD5 パケットのシーケンス番号が 0 を超える場合、MD5 で認証された RIPv2 ネイバー セッションの開始を許可します。ネットワーク内で Cisco ルータのみを使用する場合、IP-RIP Delay Start 機能を使用する必要はありません。

前提条件

ルータは Cisco IOS XE Release 2.6 を実行する必要があります。

RIPv2 の設定

この必須の作業を実行して、ルータで RIPv2 を設定します。

（注） この作業手順は、お使いのルータで RIPv2 を設定する際に利用できる多くの手順の一例です。

手順の概要

1. **enable**
2. **configure terminal**
3. **router rip**
4. **network** *ip-network*
5. **version** {**1** | **2**}
6. [**no**] **auto-summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**router rip** **例：** `Router(config)# router rip`	RIP ルーティング プロセスをイネーブルにして、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	**network** *ip-network* **例：** `Router(config-router)# network 192.168.0.0`	ネットワークを RIP ルーティング プロセスと関連付けます。
ステップ 5	**version** {**1**	**2**} **例：** `Router(config-router)# version 2`	RIP Version 1 パケットのみまたは RIP Version 2 パケットのみを送受信するように、ソフトウェアを設定します。
ステップ 6	[**no**] **auto-summary** **例：** `Router(config-router)# no auto-summary`	サブネット ルートをネットワーク レベル ルートに自動集約するデフォルトの動作をディセーブルまたは復元します。

シリアル サブインターフェイスでのフレーム リレーの設定

この必須の作業を実行して、フレーム リレーのシリアル サブインターフェイスを設定します。

（注） この作業手順は、サブインターフェイスでフレーム リレーを設定する際に利用できる多くの手順の一例です。フレーム リレーの設定の詳細と手順については、『*Cisco IOS XE Wide-Area Networking Configuration Guide*』の「Configuring Frame Relay」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **encapsulation frame-relay** [**mfr** ***number*** **| ietf]**
6. **frame-relay lmi-type** {**cisco** | **ansi** | **q933a**}
7. **exit**
8. **interface** *type slot*/subslot/*port* {**point-to-point** | **multipoint**}
9. **frame-relay interface-dlci** *dlci* [**ietf** | **cisco**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**interface** *type slot/sublslot/port* **例：** `Router (config)# interface serial 2/0/0`	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 4	**no ip address** **例：** `Router (config-if)# no ip address`	以前に設定した IP アドレスをインターフェイスから削除します。
ステップ 5	**encapsulation frame-relay** [**mfr** *number*	**ietf**] **例：** `Router(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレーム リレー カプセル化のタイプを指定します。

	コマンドまたはアクション	目的
ステップ 6	**frame-relay lmi-type** {**cisco** | **ansi** | **q933a**} **例：** `Router(config-if)# frame-relay lmi-type ansi`	そのインターフェイスのフレーム リレー Local Management Interface（LMI; ローカル管理インターフェイス）のタイプを指定します。
ステップ 7	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**interface** *type slot/subslot/port* {**point-to-point** | **multipoint**} **例：** `Router(config)# interface serial 2/0/0 point-to-point`	サブインターフェイスとサブインターフェイスの接続タイプを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**frame-relay interface-dlci** *dlci* [**ietf** | **cisco**] **例：** `Router(config-subif)# frame-relay interface-dlci 100 ietf`	Data-Link Connection Identifier（DLCI; データリンク接続 ID）をフレーム リレー サブインターフェイスに割り当てます。

フレーム リレー サブインターフェイスでの IP、RIPv2 用 MD5 認証、および IP-RIP Delay Start 機能の設定

この必須の作業を実行して、フレーム リレー サブインターフェイスで IP、RIPv2 用 MD5 認証、および IP-RIP Delay Start 機能を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *number*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type slot*/subslot/*port*
9. **no cdp enable**
10. **ip address** *ip-address subnet-mask*
11. **ip rip authentication mode** {**text** | **md5**}
12. **ip rip authentication key-chain** *name-of-chain*
13. **ip rip initial-delay** *delay*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**key chain** *name-of-chain* **例：** `Router(config)# key chain rip-md5`	キー チェーンの名前を指定し、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	**key** *number* **例：** `Router(config-keychain)# key 123456`	キー ID を指定し、キー チェーン キー コンフィギュレーション モードを開始します。範囲は 0 ～ 2147483647 です。
ステップ 5	**key-string** *string* **例：** `Router(config-keychain-key)# key-string abcde`	キー ストリングを設定します。
ステップ 6	**exit** **例：** `Router(config-keychain-key)# exit`	キー チェーン キー コンフィギュレーション モードを終了します。
ステップ 7	**exit** **例：** `Router(config-keychain)# exit`	キー チェーン コンフィギュレーション モードを終了します。
ステップ 8	**interface** *type slot/subslot/port* **例：** `Router(config)# interface serial 2/0/0`	インターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**no cdp enable** **例：** `Router(config-subif)# no cdp enable`	インターフェイスで Cisco Discovery Protocol（CDP）オプションをディセーブルにします。 **（注）** シスコ製以外のデバイスでは CDP はサポートされません。また、IP-RIP Delay Start 機能が必要なのは、シスコ製以外のルータに接続する場合のみです。そのため、IP-RIP Delay Start 機能を設定するインターフェイスでは、CDP をディセーブルにする必要があります。

	コマンドまたはアクション	目的
ステップ 10	**ip address** *ip-address subnet-mask* **例：** `Router (config-subif)# ip address 172.16.10.1 255.255.255.0`	フレーム リレー サブインターフェイスの IP アドレスを設定します。
ステップ 11	**ip rip authentication mode** {**text** | **md5**} **例：** `Router(config-subif)# ip rip authentication mode md5`	RIPv2 認証のモードを指定します。
ステップ 12	**ip rip authentication key-chain** *name-of-chain* **例：** `Router (config-subif)# ip rip authentication key-chain rip-md5`	RIPv2 MD5 認証用に以前に設定したキー チェーンを指定します。
ステップ 13	**ip rip initial-delay** *delay* **例：** `Router(config-subif)# ip rip initial-delay 45`	インターフェイスで IP-RIP Delay Start 機能を設定します。ルータは、*delay* 引数に指定された秒数、RIPv2 ネイバーに対する最初の MD5 認証パケットの送信を遅延します。範囲は 0 ～ 1800 です。
ステップ 14	**end** **例：** `Router(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP の設定例

ここでは、次の設定例について説明します。

ルート集約の設定：例

ここでは、ルート集約の正しい設定例と誤った設定例を紹介します。

例 1：正しい設定

次に、グローバル コンフィギュレーション モードで、**ip summary-address rip** ルータ コンフィギュレーション コマンドが RIP の自動サマリー アドレス指定と連動する例を示します。この例で、メジャー ネットワークは 10.0.0.0 です。サマリー アドレス 10.2.0.0 は 10.0.0.0 という自動サマリー アドレスよりも優先されるため、イーサネット インターフェイス 1 では 10.2.0.0 がアドバタイズされ、10.0.0.0 はアドバタイズされません。

（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 アドレスもインターフェイス サマリー アドレス（**ip summary-address rip** インターフェイス コンフィギュレーション コマンドで設定されたアドレス）もアドバタイズされません。

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# exit
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)# no ip split-horizon
Router(config-if)# end
```

例 2：誤った設定

次に、集約対象の両方のアドレスが同じメジャー ネットワークのため、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドの使用に誤りがある例を示します。アドレスに固有のアドレス マスクがあるかどうかにかかわらず、1 つのインターフェイスの各ルート集約には固有のメジャー ネットワークが必要です。

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config-if)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```

スプリット ホライズンの設定：例

ここでは、スプリット ホライズンの設定例を 2 つ示します。

例 1

次の設定では、シリアル リンクでスプリット ホライズンをディセーブルにする単純な例を示します。この例では、シリアル リンクは X.25 ネットワークに接続します。

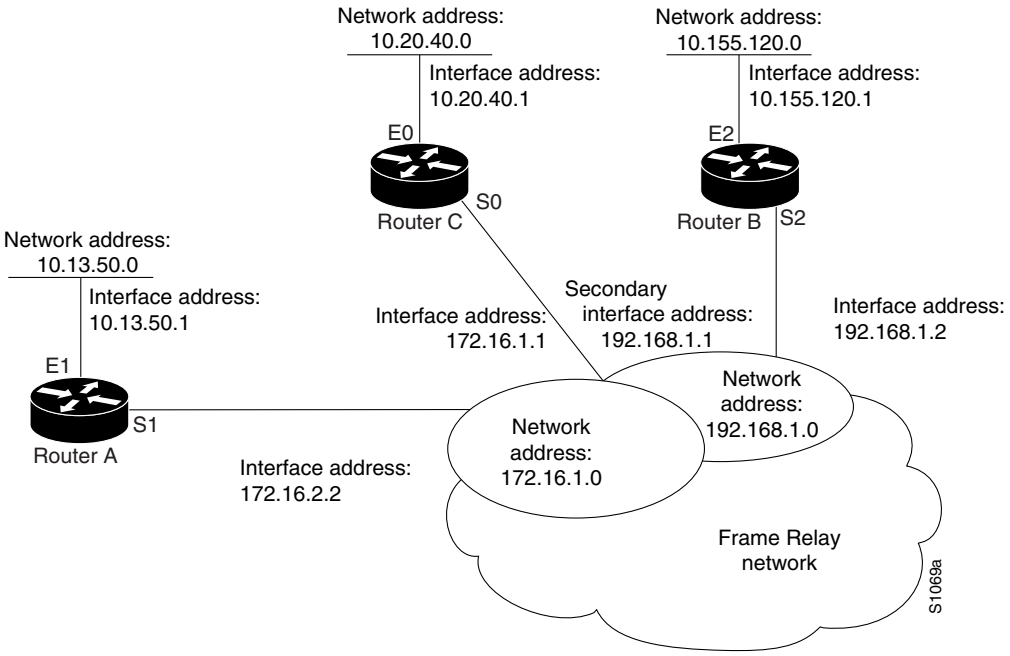
```
Router(config)# interface Serial 0/0/0
Router(config-if)# no ip split-horizon
```

例 2

次の例の図 1 では、**no ip split-horizon** インターフェイス コンフィギュレーション コマンドが有効な一般的な状況を示します。この図は、（フレーム リレー ネットワークに接続している）ルータ C 上のシリアル インターフェイス経由でアクセスできる 2 つの IP サブネットを示してします。この例では、ルータ C 上のシリアル インターフェイスは、セカンダリ IP アドレスの割り当てによってサブネットの 1 つに対応します。

ルータ A、ルータ B、およびルータ C（それぞれ IP ネットワーク 10.13.50.0、10.155.120.0、および 10.20.40.0 に接続）のギガビット イーサネット インターフェイスは、いずれもスプリット ホライズンがデフォルトでイネーブルです。一方、ネットワーク 172.16.1.0 および 192.168.1.0 に接続するシリアル インターフェイスは、いずれも **no ip split-horizon** コマンドでスプリット ホライズンがディセーブルにされています。図 1 にトポロジとインターフェイスを示します。

図 1　フレーム リレー ネットワークでディセーブルにされたスプリット ホライズンの例



この例では、すべてのシリアル インターフェイスでスプリット ホライズンがディセーブルです。ネットワーク 172.16.0.0 をネットワーク 192.168.0.0 に、またはその逆方向にアドバタイズするには、ルータ C でスプリット ホライズンをディセーブルにする必要があります。これらのサブネットは、ルータ C、インターフェイス S0 で重複しています。シリアル インターフェイス S0 でスプリット ホライズンがイネーブルだった場合、これらのネットワークのいずれについても、フレーム リレー ネットワークにルートはアドバタイズされません。

ルータ A の設定

```
interface gigabitethernet 0/0/0
 ip address 10.13.50.1
!
interface serial 0/0/0
 ip address 172.16.2.2
 encapsulation frame-relay
 no ip split-horizon
```

ルータ B の設定

```
interface gigabitethernet 0/0/0
 ip address 10.155.120.1
!
interface serial 0/0/0
 ip address 192.168.1.2
 encapsulation frame-relay
 no ip split-horizon
```

ルータ C の設定

```
interface gigabitethernet 0/0/0
 ip address 10.20.40.1
!
interface serial serial 0/0/0
 ip address 172.16.1.1
 ip address 192.168.1.1 secondary
 encapsulation frame-relay
```

```
 no ip split-horizon
```

アドレス ファミリ タイマーの設定：例

次に、個々のアドレス ファミリ タイマーを調整する例を示します。アドレス ファミリ「notusingtimers」では、汎用的な RIP 設定で 5、10、15、および 20 のタイマー値が使用されている場合でも、30、180、180、および 240 のシステム デフォルトが使用されます。アドレス ファミリ タイマーは、汎用の RIP 設定から継承されません。

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# timers basic 5 10 15 20
Router(config-router)# redistribute connected
Router(config-router)# network 5.0.0.0
Router(config-router)# default-metric 10
Router(config-router)# no auto-summary
Router(config-router)#
Router(config-router)# address-family ipv4 vrf abc
Router(config-router-af)# timers basic 10 20 20 20
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# default-metric 5
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#
Router(config-router)# address-family ipv4 vrf xyz
Router(config-router-af)# timers basic 20 40 60 80
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#
Router(config-router)# address-family ipv4 vrf notusingtimers
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#
```

フレーム リレー インターフェイスでの IP-RIP Delay Start の設定：例

次に、お使いのルータで IP-RIP Delay Start 機能を設定するために必要な最小限のコマンド例を示します。

```
!
key chain rip-md5
 key 123456
  key-string abcde
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

```
!
interface Serial 0/0/0
 no ip address
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
!
interface Serial 2/0/0 point-to-point
 ip address 172.16.10.1 255.255.255.0
 ip rip initial-delay 45
 ip rip authentication mode md5
 ip rip authentication key-chain rip-md5
 frame-relay interface-dlci 100
!
```

その他の関連資料

ここでは、Routing Information Protocol の設定に関連する資料を紹介します。

関連マニュアル

内容	参照先
プロトコルから独立した機能、RIP 情報のフィルタリング、キー管理（RIP Version 2 で使用可能）、および VLSM	『*Configuring IP Routing Protocol-Independent Features*』
RIP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Routing: RIP Command Reference*』
フレーム リレーの設定	『*Cisco IOS XE Wide-Area Networking Configuration Guide*』

標準

標準	タイトル
なし	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1058	『*Routing Information Protocol*』
RFC 2082	『*RIP-2 MD5 Authentication*』
RFC 2091	『*Triggered Extensions to RIP to Support Demand Circuits*』
RFC 2453	『*RIP version 2*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RIP の設定に関する機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　Routing Information Protocol の設定に関する機能情報

機能名	リリース	機能情報
IP-RIP Delay Start	Cisco IOS XE Release 2.6	IP-RIP Delay Start 機能は、ネイバー ルータ間のネットワーク接続が完全に機能するまで、RIPv2 ネイバー セッションの開始を遅延させるために Cisco ルータで使用されます。その結果、ルータがシスコ製以外のネイバー ルータに送信する最初の MD5 パケットのシーケンス番号は常に 0 です。MD5 認証を使用してネイバー ルータとの RIPv2 ネイバー セッションを確立するように設定されたルータのデフォルト動作では、物理インターフェイスの起動時に、MD5 パケットの送信を開始します。 この機能に関する詳細については、次の各項を参照してください。 • 「ネイバー ルータ認証」（P.6） • 「IP-RIP Delay Start」（P.7） 導入または変更されたコマンド：**ip rip initial-delay** *delay*
RIPv2 用の IP サマリー アドレス	Cisco IOS XE Release 2.1	RIPv2 用の IP サマリー アドレス機能によって、ルートを集約する機能が導入されました。RIP Version 2 のルートを集約すると、大規模なネットワークのスケーラビリティと効率が改善されます。IP アドレスの集約とは、RIP ルーティング テーブルに子ルート（サマリー アドレスに含まれる個々の IP アドレスの任意の組み合わせに対して作成されるルート）のエントリがないことを意味します。そのため、テーブルのサイズが削減され、ルータが処理できるルート数が増えます。 この機能に関する詳細については、次の各項を参照してください。 • 「RIP のルート集約」（P.5） • 「RIP ルートの集約」（P.11） • 「ルート集約の設定：例」（P.23） この機能で導入または変更されたコマンド：**ip summary-address rip**

表 1　Routing Information Protocol の設定に関する機能情報（続き）

機能名	リリース	機能情報
Routing Information Protocol	Cisco IOS XE Release 2.1	Routing Information Protocol（RIP）は小規模から中規模の TCP/IP ネットワークで一般的に使用されるルーティング プロトコルです。また、距離ベクトル アルゴリズムを使用してルートを計算する安定したプロトコルです。
トリガー RIP	Cisco IOS XE Release 2.1	トリガー RIP は、費用のかかる回路ベースの WAN リンクでの継続的な RIP アップデートに対処するために導入されました。RIP のトリガー拡張機能によって、ルーティング データベースに更新があった場合にのみ、RIP は WAN 上で情報を送信します。この機能をイネーブルにしたインターフェイスでは、定期的な更新パケットは抑制されます。ポイント間のシリアル インターフェイスでは、RIP ルーティング トラフィックが減ります。 この機能に関する詳細については、次の各項を参照してください。 • 「WAN 上の RIP の最適化」（P.16） 導入または変更されたコマンド：**ip rip triggered**、**show ip rip database**

用語集

IS-IS : Intermediate System-to-Intermediate System。DECnet Phase V ルーティングに基づく OSI リンクステート階層型ルーティング プロトコルであり、ルータはこれを使用して、ネットワーク トポロジを決定するために、1 つのメトリックに基づいてルーティング情報を交換します。

RIP : Routing Information Protocol。RIP は、ローカル ネットワークおよびワイドエリア ネットワークで使用されるダイナミック ルーティング プロトコルです。

VRF : VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス。VRF は、IP ルーティング テーブル、取得された転送テーブル、その転送テーブルを使用する一連のインターフェイス、転送テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

アドレス ファミリ : ネットワーク アドレスの共通形式を共有するネットワーク プロトコルのグループ。アドレス ファミリは RFC 1700 で定義されています。

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視

このマニュアルでは、RFC 1724『*RIP Version 2 MIB Extensions*』の Cisco IOS XE での実装について説明します。RFC 1724 では、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して RIPv2 を監視できる Management Information Base（MIB; 管理情報ベース）を定義しています。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視に関する機能情報」（P.13）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視の前提条件

- ルータで RIPv2 が設定されている必要があります。
- SNMP Network Management Station（NMS; ネットワーク管理ステーション）に RFC 1724 RIPv2 MIB がインストールされている必要があります。
- SNMP NMS に次の MIB がインストールされている必要があります。RFC 1724 ではこの MIB からデータ タイプと Object Identifier（OID; オブジェクト ID）をインポートするためです。
  - SNMPv2-SMI
  - SNMPv2-TC
  - SNMPv2-CONF
  - RFC1213-MIB

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視の制約事項

この RIPv2 MIB の実装では、RIP Virtual Routing and Forwarding（VRF）インスタンスに関連するデータを追跡しません。RIP ルータ コンフィギュレーション モードの **network** コマンドで設定された IP アドレス空間で IP アドレスが割り当てられたインターフェイスのみが追跡されます。グローバル データは、メイン ルーティング テーブルの変更についてのみ追跡されます。

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視に関する情報

ここでは、RFC 1724 の一部として標準化された MIB オブジェクトに関する情報と、RFC 1724 MIB の利点について説明します。

- 「RIPv2 MIB」（P.2）
- 「RIPv2 MIB の利点」（P.5）

RIPv2 MIB

ここでは、RFC 1724 の定義によって追加された MIB オブジェクトについて説明します。RIPv2 MIB は次の管理対象オブジェクトから構成されます。

- グローバル カウンタ：ルートの変更やネイバーの変更を追跡するために使用されます。
- インターフェイス ステータス テーブル：インターフェイスに固有の統計情報を追跡するために使用されるオブジェクトを定義します。
- インターフェイス設定テーブル：インターフェイス設定の統計情報を追跡するために使用されるオブジェクトを定義します。
- ピア テーブル：ネイバー関係を監視するために定義します。このオブジェクトは、Cisco IOS XE ソフトウェアでは実装されません。

表 1、表 2、および表 3 に、RFC 1724 RIPv2 MIB 定義に提供されるオブジェクトを示します。RFC 1724 RIPv2 MIB に記述されている順序で、オブジェクトが書き込まれるテーブルごとに示してあります。グローバル カウンタのすべてのオブジェクトに関する統計情報は、**snmpwalk** または同様の SNMP ツールセット コマンドを NMS で使用して、rip2Globals Object Identifier（OID; オブジェクト ID）を照会することで取得できます。

表 1 に、RFC 1724 RIPv2 MIB グローバル カウンタ オブジェクトを示します。

表 1　　RFC 1724 RIPv2 MIB グローバル カウンタ オブジェクト

グローバル カウンタ	オブジェクト	説明
rip2Globals	rip2GlobalRouteChanges	RIP によって IP ルート データベースに加えられたルート変更の数。ルートが変更されると、数は増加します。
	rip2GlobalQueries	他のシステムからの RIP クエリーに送信される応答の数。別のシステムからのクエリーに対して RIP が応答すると、数は増加します。

RFC 1724 RIPv2 MIB インターフェイス テーブルのオブジェクトは、インターフェイスごとに情報を追跡します。rip2IfStatAddress オブジェクトを除く RFC 1724 RIPv2 MIB インターフェイス テーブルのすべてのオブジェクトは、RIP 内で新しく追跡されるデータを表します。これらのオブジェクトについて同等の **show** コマンドはありません。RIPv2 MIB インターフェイス テーブルのすべてのオブジェクトは読み取り専用です。

表 2 に、RFC 1724 RIPv2 MIB インターフェイス テーブル オブジェクトを示します。インターフェイス テーブルのすべてのオブジェクトの統計情報は、**snmpwalk** または同様の SNMP ツールセットを NMS で使用して、シーケンス名 Rip2IfStatEntry を照会することで取得できます。

表 2　RFC 1724 RIPv2 MIB インターフェイス テーブル オブジェクト

シーケンス名	オブジェクト	説明
Rip2IfStatEntry	rip2IfStatAddress	指定したサブネットでのこのシステムの IP アドレス。番号が指定されていないインターフェイスの場合は 0.0.0.N の値。この最下位の 24 ビット（N）は、ネットワークバイト順の IP インターフェイスの ifIndex です。
	rip2IfStatRcvBadPackets	RIP プロセスで受信され、何らかの理由でその後に廃棄された RIP 応答パケットの数。たとえば、バージョン 0 パケットまたは不明なコマンド タイプの場合です。
	rip2IfStatRcvBadRoutes	有効な RIP パケットに含まれ、何らかの理由で無視されたルートの数。この数は、次の場合に増加されます。 • アドレス ファミリ ID が AF_INET と同じではない場合。 • RIP v2 アップデートが受信され、クラス D 以上の場合。 • RIP v2 アップデートが受信され、アドレスが martian アドレスの場合。
	rip2IfStatSentUpdates	このインターフェイスで実際に送信された、トリガーされた RIP アップデートの数。この数には、新しい情報を含むフル アップデートは明示的に含まれません。
	rip2IfStatStatus	この値は常に 1 に設定されます。

RFC 1724 RIPv2 MIB インターフェイス設定テーブルのオブジェクトは、インターフェイスごとに情報を追跡します。Rip2IfConfAuthType オブジェクトを除き、RFC 1724 RIPv2 MIB インターフェイス設定テーブルのオブジェクトのデータは、**show ip protocol** コマンドでも収集できます。RIPv2 MIB インターフェイス テーブルのすべてのオブジェクトは読み取り専用です。

表 3 に、RIPv2 MIB インターフェイス設定テーブル オブジェクトを示します。設定テーブルのすべてのオブジェクトの統計情報は、**snmpwalk** または同様の SNMP ツールセットを NMS で使用して、シーケンス名 rip2IfConfEntry を照会することで取得できます。

表 3　　RFC 1724 RIPv2 MIB インターフェイス設定テーブル オブジェクト タイプ

シーケンス名	オブジェクト タイプ	説明
rip2IfConfEntry	rip2IfConfAddress	指定したサブネットでのこのシステムの IP アドレス。番号が指定されていないインターフェイスの場合は 0.0.0.N の値。この最下位の 24 ビット（N）は、ネットワークバイト順の IP インターフェイスの ifIndex です。
	rip2IfConfDomain	この値は常に "" と等価です。
	rip2IfConfAuthType	このインターフェイスで使用される認証のタイプ。
	rip2IfConfAuthKey	対応する rip2IfConfAuthType のインスタンスが認証以外の値を持つ場合に、認証キーとして使用される値。
	rip2IfConfSend	このインターフェイスで送信される RIP アップデートのバージョン。
	rip2IfConfReceive	このインターフェイスで受け入れられる RIP アップデートのバージョン。
	rip2IfConfDefaultMetric	この変数は、このインターフェイスで開始される RIP アップデートのデフォルト ルート エントリに使用されるメトリックを示します。
	rip2IfConfStatus	この値は常に 1 に設定されます。
	rip2IfConfSrcAddress	このシステムがこのインターフェイスで送信元アドレスとして使用する IP アドレス。番号が指定されたインターフェイスの場合、この値は rip2IfConfAddress と同じにする必要があります。番号が指定されていないインターフェイスでは、システム上のいずれかのインターフェイスの rip2IfConfAddress 値にする必要があります。

RIPv2 MIB の利点

ネットワーク管理者は RFC 1724 RIPv2 MIB 拡張を使用して、以前は RFC 1389 RIPv2 MIB でサポートされていなかった新しいグローバル カウンタおよびテーブル オブジェクトを追加することで、SNMP を使用して RIPv2 ルーティング プロトコルを監視できます。新しいグローバル カウンタおよびテーブル オブジェクトの目的は、ルートの変更とネイバーの放棄を迅速に行うことです。

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視をイネーブルにする方法

ここでは、次の作業について説明します。

- 「ルータでの SNMP 読み取り専用アクセスのイネーブル化」（P.6）（必須）
- 「RIPv2 のステータスの確認：ルータおよびネットワーク管理ステーションでの RFC1724 MIB 拡張」（P.7）（任意）

ルータでの SNMP 読み取り専用アクセスのイネーブル化

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視機能自体に必要なルータ設定作業はありません。RFC 1724 RIPv2 MIB のオブジェクトに対する SNMP 読み取り専用アクセスをイネーブルにするのは、ルータで SNMP サーバ読み取り専用コミュニティ ストリングを設定する場合です。

（注） ルータで SNMP サーバ読み取り専用コミュニティ ストリングを設定すると、そのルータで実行されている Cisco IOS XE のバージョンで使用できるすべての MIB の読み取り専用アクセスをサポートするオブジェクトに対して、SNMP の読み取り専用アクセスを付与することになります。

この作業を実行して、SNMP サーバ読み取り専用コミュニティ ストリングをルータで設定して、ルータ上の MIB オブジェクト（RFC 1724 RIPv2 MIB 拡張を含みます）に対する SNMP 読み取り専用アクセスをイネーブルにします。

SNMP コミュニティ ストリング

ルータは、複数の読み取り専用 SNMP コミュニティ ストリングを持つことができます。ルータで **snmp-server** コマンドの SNMP 読み取り専用コミュニティ ストリングを設定した場合、既存の SNMP **snmp-server** 読み取り専用コミュニティ ストリングは上書きされません。たとえば、**snmp-server community** *string1* **ro** および **snmp-server community** *string2* **ro** コマンドをルータで入力すると、ルータは *string1* および *string2* という 2 つの有効な読み取り専用コミュニティ ストリングを持ちます。これが目的の動作ではない場合、**no snmp-server community** *string* **ro** コマンドを使用して、既存の SNMP 読み取り専用コミュニティ ストリングを削除します。

ワンポイント アドバイス ルータで SNMP 読み取り専用コミュニティ ストリングが設定済みの場合、この作業を実行する必要はありません。ルータに Cisco IOS XE Release 2.1 以降のリリースをロードした後は、NMS で SNMP コマンドを使用して、ルータ上の RFC 1724 RIPv2 MIB を照会できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string1* **ro**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**snmp-server community** *string1* **ro** **例：** `Router(config)# snmp-server community T8vCx3 ro`	ルータで実行されている Cisco IOS XE ソフトウェアのバージョンに含まれる MIB のオブジェクトに対して、SNMP 読み取り専用アクセスをイネーブルにします。 **（注）** セキュリティのために、読み取り専用コミュニティ ストリングには標準のデフォルト値である *public* を使用しないでください。パスワードには、大文字、小文字、および数字を組み合わせて使用します。
ステップ 4	**end** **例：** `Router(config)# end`	コンフィギュレーション セッションを終了し、特権 EXEC モードに戻ります。

RIPv2 のステータスの確認：ルータおよびネットワーク管理ステーションでの RFC1724 MIB 拡張

このオプション作業を NMS で実行して、ルータおよび NMS で RFC 1724 RIPv2 MIB 拡張のステータスを確認します。

（注） この作業では、パブリック ドメインで使用できる NET-SNMP ツールセットを使用します。この説明の手順では、Linux 上で実行されている NMS のターミナル セッションを使用します。この作業を実行するときに、必要に応じて、NMS 上の SNMP ツールセットから SNMP コマンドを代用します。

前提条件

NMS に RFC 1724 MIB がインストールされている必要があります。

手順の概要

1. **snmpwalk -m all -v2c** *ip-address* **-c** *read-only-community-string* **rip2Globals**

手順の詳細

ステップ 1 **snmpwalk -m all -v2c** *ip-address* **-c** *read-only-community-string* **rip2Globals**

RFC 1724 RIPv2 MIB の **rip2Globals** オブジェクトについて **snmpwalk** コマンドを使用して、そのオブジェクトに関連するオブジェクトのデータを表示します。この手順では、RFC 1724 RIPv2 MIB のオブジェクトに関するクエリーを送信するように NMS が設定され、そのクエリーに対して応答するようにルータが設定されていることを確認します。

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2Globals

RIPv2-MIB::rip2GlobalRouteChanges.0 = Counter32: 5
RIPv2-MIB::rip2GlobalQueries.0 = Counter32: 1
$
```

RIPv2 を使用した SNMP による RIPv2 監視の設定例：RFC1724 MIB 拡張

ここでは、次の例について説明します。

- 「RIP インターフェイス ステータス テーブル オブジェクトの照会：例」（P.8）
- 「RIP インターフェイス設定テーブル オブジェクトの照会：例」（P.9）

RIP インターフェイス ステータス テーブル オブジェクトの照会：例

次に、**snmpwalk** コマンドを使用して、SNMP クエリーを送信し、RIP インターフェイス ステータス テーブルに含まれるすべてのオブジェクトのデータを取得する例を示します。

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 Rip2IfStatEntry

RIPv2-MIB::rip2IfStatAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfStatAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfStatAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfStatAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfStatAddress.172.17.2.1 = IpAddress: 172.17.2.1
RIPv2-MIB::rip2IfStatRcvBadPackets.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadPackets.172.16.1.1 = Counter32: 1654
RIPv2-MIB::rip2IfStatRcvBadPackets.172.16.2.1 = Counter32: 1652
RIPv2-MIB::rip2IfStatRcvBadPackets.172.17.1.1 = Counter32: 1648
RIPv2-MIB::rip2IfStatRcvBadPackets.172.17.2.1 = Counter32: 1649
RIPv2-MIB::rip2IfStatRcvBadRoutes.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.16.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.16.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.17.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatRcvBadRoutes.172.17.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.10.0.0.253 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.16.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.16.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.17.1.1 = Counter32: 0
RIPv2-MIB::rip2IfStatSentUpdates.172.17.2.1 = Counter32: 0
RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.2.1 = INTEGER: active(1)
```

次に、**snmpwalk** コマンドを使用して、SNMP クエリーを送信し、RIP インターフェイス ステータス テーブルに含まれるすべてのインターフェイスの rip2IfStatStatus オブジェクトのデータを取得する例を示します。

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfStatStatus

RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfStatStatus.172.17.2.1 = INTEGER: active(1)
$
```

次に、**snmpget** コマンドを使用して、SNMP クエリーを送信し、RIP インターフェイス ステータス テーブルに含まれる特定のインターフェイス IP アドレスの rip2IfStatStatus オブジェクトのデータを取得する例を示します。

```
$ snmpget -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfStatStatus.10.0.0.253

RIPv2-MIB::rip2IfStatStatus.10.0.0.253 = INTEGER: active(1)
$
```

RIP インターフェイス設定テーブル オブジェクトの照会：例

次に、**snmpwalk** コマンドを使用して、SNMP クエリーを送信し、RIP インターフェイス設定テーブルに含まれるすべてのオブジェクトのデータを取得する例を示します。

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfConfEntry

RIPv2-MIB::rip2IfConfAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfAddress.172.17.2.1 = IpAddress: 172.17.2.1
RIPv2-MIB::rip2IfConfDomain.10.0.0.253 = ""
RIPv2-MIB::rip2IfConfDomain.172.16.1.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.16.2.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.17.1.1 = ""
RIPv2-MIB::rip2IfConfDomain.172.17.2.1 = ""
RIPv2-MIB::rip2IfConfAuthType.10.0.0.253 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.16.1.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.16.2.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.17.1.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthType.172.17.2.1 = INTEGER: noAuthentication(1)
RIPv2-MIB::rip2IfConfAuthKey.10.0.0.253 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.16.1.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.16.2.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.17.1.1 = ""
RIPv2-MIB::rip2IfConfAuthKey.172.17.2.1 = ""
RIPv2-MIB::rip2IfConfSend.10.0.0.253 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.16.1.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.16.2.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.17.1.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfSend.172.17.2.1 = INTEGER: ripVersion2(4)
RIPv2-MIB::rip2IfConfReceive.10.0.0.253 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.16.1.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.16.2.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.17.1.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfReceive.172.17.2.1 = INTEGER: rip2(2)
RIPv2-MIB::rip2IfConfDefaultMetric.10.0.0.253 = INTEGER: 1
```

```
RIPv2-MIB::rip2IfConfDefaultMetric.172.16.1.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.16.2.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.17.1.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfDefaultMetric.172.17.2.1 = INTEGER: 1
RIPv2-MIB::rip2IfConfStatus.10.0.0.253 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.16.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.16.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.17.1.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfStatus.172.17.2.1 = INTEGER: active(1)
RIPv2-MIB::rip2IfConfSrcAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfSrcAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfSrcAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfSrcAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfSrcAddress.172.17.2.1 = IpAddress: 172.17.2.1
$
```

次に、**snmpwalk** コマンドを使用して、SNMP クエリーを送信し、RIP インターフェイス設定テーブルに含まれるすべてのインターフェイスの rip2IfConfAddress オブジェクトのデータを取得する例を示します。

```
$ snmpwalk -m all -v2c 10.0.0.253 -c T8vCx3 rip2IfConfAddress

RIPv2-MIB::rip2IfConfAddress.10.0.0.253 = IpAddress: 10.0.0.253
RIPv2-MIB::rip2IfConfAddress.172.16.1.1 = IpAddress: 172.16.1.1
RIPv2-MIB::rip2IfConfAddress.172.16.2.1 = IpAddress: 172.16.2.1
RIPv2-MIB::rip2IfConfAddress.172.17.1.1 = IpAddress: 172.17.1.1
RIPv2-MIB::rip2IfConfAddress.172.17.2.1 = IpAddress: 172.17.2.1
$
```

関連情報

SNMP および SNMP 操作の詳細については、『Cisco IOS XE Network Management Configuration Guide, Release 2』の「Configuring SNMP Support」の章を参照してください。

その他の関連資料

ここでは、RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視に関連する関連資料を紹介します。

関連マニュアル

内容	参照先
RIP コンフィギュレーション	「Configuring Routing Information Protocol」
RIP コマンド	『*Cisco IOS IP Routing: RIP Command Reference*』
SNMP の設定	「Configuring SNMP Authentication」
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
RIPv2 MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1724	『*RIP Version 2 MIB Extensions*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RFC 1724 MIB 拡張を使用した SNMP による RIPv2 監視に関する機能情報

表 4 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 4 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 4　RIPv2 に関する機能情報：RFC 1724 MIB 拡張

機能名	リリース	機能情報
RIPv2：RFC 1724 MIB 拡張	Cisco IOS XE Release 2.1	この機能によって、RFC 1724『*RIP Version 2 MIB Extensions*』の Cisco IOS XE の実装が導入されました。RFC 1724 では、SNMP を使用した RIPv2 の管理および制限された制御を可能にする MIB オブジェクトを定義しています。 Cisco IOS XE Release 2.1 では、この機能は Cisco ASR 1000 シリーズ ルータに導入されました。

用語集

OID：Object Identifier（オブジェクト ID）。オブジェクト ツリー内の管理対象オブジェクト。

SNMP：Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。ネットワーキング デバイスの監視および管理に使用されるプロトコル。

snmpwalk：MIB のブランチから統計情報を照会する SNMP コマンド。

snmpget：MIB 内の特定の OID から統計情報を照会する SNMP コマンド。
