ベーシック パフォーマンス ルーティングの設定

Performance Routing（PfR; パフォーマンス ルーティング）では、従来のルーティング テクノロジーに機能が追加され、Wide Area Networking（WAN）インフラストラクチャを介した 2 つのデバイス間のパスのパフォーマンスを追跡したり、そのパスの品質を確認したりしてアプリケーション トラフィックに最適な出力パスまたは入力パスを決定できるようになります。

Cisco パフォーマンス ルーティングは、アプリケーション パフォーマンスの要件を満たす最適なパスを選択する機能を追加することで、従来の IP ルーティング テクノロジーを補完します。パフォーマンス ルーティング テクノロジーの第 1 フェーズでは、エンタープライズ WAN 全体とインターネット接続のパフォーマンスがインテリジェントに最適化されます。このテクノロジーは進化し、エンドツーエンドのパフォーマンス認識ネットワークによってエンタープライズ ネットワーク全体でアプリケーション パフォーマンスの最適化が行われるようになります。

このマニュアルでは、パフォーマンス ルーティングを実装するのに必要な基本的な概念とタスクについて紹介します。概念の詳細については、「Understanding Performance Routing」モジュールを参照してください。詳細、設定タスクおよび例については、「Configured Advanced Performance Routing」モジュール、または「Cisco IOS Performance Routing Features Roadmap」の個々の機能を参照してください。

（注） PfR コンフィギュレーション モジュールでは、Cisco IOS Release 15.1(2)T で導入された PfR 構文が紹介されています。Cisco IOS Release 15.1(1)T 以前のリリース、または 12.2SR あるいは 12.2SX のイメージを実行している場合、Optimized Edge Routing に関するすべての資料については、「Cisco IOS Optimized Edge Routing Overview」モジュールを参照してください。

機能情報の検索

このモジュールに記載されている機能の一部が、ご使用のソフトウェア リリースでサポートされていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「ベーシック パフォーマンス ルーティングの設定に関する機能情報」（P.22）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

ベーシック パフォーマンス ルーティングの設定に関する情報

パフォーマンス ルーティングの概要

パフォーマンス ルーティング（PfR）はシスコの先進テクノロジーです。追加のサービスアビリティ パラメータを使用して従来のルーティング テクノロジーを補完して、最良の出力パスまたは入力パスを選択できます。PfR は、追加機能を使用して従来のルーティング テクノロジーを補完します。PfR は、到達可能性、遅延、コスト、ジッター、Mean Opinion Score（MOS; 平均オピニオン評点）などのパラメータに基づいて、出力または入力の WAN インターフェイスを選択できます。または、負荷、スループット、および金銭的コストなどのインターフェイス パラメータを使用することもできます。一般的に従来のルーティング（たとえば、EIGRP、OSPF、Routing Information Protocol version 2（RIPv2）、BGP など）では、最短または最小のコスト パスに基づいてループフリーのトポロジを作成することが重視されます。

PfR には、計測装置を使用する追加機能が備わっています。PfR は、インターフェイス統計、Cisco IP Service Level Agreement（SLA; サービス レベル契約）（アクティブ モニタリング）、および NetFlow（パッシブ モニタリング）を使用します。IP SLA または NetFlow に関する予備知識または経験は不要です。PfR は、手動設定なしでこれらのテクノロジーを自動的にイネーブルにします。

Cisco パフォーマンス ルーティングは、到達可能性、遅延、コスト、ジッター、平均オピニオン評点（MOS）などの、アプリケーション パフォーマンスに影響を与えるパラメータに基づいて、出力または入力の WAN パスを選択します。このテクノロジーでは、ロード バランシングを効率化したり、WAN をアップグレードせずにアプリケーション パフォーマンスを向上させたりすることによって、ネットワーク コストを削減できます。

PfR は、IP トラフィック フローを監視してから、トラフィック クラスのパフォーマンス、リンクの負荷分散、リンク帯域幅の金銭的コスト、およびトラフィック タイプに基づいてポリシーとルールを定義できる、統合型の Cisco IOS ソリューションです。PfR は、アクティブ モニタリング システム、パッシブ モニタリング システム、障害のダイナミック検出、およびパスの自動修正を実行できます。PfR を導入することによって、インテリジェントな負荷分散や、企業ネットワーク内での最適なルート選択が可能になります。

パフォーマンス ルーティングと Optimized Edge Routing

Cisco パフォーマンス ルーティングは、Cisco IOS ソフトウェアに組み込まれた多くの機能を使用し、ネットワークおよびアプリケーション ポリシーに基づいて最適なパスを決定します。Cisco パフォーマンス ルーティングは Cisco IOS Optimized Edge Routing（OER）テクノロジーが進化したものであり、さらに機能が強化されています。OER は元々、1 つの送信先プレフィクスごとにルート制御を提供するよう設計されましたが、パフォーマンス ルーティングでは、1 つのアプリケーションごとにインテリジェントなルート制御を行うよう機能が拡張されました。拡張された機能により、柔軟性が向上し、OER よりもアプリケーションの最適化を細かく行えるようになります。

Optimized Edge Routing からパフォーマンス ルーティングへの移行

以前の Cisco IOS リリースのイメージに実装されていた Optimized Edge Routing からパフォーマンス ルーティングに移行する場合は、移行パスを円滑にするために次の情報に留意してください。Cisco IOS Release 15.1(2)T では、OER 構文は引き続き認識されます。OER 構文を入力すると、構文はソフトウェアにより実行コンフィギュレーションで新しい PfR 構文に変更されます。実行コンフィギュレーションを保存すると、PfR バージョンの構文が保存されます。古い Cisco IOS イメージをリロードする必要がある場合は、OER バージョンの構文を使用するすべての設定スクリプトのバックアップ コピーを保存することを推奨します。新しい PfR 構文は古い Cisco IOS ソフトウェア イメージでは動作しません。

パフォーマンス ルーティング テクノロジーと従来のルーティング テクノロジー

PfR は、従来の IP ルーティングでは対応できなかったネットワーク パフォーマンスの問題を識別および制御するために開発されました。従来の IP ルーティングでは、各ピア デバイスはプレフィクス送信先への到達可能性のビューをメトリックへの到達に関連するコストの概念とともに伝達します。通常、プレフィクス送信者への最適なパス ルートは、コストが最も安いメトリックを使用して決定され、このルートはデバイスの Routing Information Base（RIB; ルーティング情報ベース）に入力されます。結果として、RIB に導入された任意のルートが、プレフィクス送信先に送信されるトラフィックを制御する最適なパスとして取り扱われます。コスト メトリックはスタティックに設計されたネットワークのビューを反映するように設定されます。たとえば、コスト メトリックはパスのユーザ設定または大

きい帯域幅のインターフェイス（インターフェイスのタイプから推測）の設定のいずれかを反映します。コスト メトリックは、ネットワークの状態またはネットワークを通過しているトラフィックのパフォーマンスの状態を反映しません。したがって、従来の IP ルーテッド ネットワークはネットワークの物理的な状態の変化（インターフェイスのダウンなど）に対応しますが、ネットワークでのパフォーマンスの変化（劣化または改善）には対応しません。場合によっては、トラフィックの劣化はルーティング デバイスのパフォーマンスの劣化やセッション接続の損失から推測できますが、これらのトラフィック劣化の症状は、トラフィックのパフォーマンスを直接測定することによって得られたものではなく、最適なパス ルーティングの決定で考慮すべきではありません。

ネットワーク内にあるトラフィックのパフォーマンスの問題を解決するために、PfR はトラフィック クラスを管理します。トラフィック クラスはネットワーク上のトラフィックのサブセットとして定義され、サブセットはアプリケーションなどに関連するトラフィックを表すことができます。各トラフィック クラスのパフォーマンスは、設定されたメトリックまたは PfR ポリシーで定義されたデフォルトのメトリックに対して測定および比較されます。PfR はトラフィック クラス パフォーマンスを監視し、トラフィック クラスの最適な入口または出口を選択します。後続のトラフィック クラス パフォーマンスがポリシーに準拠しないと、PfR はトラフィック クラスの別の入口または出口を選択します。

ベーシック パフォーマンス ルーティングの導入

PfR は、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）の設定を使用して Cisco ルータで設定します。パフォーマンス ルーティングは Master Controller（MC; マスター コントローラ）と Border Router（BR; ボーダー ルータ）の 2 つのコンポーネントから構成されます。PfR の導入では、1 つの MC と 1 つまたは複数の BR が必要です。MC と BR 間の通信はキー チェーン認証によって保護されます。パフォーマンス ルーティングの導入シナリオとスケーリングの要件に応じて、MC は専用ルータに導入したり、同じ物理ルータで BR とともに導入したりできます。

PfR 管理のネットワークには、送信トラフィックを伝達できるインターフェイスと外部インターフェイスとして設定できるインターフェイスの少なくとも 2 つの出力インターフェイスが必要です。これらのインターフェイスはネットワーク エッジで ISP または WAN リンク（フレームリレー、ATM）と接続されている必要があります。また、ルータには、パッシブ モニタリングのために内部インターフェイスとして設定できる 1 つのインターフェイス（内部ネットワークから到達可能）が必要です。PfR を導入するには、外部インターフェイス、内部インターフェイス、およびローカル インターフェイスの 3 つのインターフェイス設定が必要です。

PfR ボーダー ルータ

BR コンポーネントは、ISP または他の参加ネットワークへの 1 つまたは複数の出口リンクがあるエッジ ルータのデータ プレーン内に存在します。BR は NetFlow を使用してスループットと TCP パフォーマンス情報をパッシブに収集します。また、BR は、明示的なアプリケーション パフォーマンス モニタリングに使用されるすべての IP のサービス レベル契約（SLA）のプローブを行います。BR では、ネットワークのルーティングに対するすべてのポリシー決定と変更が行われます。BR は、プレフィクスおよび出口リンクの測定値をマスター コントローラに報告し、マスター コントローラから受け取ったポリシー変更を適用することにより、プレフィクス モニタリングとルート最適化に参加します。BR は、優先されるルートを挿入してネットワーク内でルーティングを変更することによりポリシー変更を適用します。BR プロセスは、マスター コントローラ プロセスと同じルータでイネーブルにすることができます。

PfR マスター コントローラ

MC は、パフォーマンス ルーティング システムの中央プロセッサおよびデータベースとして動作する単一ルータです。MC コンポーネントはフォワーディング プレーン内に存在せず、スタンドアロンで導入された場合は BR 内に含まれるルーティング情報のビューを持ちません。マスター コンポーネントは通信を保持し、BR とのセッションを認証します。MC の役割は、BR から情報を収集してトラフィック クラスがポリシーに準拠しているかどうかを決定し、ルート挿入またはダイナミック Policy-Based Routing（PBR; ポリシーベース ルーティング）挿入を使用してトラフィック クラスがポリシーに準拠する方法を BR に指示することです。

また、MC はレポート機能用の Application Programming Interface（API; アプリケーション プログラミング インターフェイス）も提供します。詳細については、「Performance Routing Application Interface」モジュールを参照してください。

PfR コンポーネント バージョン

MC と BR 間の API を変更する新しい PfR 機能が導入された場合、パフォーマンス ルーティング コンポーネント、マスター コントローラ、およびボーダー ルータのバージョン番号が増加します。マスター コントローラのバージョン番号はボーダー ルータのバージョン番号以上である必要があります。マスター コントローラとボーダー ルータのバージョン番号は **show pfr master** コマンドを使用して表示します。次の一部の出力では、MC バージョンが最初の段落に示され、BR バージョンがボーダー ルータの情報の最後のカラムに示されます。

```
Router# show pfr master

OER state: ENABLED and ACTIVE
 Conn Status: SUCCESS, PORT: 7777
  Version: 2.0
  Number of Border routers: 2
  Number of Exits: 2
.
.
.
Border           Status   UP/DOWN             AuthFail  Version
1.1.1.2          ACTIVE   UP       00:18:57          0  2.0
1.1.1.1          ACTIVE   UP       00:18:58          0  2.0
.
.
.
```

バージョン番号は、特定のリリース群の各 Cisco IOS ソフトウェア リリースでは更新されませんが、Cisco IOS ソフトウェア イメージがマスター コントローラとして設定されたデバイスとすべてのボーダー ルータで同じリリースである場合、バージョンには互換性があります。

PfR のキー チェーン認証

マスター コントローラとボーダー ルータ間の通信は、キー チェーン認証によって保護されます。認証キーは、通信を確立する前にマスター コントローラとボーダー ルータの両方で設定されている必要があります。キー チェーン設定は、マスター コントローラとボーダー ルータ間の通信に対するキー チェーン認証がイネーブルになる前に、マスター コントローラとボーダー ルータの両方でグローバル コンフィギュレーション モードで定義します。Cisco IOS ソフトウェアでのキー管理の詳細については、『*Cisco IOS IP Routing: Protocol Independent Configuration Guide*』の「Configuring IP Routing Protocol-Independent Features」の章の「Managing Authentication Keys」の項を参照してください。

PfR 管理のネットワーク インターフェイス

PfR 管理のネットワークには、送信トラフィックを伝達できるインターフェイスと外部インターフェイスとして設定できるインターフェイスの少なくとも 2 つの出力インターフェイスが必要です。これらのインターフェイスはネットワーク エッジで ISP または WAN リンク（フレームリレー、ATM）と接続されている必要があります。また、ルータには、パッシブ モニタリングのために内部インターフェイスとして設定できる 1 つのインターフェイス（内部ネットワークから到達可能）が必要です。PfR を導入するには、3 つのインターフェイス設定が必要です。

- *外部インターフェイス*はトラフィックを転送する、PfR により管理された出口リンクとして設定されます。物理的な外部インターフェイスはボーダー ルータでイネーブルになります。外部インターフェイスは、マスター コントローラで PfR 外部インターフェイスとして設定されます。マスター コントローラはこれらのインターフェイスのプレフィクスおよび出口リンク パフォーマンスをアクティブに監視します。各ボーダー ルータには少なくとも 1 つの外部インターフェイスが必要であり、PfR 管理のネットワークには少なくとも 2 つの外部インターフェイスが必要です。
- *内部インターフェイス*は、NetFlow によるパッシブ パフォーマンス モニタリングにだけ使用されます。明示的に NetFlow を設定する必要はありません。内部インターフェイスは内部ネットワークに接続するアクティブなボーダー ルータ インターフェイスです。内部インターフェイスは、マスター コントローラで PfR 内部インターフェイスとして設定されます。各ボーダー ルータでは、少なくとも 1 つの内部インターフェイスを設定する必要があります。
- *ローカル インターフェイス*は、マスター コントローラとボーダー ルータとの通信に対してだけ使用されます。各ボーダー ルータでは、単一インターフェイスをローカル インターフェイスとして設定する必要があります。ローカル インターフェイスは、マスター コントローラとの通信用のソース インターフェイスとして識別されます。

ヒント マスター コントローラおよびボーダー ルータ プロセスが同じルータでイネーブルな場合は、ループバック インターフェイスをローカル インターフェイスとして設定する必要があります。

次のインターフェイス タイプを外部インターフェイスおよび内部インターフェイスとして設定できます。

- ATM
- Basic Rate Interface（BRI）
- CTunnel
- ダイヤラ
- イーサネット
- ファスト イーサネット
- ギガビット イーサネット
- High-Speed Serial Interface（HSSI）
- ループバック（Cisco IOS 15.0(1)M 以降のリリースでサポート）
- マルチリンク
- Multilink Frame Relay（MFR）
- ヌル
- Packet-over-SONET（POS）
- ポート チャネル
- シリアル

- トンネル
- VLAN

次のインターフェイス タイプをローカル インターフェイスとして設定できます。

- 非同期
- Bridge Group Virtual Interface（BVI）
- Code Division Multiple Access Internet Exchange（CDMA-Ix）
- CTunnel
- ダイヤラ
- イーサネット
- グループ非同期
- ループバック
- マルチリンク
- Multilink Frame Relay（MFR）
- ヌル
- シリアル
- トンネル
- Virtual host interface（Vif）
- 仮想 PPP
- 仮想テンプレート
- 仮想トークンリング

（注） 仮想トークンリング インターフェイスはローカル インターフェイスとして設定できます。ただし、トークンリング インターフェイスはサポートされておらず、外部インターフェイス、内部インターフェイス、またはローカル インターフェイスとして設定できません。

（注） PfR では、イーサネット スイッチ インターフェイスなど、レイヤ 2 のみのイーサネット インターフェイスはサポートされません。

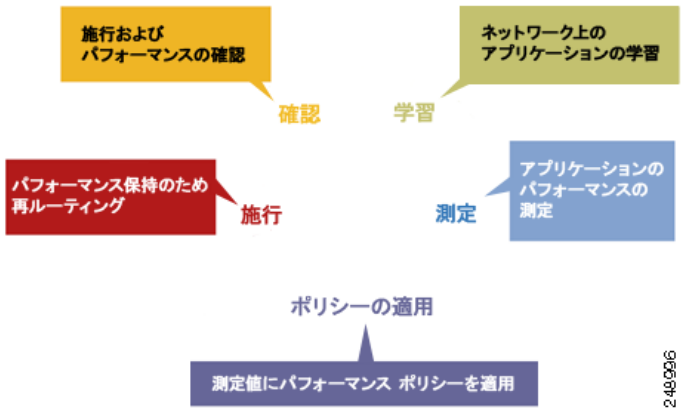
パフォーマンス ルーティング DMVPN mGre のサポート

- PfR はスプリット トンネリングをサポートしません。
- PfR はハブツースポーク リンクだけをサポートします。スポークツースポーク リンクはサポートされていません。
- PfR は、DMVPN Multipoint GRE（mGRE; マルチポイント GRE）導入でサポートされています。同じ宛先 IP アドレスに対して複数のネクスト ホップがあるマルチポイント インターフェイス導入（イーサネットなど）はサポートされていません。

PfR ネットワーク パフォーマンス ループ

従来の各ルーティング プロトコルでは、ルーティング トポロジを形成するためにデバイス間でフィードバック ループが作成されます。パフォーマンス ルーティング インフラストラクチャには、クライアント - サーバ メッセージング モードで通信されるパフォーマンス ルーティング プロトコルが含まれます。PfR で使用されるルーティング プロトコルは、マスター コントローラと呼ばれるネットワーク コントローラと、ボーダー ルータと呼ばれるパフォーマンスアウェアなデバイスとの間で実行されます。このパフォーマンス ルーティング プロトコルは、ネットワーク パフォーマンス ループを作成します。このネットワーク パフォーマンス ループでは、ネットワークが、最適化が必要なトラフィック クラスのプロファイリング、識別したトラフィック クラスのパフォーマンス メトリックの測定と監視、このトラフィック クラスへのポリシーの適用、および指定されたトラフィック クラスの最良のパフォーマンス パスに基づくルーティングを行います。図 1 に、5 つの PfR フェーズ（プロファイル作成、測定、ポリシー適用、施行、確認）を示します。

図 1　　PfR ネットワーク パフォーマンス ループ



ネットワークで PfR がどのように動作するのかを理解するには、次の 5 つの PfR フェーズを理解し、実行する必要があります。

- 「プロファイル フェーズ」（P.8）
- 「測定フェーズ」（P.9）
- 「ポリシー適用フェーズ」（P.9）
- 「施行フェーズ」（P.10）
- 「確認フェーズ」（P.10）

PfR パフォーマンス ループは、プロファイル フェーズから始まり、測定、ポリシー適用、制御、および確認の各フェーズが続きます。このフローは、確認フェーズ後にプロファイル フェーズに戻って続行し、プロセスを通じてトラフィック クラスおよびサイクルをアップデートします。

プロファイル フェーズ

中規模から大規模のネットワークでは、何十万台ものルータが Routing Information Base（RIB; ルーティング情報ベース）に存在し、デバイスがトラフィックのルーティングを試みています。パフォーマンス ルーティングは一部のトラフィックを優先させる手段なので、RIB 内の全ルートのサブセットを選択してパフォーマンス ルーティング用に最適化する必要があります。PfR は、自動学習または手動設定のいずれかの方法でトラフィックをプロファイリングします。

- 自動学習：デバイスは、デバイスを通過するフローを学習し、遅延またはスループットが最も高いフローを選択することによって、パフォーマンス ルーティング（最適化）の必要なトラフィックをプロファイリングします。
- 手動設定：学習に加えて、または学習の代わりに、トラフィック クラスにパフォーマンス ルートを設定します。

測定フェーズ

パフォーマンス ルーティングの必要なトラフィックのプロファイリングが終わると、PfR は、これらの個々のトラフィック クラスのパフォーマンス メトリックを測定します。パフォーマンス メトリックの測定には、パッシブ モニタリングとアクティブ モニタリングという 2 種類のメカニズムがあり、1 つまたは両方のメカニズムをネットワークに導入して次のタスクを実行できます。モニタリングとは、定期的な間隔で測定するアクションです。

パッシブ モニタリングとは、フローがデータ パス内のデバイスを通過するときにトラフィックのパフォーマンス メトリックを測定するアクションです。パッシブ モニタリングは NetFlow 機能を使用しますが、一部のトラフィック クラスのパフォーマンス メトリック測定には使用できません。一部のハードウェアまたはソフトウェアに関する制約もあります。

アクティブ モニタリングは、IP サービス レベル契約（SLA）を使用して合成トラフィックを生成し、監視対象のトラフィック クラスをエミュレートすることからなります。合成トラフィックは、実際のトラフィック クラスの代わりに測定されます。合成トラフィックのモニタリング結果は、合成トラフィックで表されるトラフィック クラスをパフォーマンス ルーティングするために適用されます。

トラフィック クラスには、パッシブ モニタリング モードとアクティブ モニタリング モードの両方を適用できます。パッシブ モニタリング フェーズは、PfR ポリシーに準拠しないトラフィック クラスのパフォーマンスを検出することがあります。次に、このトラフィック クラスにアクティブ モニタリングを適用して、代替パフォーマンス パスがある場合は、最良の代替パフォーマンス パスを検出できます。

NetFlow または IP SLA 設定のサポートは、自動的にイネーブルになります。

ポリシー適用フェーズ

最適化の対象となるトラフィック クラスのパフォーマンス メトリックを収集すると、PfR は、その結果と、ポリシーとして設定された各メトリックに設定された低しきい値および高しきい値のセットを比較します。メトリックでは、その結果としてポリシーが境界値を越えた場合は、Out-of-Policy（OOP; ポリシー違反）イベントになります。結果の比較は、相対ベース（実際の平均値からの偏差）、しきい値ベース（値の下限または上限）、または両方の組み合わせで行われます。

PfR で定義できるポリシーは、トラフィック クラス ポリシーとリンク ポリシーの 2 種類です。トラフィック クラス ポリシーは、プレフィクスまたはアプリケーションに対して定義されます。リンク ポリシーは、ネットワーク エッジの出口リンクまたは入口リンクに対して定義されます。どちらのタイプの PfR ポリシーも、OOP イベントを判断する基準を定義します。ポリシーは、すべてのトラフィック クラスに一連のポリシーが適用されるグローバル ベース、またはトラフィック クラスの選択された（フィルタリングされた）リストに一連のポリシーが適用されるより絞り込まれたベースで適用されます。

複数のポリシー、多数のパフォーマンス メトリック パラメータ、およびこれらのポリシーをトラフィック クラスに割り当てるさまざまな方法が存在するために、ポリシーの競合解決方法が作成されました。デフォルトの裁定方法では、各パフォーマンス メトリック変数および各ポリシーに指定されたデフォルトのプライオリティ レベルが使用されます。異なるプライオリティ レベルを設定して、すべてのポリシーまたは選択した一連のポリシーに対してデフォルトの裁定を上書きするように設定できます。

施行フェーズ

パフォーマンス ループの PfR 施工フェーズ（制御フェーズとも呼ばれます）では、ネットワークのパフォーマンスが向上するようにトラフィックが制御されます。トラフィックの制御に使用される方法は、トラフィックのクラスによって異なります。プレフィクスだけを使用して定義されるトラフィック クラスでは、従来のルーティングで使用されるプレフィクスの到達可能性情報が操作されることがあります。ボーダー ゲートウェイ プロトコル（BGP）または RIP などのプロトコルは、ルートやその適切なコスト メトリックを導入または削除することによってプレフィクスの到達可能性情報をアナウンスしたり、削除したりするために使用されます。

プレフィクスおよび追加のパケット一致基準が指定されているアプリケーションによって定義されるトラフィック クラスでは、PfR は従来のルーティング プロトコルを使用できません。これは、ルーティング プロトコルが、プレフィクスの到達可能性だけを伝達し、ネットワーク全体ではなくデバイス固有の制御となるためです。このようなデバイス固有の制御は、PfR でポリシーベース ルーティング（PBR）機能を使用して実行されます。このシナリオのトラフィックを他のデバイスにルーティングする必要がある場合、リモート ボーダー ルータはシングル ホップの位置にあるか、シングル ホップのように見えるトンネル インターフェイスである必要があります。

確認フェーズ

PfR 施行フェーズ中にトラフィック クラスが OOP の場合、PfR は制御を導入して、OOP トラフィック クラスのトラフィックに影響を及ぼします（最適化します）。スタティック ルートおよび BGP ルートは、PfR によってネットワークに導入される制御の例です。制御が導入されると、PfR は、最適化されたトラフィックがネットワーク エッジの優先出口リンクまたは優先入口リンクを経由していることを確認します。トラフィック クラスが OOP から変化しない場合、PfR は OOP トラフィック クラスのトラフィックの最適化に導入された制御をドロップし、ネットワーク パフォーマンス ループを繰り返します。

PfR とエンタープライズ ネットワーク

エンタープライズ ネットワークは、信頼性の確保と負荷分散を実現するために複数の Internet Service Provider（ISP; インターネット サービス プロバイダー）接続または WAN 接続を使用します。既存の信頼性メカニズムは、1 つのプレフィクスまたはプレフィクスのセットにとって最良の出口リンクを選択するためにボーダー ルータのリンク状態またはルート削除に依存します。接続が複数あると、エンタープライズ ネットワークを深刻な障害から守ることができますが、不安定な電力供給や、ネットワークの混雑のため発生する深刻でない障害からネットワークを守ることはできません。既存のメカニズムは障害の兆候が現れたときに深刻な障害に対応できます。ただし、停電や不安定な電力供給は検出されないことがあり、多くの場合、ネットワーク オペレータが問題を解決するためにアクションを起こす必要があります。パケットが外部ネットワーク間（国内または海外）で送信される場合、パケットはそのライフサイクルのほとんどの時間をネットワークの WAN セグメントで費やします。エンタープライズ ネットワークで WAN ルート選択を最適化すると、パフォーマンスが大幅に改善されます（ローカル ネットワークの LAN 速度の改善よりも効果的です）。

PfR 導入の説明に使用される例の多くはエッジ デバイスが通信するネットワークとして ISP を示していますが、他のソリューションも存在します。ネットワーク エッジはネットワーク内で論理的に区切るものとして定義できます。これには、同じ場所にあるデータ センター ネットワークなどのネットワークの別の部分や WAN 接続および ISP 接続などがあります。元のネットワーク エッジ デバイスに接続されたネットワークまたはネットワークの一部は、BGP を使用して通信する場合は個別の自律システム番号を持つ必要があります。

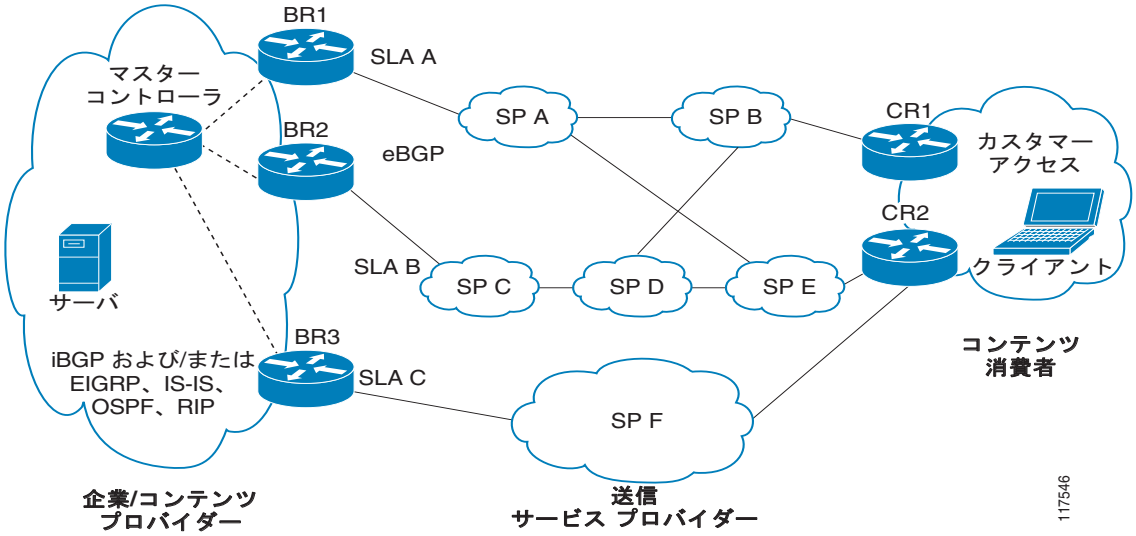
PfR は Cisco IOS ソフトウェアでシスコ コア ルーティング機能の統合された部分として実装されます。PfR を導入すると、インテリジェントなネットワーク トラフィック負荷分散とネットワーク エッジのデータ パスのダイナミック障害検出がイネーブルになります。他のルーティング メカニズムは負荷分

散と障害緩和の両方を提供できますが、応答時間、パケット損失、パス利用可能性、トラフィック負荷分散などの、スタティックなルーティング メトリック以外の基準に基づいてルーティング調整を行うことができるのは PfR だけです。PfR を導入すると、帯域幅コストを最小化し、稼動コストを削減しつつネットワーク パフォーマンスとリンク使用率を最適化できます。

PfR が導入される典型的なトポロジ

図 2 に、PfR 管理コンテンツ プロバイダーの典型的なエンタープライズ ネットワークを示します。エンタープライズ ネットワークは、カスタマー アクセス ネットワークにコンテンツを配信するために使用する 3 つの出口インターフェイスを持ちます。コンテンツ プロバイダーは、各出口リンクに対して異なる ISP と個別のサービス レベル契約（SLA）を結びます。カスタマー アクセス ネットワークは、インターネットに接続する 2 つのエッジ ルータを持ちます。トラフィックはエンタープライズ ネットワークとカスタマー アクセス ネットワークとの間を流れ、その間には 6 つの Service Provider（SP; サービス プロバイダー）が存在します。

図 2　　典型的な PfR 導入



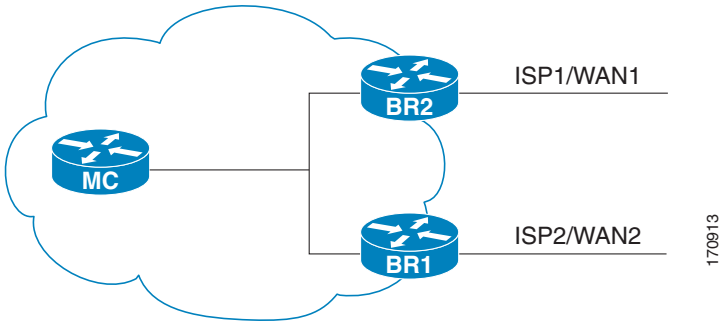
PfR は、3 つのボーダー ルータ（BR）で送信トラフィックを監視および制御します。PfR は、BR1、BR2、および BR3 の出力インターフェイスからパケット応答時間とパス利用可能性を測定します。ボーダー ルータでの出口リンク パフォーマンスの変更は、1 つのプレフィクスごとに検出されます。プレフィクスのパフォーマンスがデフォルトまたはユーザ定義のポリシー パラメータよりも下になると、パフォーマンスを最適化し、エンタープライズ ネットワークの外部で発生した障害状況を回避するためにルーティングがエンタープライズ ネットワークにおいてローカルで変更されます。たとえば、SP D ネットワークでのインターフェイスの障害やネットワークの設定ミスによって、BR2 出口インターフェイスを通過する送信トラフィックが混雑したり、カスタマー アクセス ネットワークに到達できなかったりすることがあります。従来のルーティング メカニズムでは、ネットワーク オペレータの介入なしにこのような問題を予測または解決することはできません。PfR は障害状況を検出し、ネットワーク内部のルーティングを自動的に変更して問題を回避できます。

ベーシック パフォーマンス ルーティングの設定方法

PfR マスター コントローラの設定

このタスクを実行して PfR マスター コントローラを設定し、PfR 管理のネットワークを管理します。このタスクは、PfR マスター コントローラとして指定されたルータで実行する必要があります。1 つのマスター ルータと 2 つのボーダー ルータのネットワーク設定例については、図 3 を参照してください。最初に、マスター コントローラとボーダー ルータとの間で通信が確立されます（マスター コントローラとボーダー ルータとの間の通信セッションを保護するためにキー チェーン認証が設定されます）。また、内部および外部ボーダー ルータ インターフェイスも指定されます。

図 3　　マスター コントローラとボーダー ルータの図



マスター コントローラをディセーブルにし、実行コンフィギュレーションからプロセス設定を完全に削除するには、グローバル コンフィギュレーション モードで **no pfr master** コマンドを使用します。

マスター コントローラを一時的にディセーブルにするには、PfR マスター コントローラ コンフィギュレーション モードで **shutdown**（PfR）コマンドを使用します。**shutdown**（PfR）コマンドを入力すると、アクティブなマスター コントローラ プロセスが停止しますが、設定パラメータは削除されません。**shutdown**（PfR）コマンドは、イネーブルな場合、実行コンフィギュレーション ファイルに表示されます。

前提条件

インターフェイスは、PfR 管理のネットワークを設定する前に定義され、マスター コントローラとボーダー ルータによって到達できる必要があります。

PfR 管理のネットワークを設定するには、ボーダー ルータとピア ルータとの間にスタティック ルーティング、またはルーティング プロトコルのピアリングまたは再配布を設定して、PfR でルーティングが制御されるようにする必要があります。PfR は、（Protocol Independent Route Optimization（PIRO）により）スタティック ルート、BGP、EIGRP または RIB を使用して、最適なパスのための親ルートを検索できます。

ヒント　PfR 管理のネットワークでの通信応答時間を最小化するため、マスター コントローラとボーダー ルータを物理的に近づけて置くことを推奨します。トラフィックがボーダー ルータ間でルーティングされる場合も、ホップ数を最小化するためにボーダー ルータ同士を物理的に近づけて置く必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*

4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. ステップ 6 を繰り返します。
8. ステップ 3 ～ステップ 7 を繰り返して、各ボーダー ルータに対してキー チェーン認証を設定するために適切な変更を行います。
9. **pfr master**
10. **logging**
11. **border** *ip-address* [**key-chain** *key-chain-name*]
12. **interface** *type number* **external**
13. **exit**
14. **interface** *type number* **internal**
15. **exit**
16. ステップ 11 ～ステップ 15 を繰り返して、各ボーダー ルータとの通信を確立するために適切な変更を行います。
17. **keepalive** *timer*
18. **end**
19. **show running-config**

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。 • プロンプトが表示されたら、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 border1_PFR`	キー チェーン認証をイネーブルにし、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。 • キー チェーン認証は、マスター コントローラとボーダー ルータとの間の通信セッションを保護します。通信を確立するために、キー ID とキー文字列は一致する必要があります。 • この例では、ボーダー ルータ 1 との使用のためにキー チェーンが作成されます。
ステップ 4	**key** *key-id* **例：** `Router(config-keychain)# key 1`	キー チェーンの認証キーを識別します。 • キー ID は、ボーダー ルータで設定されたキー ID に一致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 5	**key-string** *text* **例：** `Router(config-keychain-key)# key-string b1`	キーの認証文字列を指定し、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。 • 認証文字列は、ボーダー ルータで設定された認証文字列に一致する必要があります。 • 暗号化レベルを設定できます。 • この例では、ボーダー ルータ 1 との使用のためにキー ストリングが作成されます。
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 モードを終了して、キー チェーン コンフィギュレーション モードに戻ります。
ステップ 7	ステップ 6 を繰り返します。	キー チェーン 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 モードに戻ります。
ステップ 8	ステップ 3 ～ステップ 7 を繰り返して、各ボーダー ルータに対してキー チェーン認証を設定するために適切な変更を行います。	—
ステップ 9	**pfr master** **例：** `Router(config)# pfr master`	PfR マスター コントローラ コンフィギュレーション モードを開始して、ルータをマスター コントローラとして設定します。 • マスター コントローラおよびボーダー ルータのプロセスを同じルータ上でイネーブルにできます（別個のサービス プロバイダーに 2 つの出口リンクを持つ 1 つのルータを含むネットワーク内など）。
ステップ 10	**logging** **例：** `Router(config-pfr-mc)# logging`	マスター コントローラまたはボーダー ルータ プロセスに対して syslog メッセージをイネーブルにします。 • syslog メッセージの通知レベルはデフォルトでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 11	**border** *ip-address* [**key-chain** *key-chain-name*] **例：** `Router(config-pfr-mc)# border 10.1.1.2 key-chain border1_PFR`	PfR 管理ボーダー ルータ コンフィギュレーション モードを開始して、ボーダー ルータとの通信を確立します。 • ボーダー ルータを識別するために、IP アドレスを設定します。 • PfR 管理のネットワークを作成するには、少なくとも 1 つのボーダー ルータを指定する必要があります。1 台のマスター コントローラで制御できるボーダー ルータは、最大 10 台です。 • *key-chain-name* 引数の値は、ステップ 3 で設定されたキー チェーン名に一致する必要があります。 **（注）** ボーダー ルータが最初に設定されている場合は、**key-chain** キーワードおよび *key-chain-name* 引数を入力する必要があります。ただし、既存のボーダー ルータを再設定する場合、このキーワードは省略可能です。
ステップ 12	**interface** *type number* **external** **例：** `Router(config-pfr-mc-br)# interface Ethernet 1/0 external`	ボーダー ルータ インターフェイスを PfR 管理の外部インターフェイスとして設定します。 • 外部インターフェイスは、トラフィックの転送およびアクティブ モニタリングに使用されます。 • PfR 管理のネットワークには、最低 2 つの外部ボーダー ルータ インターフェイスが必要です。各ボーダー ルータでは、少なくとも 1 つの外部インターフェイスを設定する必要があります。1 台のマスター コントローラで制御できる外部インターフェイスは、最大 20 です。 **ヒント** ルータでインターフェイスを PfR 管理外部インターフェイスとして設定すると、PfR ボーダー出口インターフェイス コンフィギュレーション モードが開始されます。このモードでは、インターフェイスに対して最大リンク使用率またはコストベースの最適化を設定できます。 **（注）** **external** キーワードまたは **internal** キーワードを指定せずに **interface**（PfR）コマンドを入力すると、ルータは、PfR ボーダー出口コンフィギュレーション モードではなく、グローバル コンフィギュレーション モードで開始されます。アクティブ インターフェイスがルータ設定から削除されないように、このコマンドの **no** 形式は慎重に適用してください。
ステップ 13	**exit** **例：** `Router(config-pfr-mc-br-if)# exit`	PfR 管理ボーダー出口インターフェイス コンフィギュレーション モードを終了し、PfR 管理ボーダー ルータ コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 14	**interface** *type number* **internal** **例：** `Router(config-pfr-mc-br)# interface Ethernet 0/0 internal`	ボーダー ルータ インターフェイスを PfR 制御内部インターフェイスとして設定します。 • 内部インターフェイスはパッシブ モニタリングだけに対して使用されます。内部インターフェイスはトラフィックを転送しません。 • 各ボーダー ルータでは、少なくとも 1 つの内部インターフェイスを設定する必要があります。
ステップ 15	**exit** **例：** `Router(config-pfr-mc-br)# exit`	PfR 管理ボーダー ルータ コンフィギュレーション モードを終了し、PfR マスター コントローラ コンフィギュレーション モードに戻ります。
ステップ 16	ステップ 11 ～ステップ 15 を繰り返して、各ボーダー ルータとの通信を確立するために適切な変更を行います。	—
ステップ 17	**keepalive** *timer* **例：** `Router(config-pfr-mc)# keepalive 10`	（任意）キープアライブ パケットが受信されなくなった後に PfR マスター コントローラが PfR ボーダー ルータとの接続を保持する時間の長さを設定します。 • 例では、キープアライブ タイマーを 10 秒に設定しています。デフォルトのキープアライブ タイマーは 60 秒です。
ステップ 18	**end** **例：** `Router(config-pfr-mc-learn)# end`	PfR Top Talker/Top Delay 学習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。
ステップ 19	**show running-config** **例：** `Router# show running-config`	（任意）稼動している設定を表示してこのタスクで入力された設定を確認します。

PFR ボーダー ルータの設定

このタスクを実行して PfR ボーダー ルータを設定します。このタスクは、PfR 管理のネットワークの各ボーダー ルータで実行する必要があります。1 つのマスター ルータと 2 つのボーダー ルータのネットワーク設定例については、図 3 を参照してください。最初に、ボーダー ルータとマスター コントローラとの間で通信が確立されます（ボーダー ルータとマスター コントローラとの間の通信セッションを保護するためにキー チェーン認証が設定されます）。ローカル インターフェイスはマスター コントローラとの通信元として設定され、外部インターフェイスは PfR 管理終了リンクとして設定されます。

ボーダー ルータをディセーブルにし、実行コンフィギュレーションからプロセス設定を完全に削除するには、グローバル コンフィギュレーション モードで **no pfr border** コマンドを使用します。

ボーダー ルータ プロセスを一時的にディセーブルにするには、PfR ボーダー ルータ コンフィギュレーション モードで **shutdown**（PfR）コマンドを使用します。**shutdown**（PfR）コマンドを入力すると、アクティブなボーダー ルータ プロセスが停止しますが、設定パラメータは削除されません。**shutdown**（PfR）コマンドは、イネーブルな場合、実行コンフィギュレーション ファイルに表示されます。

前提条件

- タスク「PfR マスター コントローラの設定」（P.12）を実行して、マスター コントローラを設定し、インターフェイスを定義し、ボーダー ルータとの通信を確立します。
- 各ボーダー ルータには、ISP に接続するために使用するか、または外部 WAN リンクとして使用する外部インターフェイスが少なくとも 1 つ必要です。PfR 管理のネットワークでは、少なくとも 2 つの外部インターフェイスが必要です。
- 各ボーダー ルータには、少なくとも 1 つの内部インターフェイスが必要です。内部インターフェイスは、NetFlow によるパッシブ パフォーマンス モニタリングにだけ使用されます。内部インターフェイスは、トラフィックを転送するために使用されません。
- 各ボーダー ルータには、少なくとも 1 つのローカル インターフェイスが必要です。ローカル インターフェイスは、マスター コントローラとボーダー ルータとの通信に対してだけ使用されます。各ボーダー ルータでは、単一インターフェイスをローカル インターフェイスとして設定する必要があります。

ヒント マスター コントローラおよびボーダー ルータ プロセスが同じルータでイネーブルな場合は、ループバック インターフェイスをローカル インターフェイスとして設定する必要があります。

ヒント ホップ数を最小化するためにボーダー ルータ同士を物理的に近づけて置くことが推奨されます。また、PfR 管理のネットワークでの通信応答時間を最小化するため、マスター コントローラとボーダー ルータも物理的に近づけて置くことを推奨します。

制約事項

- ボーダー ルータが同じブロードキャスト メディアを介して複数のサービス プロバイダーと通信できるインターネット交換ポイントはサポートされていません。
- PfR 管理のネットワークに 2 つ以上のボーダー ルータが導入された場合、各ボーダー ルータ上の外部ネットワークに対するネクスト ホップ（RIB に導入済み）を同じサブネットの IP アドレスにすることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. ステップ 6 を繰り返します。
8. **pfr border**
9. **local** *type number*
10. **master** *ip-address* **key-chain** *key-chain-name*
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。 • プロンプトが表示されたら、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 border1_PFR`	キー チェーン認証をイネーブルにし、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。 • キー チェーン認証は、マスター コントローラとボーダー ルータとの間の通信セッションを保護します。通信を確立するために、キー ID とキー文字列は一致する必要があります。
ステップ 4	**key** *key-id* **例：** `Router(config-keychain)# key 1`	キー チェーンの認証キーを識別し、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。 • キー ID は、マスター コントローラで設定されたキー ID に一致する必要があります。
ステップ 5	**key-string** *text* **例：** `Router(config-keychain-key)# key-string b1`	キーの認証文字列を指定します。 • 認証文字列は、マスター コントローラで設定された認証文字列に一致する必要があります。 • どのようなレベルの暗号化でも設定できます。
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 モードを終了して、キー チェーン コンフィギュレーション モードに戻ります。
ステップ 7	ステップ 6 を繰り返します。 **例：** `Router(config-keychain)# exit`	キー チェーン コンフィギュレーション モードを終了して、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 8	**pfr border** **例：** `Router(config)# pfr border`	PfR ボーダー ルータ コンフィギュレーション モードを開始して、ルータをボーダー ルータとして設定します。 • ボーダー ルータは転送パスに指定され、少なくとも 1 つの外部および内部インターフェイスを含む必要があります。

	コマンドまたはアクション	目的
ステップ 9	**local** *type number* **例：** `Router(config-pfr-br)# local Ethernet 0/0`	PfR ボーダー ルータのローカル インターフェイスを PfR マスター コントローラとの通信元として指定します。 • ローカル インターフェイスを定義する必要があります。 **ヒント** 単一ルータがマスター コントローラとボーダー ルータ プロセスの両方を実行するよう設定されている場合はループバックを設定する必要があります。
ステップ 10	**master** *ip-address* **key-chain** *key-chain-name* **例：** `Router(config-pfr-br)# master 10.1.1.1 key-chain border1_PFR`	PfR 管理ボーダー ルータ コンフィギュレーション モードを開始して、マスター コントローラとの通信を確立します。 • マスター コントローラを識別するために IP アドレスが使用されます。 • *key-chain-name* 引数の値は、ステップ 3 で設定されたキー チェーン名に一致する必要があります。
ステップ 11	**end** **例：** `Router(config-pfr-br)# end`	PfR Top Talker/Top Delay 学習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。

次に行うこと

ネットワークでスタティック ルーティングのみを使用するように設定している場合、追加のルーティング プロトコル ピアリングやスタティックな再配布の設定は必要ありません。ボーダー ルータの外部インターフェイスを示す有効なスタティック ルートが設定されている限り、PfR 管理のネットワークは稼動している必要があります。PfR のカスタマイズについては、「次の作業」（P.20）を参照してください。

ベーシック パフォーマンス ルーティングの設定例

例：PfR マスター コントローラの設定

次に、グローバル コンフィギュレーション モードで開始し、マスター コントローラ プロセスを設定して内部ネットワークを管理するのに最低限必要な設定例を示します。PFR と呼ばれるキー チェーン設定が、グローバル コンフィギュレーション モードで定義されます。

```
Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end
```

マスター コントローラは、10.100.1.1 のボーダー ルータおよび 10.200.2.2 のボーダー ルータと通信するよう設定されます。キープアライブ間隔は 10 秒に設定されます。ルート制御モードは、イネーブルです。内部および外部の PfR 制御ボーダー ルータ インターフェイスが定義されます。

```
Router(config)# pfr master
Router(config-pfr-mc)# keepalive 10
Router(config-pfr-mc)# logging
Router(config-pfr-mc)# border 10.100.1.1 key-chain PFR
Router(config-pfr-mc-br)# interface Ethernet 0/0 external
Router(config-pfr-mc-br)# interface Ethernet 0/1 internal
Router(config-pfr-mc-br)# exit
Router(config-pfr-mc)# border 10.200.2.2 key-chain PFR
Router(config-pfr-mc-br)# interface Ethernet 0/0 external
Router(config-pfr-mc-br)# interface Ethernet 0/1 internal
Router(config-pfr-mc)# exit
```

例：PfR ボーダー ルータの設定

次に、グローバル コンフィギュレーション モードで開始して、ボーダー ルータをイネーブルにするのに最低限必要な設定例を示します。キー チェーン設定はグローバル コンフィギュレーション モードで定義します。

```
Router(config)# key chain PFR
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string KEYSTRING2
Router(config-keychain-key)# end
```

通信を保護するためにキー チェーン PFR が適用されます。マスター コントローラに対してインターフェイスは、PfR 通信のローカル インターフェイス（ソース）として識別されます。

```
Router(config)# pfr border
Router(config-pfr-br)# local Ethernet 0/1
Router(config-pfr-br)# master 192.168.1.1 key-chain PFR
Router(config-pfr-br)# end
```

次の作業

マスター コントローラとボーダー ルータを設定した後に、PfR の完全な最適化機能をアクティブにするために追加の設定が必要になることがあります。詳細については、「Understanding Performance Routing」モジュールおよび「Configuring Advanced Performance Routing」モジュールを参照するか、「関連資料」（P.21）に記載された他の参考資料を参照してください。

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco PfR コマンド（コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例）	『*Cisco IOS Performance Routing Command Reference*』
アドバンスド PfR の設定	「Configuring Advanced Performance Routing」モジュール
パフォーマンス ルーティングの運用フェーズを理解するために必要な概念	「Understanding Performance Routing」モジュール
PfR 機能の位置	「Cisco IOS Performance Routing Features Roadmap」モジュール
IP SLA の概要	『*Cisco IOS IP SLAs Overview*』

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/cisco/web/support/index.html

ベーシック パフォーマンス ルーティング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。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　ベーシック パフォーマンス ルーティングの設定に関する機能情報

機能名	リリース	機能情報
Optimized Edge Routing（OER）	12.3(8)T 12.2(33)SRB	OER が導入されました。パフォーマンス ルーティングは OER の拡張機能です。