パフォーマンス ルーティング コンフィギュレーション ガイド、Cisco IOS XE Release 3S（Cisco ASR 1000）

初版：2012 年 07 月 25 日

最終更新：2012 年 11 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

目 次

第 1 章

ベーシック パフォーマンス ルーティングの設定

パフォーマンス ルーティング（PfR）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、Cisco IOS XE ソフトウェアを使用してパフォーマンス 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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

ベーシックパフォーマンスルーティングの設定の制約事項

境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 Cisco IOS XE Release 3.1S および 3.2S イメージで境界ルータとして使用されている Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

（注） Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

パフォーマンス ルーティングについて

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、MOS スコア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 サービス レベル契約（SLA）（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ッ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。

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ッ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、プレフィッ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ルーティング情報ベース（RIB）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、プレフィッ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 コマンドライン インターフェイス（CLI）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マスターコントローラ（MC）と境界ルータ（BR）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、発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。次の図を参照してください。 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 境界ルータ

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、プレフィッ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、プレフィッ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。

Cisco IOS XE Release 2、3.1S、および3.2S に含まれる境界ルータ専用機能の詳細については、「パフォーマンス ルーティング境界ルータ専用機能」モジュールを参照してください。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

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 ポリシーベース ルーティング（PBR）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。

Cisco IOS XE Release 2、3.1S、および 3.2S では、PfR は境界ルータ専用としての ASR 1000 シリーズ ルータをサポートしており、マスター コントローラは Cisco IOS Release 15.0(1)M イメージを実行している必要があります。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

PfR コンポーネントのバージョン

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、および境界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境界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境界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バージョンが境界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 XE ソフトウェア リリースでは更新されませんが、Cisco IOS XE 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境界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 のためのキー チェーン認証

マスター コントローラと境界ルータ間の通信は、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 コントローラと境界ルータの両方で設定されている必要があります。 キーチェーン認証は、マスターコントローラから境界ルータへの通信に対してキーチェーン認証がイネーブルになる前に、マスター コントローラと境界ルータの両方のグローバル

コンフィギュレーション モードで定義されます。 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」章の「Managing Authentication Keys」項を参照してください。

PfR 管理対象ネットワーク 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 リンクに接続する必要があります。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境界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ッ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。 各境界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境界ルータ 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。 各境界ルータでは、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 コントローラと境界ルータとの通信に対してだけ使用されます。 各境界ルータでは、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。

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
- チャネライズド インターフェイス（T1 への T3/STM1）
- ファスト イーサネット
- ギガビット イーサネット
- 10 ギガビット イーサネット
- Packet-over-SONET（POS）
- シリアル（Serial）

- トンネル（Cisco IOS XE Release 2、3.1S 以降のリリースでは、NAT を使用する場合サポートされません）
- VLAN（QinQ はサポートされていない）

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。

- ATM
- ファスト イーサネット
- ギガビット イーサネット
- 10 ギガビット イーサネット
- Packet-over-SONET（POS）
- シリアル（Serial）
- トンネル（Cisco IOS XE Release 2、3.1S 以降のリリースでは、NAT を使用する場合サポートされません）
- VLAN（QinQ はサポートされていない）

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 マルチポイント GRE（mGRE）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、境界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。 次の図は、5 つの PfR フェーズ（プロファイル、測定、ポリシー適用、施行、確認）を示しています。

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、この 5 つの PfR フェーズを理解し、実行する必要があります。 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ルーティング情報ベース（RIB）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、ポリシー違反（OOP）イベントになります。 結果は相対的に（実際の平均値からの偏差）、またはしきい値ベースで（値の下限または上限、または両方の組み合わせ）比較されます。

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、プレフィッ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。 プレフィッ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ッ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ッ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。

プレフィッ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、プレフィッ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、リモート境界ルータはシングル 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インターネット サービス プロバイダー（ISP）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 つのプレフィックスまたはプレフィッ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境界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で転送される（国内または国際的に）際、パケットはネットワークの WAN セグメント上でのパケット ライフ サイクルのほとんどを費やします。 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）。

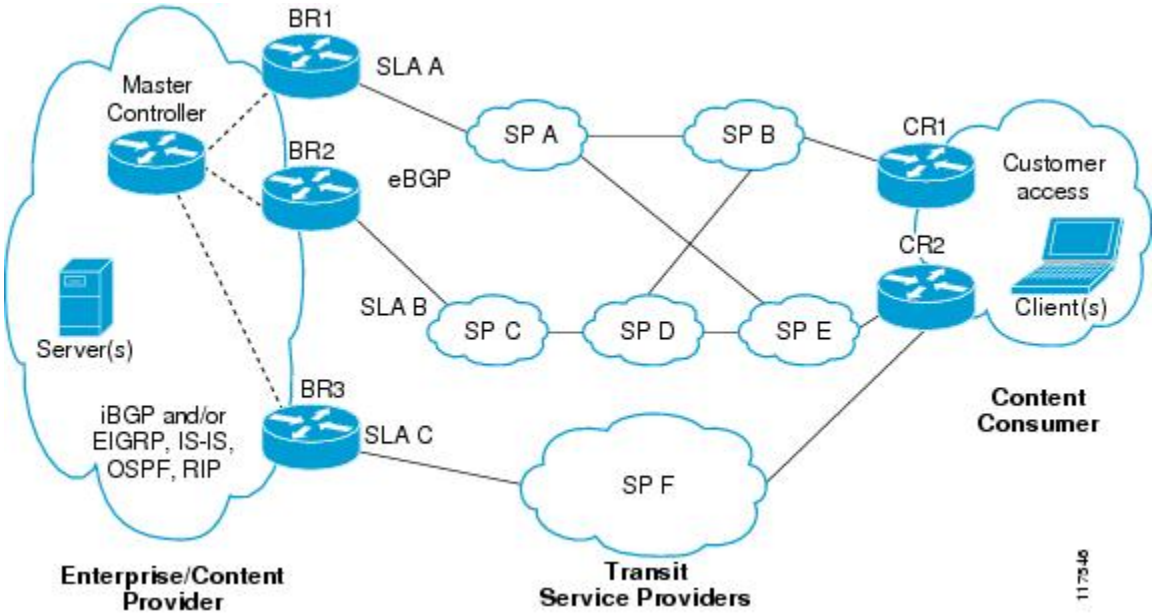
PfR 導入の説明に使用される例の多くはエッジ デバイスが通信するネットワークとして ISP を示していますが、他のソリューションも存在します。 ネットワーク エッジはネットワーク内で論理的に区切るものとして定義できます。これには、同じ場所にあるデータセンター ネットワークなどのネットワークの別の部分や WAN 接続および ISP 接続などがあります。 元のネットワーク エッジデバイスに接続されたネットワークまたはネットワークの一部は、BGP を使用して通信する場合は個別の自律システム番号を持つ必要があります。

PfR は、シスコ コア ルーティング機能に内蔵された状態で実装されています。 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、稼働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

下の図は、コンテンツ プロバイダーの一般的な PfR 管理の企業ネットワークを示しています。 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 つのサービス プロバイダー（SP）が存在します。

図 *2*：典型的な *PfR* 導入



PfR は、3 つの境界ルータ（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。境界ルータでの出口リンク パフォーマンスの変更は、1 つのプレフィックスごとに検出されます。プレフィッ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 ネットワーク内のインターフェイス障害またはネットワークの設定ミスが

原因で、BR2 出口インターフェイス上で伝送される発信トラフィックに輻輳が発生する、またはカスタマー アクセス ネットワークに到達できない場合があります。 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。

（注） Cisco IOS XE Release 2、3.1S、および 3.2S では、PfR は境界ルータ専用としての ASR 1000 シリーズ ルータをサポートしており、マスター コントローラは、バージョンの互換性のため Cisco IOS Release 15.0M イメージを実行している必要があります。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

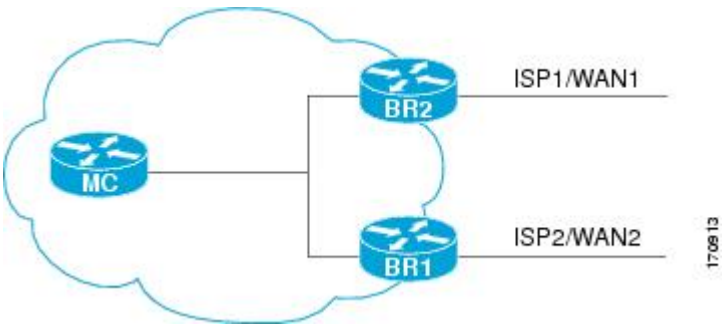
ベーシック パフォーマンス ルーティングの設定方法

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 つの境界ルータのネットワーク設定例については、下の図を参照してください。 まずマスター コントローラと境界ルータとの間で、マスター コントローラと境界ルータとの間の通信セッションを保護するために設定されるキー チェーン認証を使用し、通信が確立されます。 また、内部および外部境界ルータ インターフェイスも指定されます。

（注） Cisco IOS XE Release 3.1S 以降のリリースでは、PfR は境界ルータ専用としての ASR 1000 シリーズ ルータをサポートしており、マスター コントローラは、Cisco IOS Release 15.0M イメージを実行している必要があります。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

図 *3*：マスター コントローラと境界ルータの図



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、**shutdown** コマンドを PfR マスター コントローラ コンフィギュレーション モードで使用します。 **shutdown** コマンドを入力することで、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。 イネーブルの場合、**shutdown** コマンドは実行コンフィギュレーション ファイルに表示されます。

はじめる前に

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 コントローラと境界ルータによって到達できる必要があります。

PfR 管理対象ネットワークを設定するには、PfR がルーティングを制御するため、境界ルータとピア ルータとの間でルーティング プロトコル ピアリングまたは再配布を設定する必要があります。

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 コントローラと境界ルータを物理的に近づけて置くことを推奨します。 トラフィックが境界ルータ間でルーティングされる場合も、ホップ カウントを最小化するために境界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 3 ～ 7 を繰り返します。
8. 適切な変更を加えてステップ 3 ～ 7 を繰り返し、各境界ルータのキー チェーン認証を設定します。
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. 適切な変更を加えてステップ 11 ～ 15 を繰り返し、各境界ルータとの通信を確立します。
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。 • パスワードを入力します（要求された場合）。
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 コントローラと境界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。

	コマンドまたはアクション	目的
		• この例では、境界ルータ 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、境界ルータで設定されたキー 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、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、境界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、境界ルータ 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 3 ～ 7 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	適切な変更を加えてステップ 3 ～ 7 を繰り返し、各境界ルータのキーチェーン認証を設定します。	--
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境界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境界ルータ プロセスに対して syslog メッセージをイネーブルにします。

	コマンドまたはアクション	目的
		• 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。
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 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界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 つの境界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境界ルータは、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） 境界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、既存の境界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 GigabitEthernet 0/0/0 external`	境界ルータ 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 つの外部境界ルータ インターフェイスが必要です。 各境界ルータでは、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** 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。

	コマンドまたはアクション	目的
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 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* **internal** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 1/0/0 internal`	境界ルータ 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。 • 各境界ルータでは、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 管理境界ルータ 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	適切な変更を加えてステップ 11 ～ 15 を繰り返し、各境界ルータとの通信を確立します。	--
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 境界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）稼働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 境界ルータの設定

このタスクを実行して PfR 境界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境界ルータで実行する必要があります。最初に、境界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（境界ルータとマスター 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。

境界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。

境界ルータ プロセスを一時的にディセーブルにするには、**shutdown** コマンドを PfR 境界ルータ コンフィギュレーション モードで使用します。 **shutdown** コマンドを入力することで、アクティブな境界ルータ 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。 イネーブルの場合、**shutdown** コマンドは実行コンフィギュレーション ファイルに表示されます。

はじめる前に

- PfR マスター コントローラの設定タスクを実行して、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、境界ルータとの通信を確立します。
- 各境界ルータには、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。
- 各境界ルータには、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。
- 各境界ルータには、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 コントローラと境界ルータとの通信に対してだけ使用されます。 各境界ルータでは、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 Cisco IOS XE Release 3.1S および 3.2S では、PfR は境界ルータ専用としての ASR 1000 シリーズ ルータをサポートしており、マスター コントローラは ASR 1000 シリーズ ルータ上でイネーブルにできません。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

ヒント ホップ カウントを最小化するために境界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 コントローラと境界ルータも物理的に近づけて置くことを推奨します。

（注）
- 境界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 つ以上の境界ルータが導入された場合、各境界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。 • パスワードを入力します（要求された場合）。
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 コントローラと境界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。

	コマンドまたはアクション	目的
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 境界ルータ コンフィギュレーション モードを開始して、ルータを境界ルータとして設定します。 • 境界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。
ステップ 9	**local** *type number* 例： `Router(config-pfr-br)# local GigabitEthernet 0/0/0`	PfR 境界ルータのローカル 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。
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 管理境界ルータ 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。

	コマンドまたはアクション	目的
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。

次の作業

ネットワークがスタティック ルーティングだけを使用するように設定されている場合、追加の設定は必要ありません。境界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働している必要があります。

そのように設定されていない場合、PfR 管理対象ネットワーク内の境界ルータとその他のルータとの間にルーティング プロトコル ピアリングまたはスタティック再配布が設定されている必要があります。

ベーシック パフォーマンス ルーティングの設定例

PfR マスター コントローラの設定例

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。

（注） この設定は、マスター コントローラ上で実施します。 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S に含まれます。マスター コントローラ設定は使用できません。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

```
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 の境界ルータおよび 10.200.2.2 の境界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 制御境界ルータ 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 GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 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 GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-pfr-mc)# exit
```

PfR 境界ルータの設定例

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、境界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 GigabitEthernet 1/0/0
Router(config-pfr-br)# master 192.168.1.1 key-chain PFR
Router(config-pfr-br)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール

関連項目	マニュアル タイトル
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

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）	Cisco IOS XE Release 2.6.1、Cisco IOS XE Release 3.1S	OER は Cisco ASR 1000 シリーズ ルータで導入されました。パフォーマンス ルーティングは OER の拡張機能です。 PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 次のコマンドが導入または変更されました。pfr、show pfr master。 （注） 境界ルータ専用機能は Cisco IOS XE Release 2.6.1 および Cisco IOS XE Release 3.1S リリースに含まれています。マスター コントローラ設定は使用できません。 境界ルータとして使用される Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M を実行するルータでなければなりません。

機能名	リリース	機能情報
ASR 1000 用 PfR マスター コントローラのサポート	Cisco IOS XE Release 3.3S	Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ機能がサポートされます。

パフォーマンス ルーティング コンフィギュレーション ガイド、**Cisco IOS XE Release 3S**（**Cisco ASR 1000**）

第 2 章

パフォーマンス ルーティング境界ルータ専用機能

パフォーマンス ルーティング（PfR）によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上での境界ルータ（BR）専用機能のサポートが導入されました。 境界ルータ専用機能をサポートするソフトウェア イメージでは、マスター コントローラ設定は使用できません。 この状況で境界ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータである必要があります。 他のプラットフォーム上のパフォーマンス ルーティング境界ルータ専用機能と異なり、Cisco ASR 1000 シリーズ ルータでは境界ルータ パッシブ モニタリング機能をアクティブ モニタリング機能と同様にフルに提供できます。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

（注） PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 Optimized Edge Routing（OER）構文を使用して Cisco IOS XE Release 2.6.1 を実行している場合、『Cisco IOS XE Performance Routing Configuration Guide, Release 2』を参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR 境界ルータ専用機能の前提条件

PfR 境界ルータとして使用する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、Cisco IOS XE Release 3.1S 以降のリリースを実行している必要があります。

PfR 境界ルータ専用機能の制約事項

境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 Cisco IOS XE Release 3.1S および 3.2S イメージで境界ルータとして使用されている Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

PfR 境界ルータ専用機能に関する情報

ASR 1000 シリーズ ルータ上での PfR 境界ルータ専用機能

PfR によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上での境界ルータ（BR）専用機能のサポートが導入されました。 Cisco IOS XE Release 3.1S で PfR 構文が導入されました。 境界ルータ専用機能をサポートするソフトウェア イメージでは、マスター コントローラ設定は使用できません。 この状況で境界ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M を実行するルータでなければなりません。 他のプラットフォーム上の境界ルータ専用機能と異なり、Cisco ASR 1000 シリーズ ルータでは境界ルータ パッシブ モニタリング機能をアクティブ モニタリング機能と同様にフルに提供できます。

PfR は、次の 3 つのトラフィック クラス パフォーマンス測定手法を使用します。

- パッシブ モニタリング：トラフィックが NetFlow 機能を使用してデバイスを通過する間に、トラフィック クラス エントリのパフォーマンス メトリックを測定します。 学習および設定されたプレフィックスに基づき、パフォーマンス ルーティングは（現在の出口の）すべての

フロー上のトラフィックに対するTCPフラグをパッシブに監視し、遅延、パケット損失、および到達可能性を測定します。 スループット ベースのロード バランシングはまだサポートされています。

- アクティブモニタリング：トラフィック クラスをできる限り忠実に再現して合成トラフィックのストリームを作成し、その合成トラフィックのパフォーマンス メトリックを測定します。 合成トラフィックのパフォーマンス メトリック結果は、マスター コントローラ データベース内のトラフィック クラスに適用されます。 アクティブ モニタリングでは、統合されたIP サービス レベル契約（SLA）機能が使用されます。
- アクティブ モニタリングとパッシブ モニタリングの両方：ネットワーク内のトラフィック フローをより正確に把握するために、アクティブ モニタリングとパッシブ モニタリングを組み合わせます。

モニタリング モードは、モニタリング モードをイネーブルにするための要求を境界ルータに送信するマスター コントローラ上で、コマンドライン インターフェイス（CLI）を使用して構成します。

この設定はマスター コントローラ上で実行する必要がありますが、Cisco ASR 1000 シリーズ ルータ内の境界ルータ（BR）専用機能は次の機能をサポートします。

- OER アクティブ プローブ ソース アドレス：OER アクティブ プローブ ソース アドレス機能では、境界ルータ上で特定の出口インターフェイスをアクティブ プローブのソースとして設定できます。 OER アクティブ プローブ ソース アドレスの設定の詳細については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。
- OER：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング機能によって、1 つのキーワードだけを使用して標準アプリケーションを設定できるようになりました。 この機能により、学習リストにプロファイリングされたトラフィック クラスにパフォーマンス ルーティング（PfR）ポリシーを適用できる学習リスト コンフィギュレーション モードも導入されました。 異なるポリシーを各学習リストに適用できます。 PfRが自動的に学習できるトラフィック クラス、または手動で設定するトラフィック クラスの設定を容易にするため、traffic-class コマンドおよび match traffic-class コマンドが新たに導入されました。 OER アクティブ プローブ ソース アドレスの設定の詳細については、「パフォーマンス ルーティングを使用したスタティック アプリケーション マッピング」モジュールを参照してください。
- ポリシー ルール設定およびポート ベースのプレフィックス学習に対する OER サポート：ポリシー ルール設定に対する OER サポート機能によって、OER 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 OER マップを選択して設定を適用する機能が導入され、定義済みの OER マップ間で切り替えるための方式が向上します。 ポリシー ルールおよびポート ベースのプレフィックス学習を設定する方法の詳細については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。
- OER ポートおよびプロトコル ベースのプレフィックス学習：OER ポートおよびプロトコル ベースのプレフィックス学習機能によって、プロトコル タイプおよび TCP または UDP ポート番号に基づいてプレフィックスを学習するようにマスター コントローラを設定する機能が導入されました。 プロトコルおよびポート ベースのプレフィックス学習を設定する方法の

詳細については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。

- コスト ベースの最適化および traceroute レポートに対する OER サポート：コスト ベースの最適化に対する OER サポート機能によって、金銭的なコストに基づいて出口リンク ポリシーを設定する機能、および traceroute プローブを設定してホップバイホップ ベースのプレフィックス特性を判断する機能が導入されました。 パフォーマンス ルーティングでは traceroute レポートをサポートしているので、ホップバイホップ ベースでプレフィックスのパフォーマンスを監視できます。 遅延、損失、および到達可能性の測定が、プローブ ソース（境界ルータ）からターゲット プレフィックスへのホップごとに収集されます。 詳細については、「パフォーマンス ルーティング コスト ポリシーの設定」または「パフォーマンス ルーティングの traceroute レポート」モジュールを参照してください。
- BGP インバウンド最適化：PfR BGP インバウンド最適化は、自律システム内部のプレフィックスに宛てた自律システム外部のプレフィックスを送信元とするトラフィックに対する最適な入口の選択をサポートします。 自律システムからインターネット サービス プロバイダー（ISP）への外部 EGP（eBGP）アドバタイズメントにより、ネットワークに入るトラフィックの入口パスが影響を受けることがあります。 PfR では、eBGP アドバタイズメントを使用して最適な入口選択を行います。 BGP インバウンド最適化を設定する方法の詳細については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

（注） Cisco IOS XE Release 3.1S 以降のリリースの Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上では、モニタリング期間中に学習できる内部プレフィックスの最大数は 30 です。

- DSCP モニタリング：OER DSCP モニタリングによって、プロトコル、ポート番号、および DSCP 値に基づくトラフィック クラスの自動学習が導入されました。 トラフィック クラスは、プロトコル、ポート番号、および DSCP 値で構成され、不要なトラフィックをフィルタリングでき、関心のあるトラフィックを集約できる、キーの組み合わせによって定義できます。 これで、プロトコル、ポート番号、および DSCP 情報などのレイヤ 4 情報は、レイヤ 3 プレフィックス情報に加えてマスター コントローラ データベースに送信されるようになります。 この新しい機能により、OER によるアプリケーション トラフィックのアクティブ モニタリングおよびパッシブ モニタリングの両方が可能になりました。 ポリシー ルールおよびポート ベースのプレフィックス学習を設定する方法の詳細については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。
- パフォーマンス ルーティング - Protocol Independent Route Optimization（PIRO）：PIRO は、PfR で IP ルーティング情報ベース（RIB）の親ルート（完全一致ルート、またはそれより一致度が低いルート）を検索し、OSPF および IS-IS などの内部ゲートウェイ プロトコル（IGP）を含む IP ルート環境に PfR を導入できる機能を導入しました。 PIRO の構成の詳細については、「パフォーマンス ルーティング：Protocol Independent Route Optimization（PIRO）」モジュールを参照してください。

- 高速フェール オーバー モニタリング：高速フェールオーバー モニタリングにより、高速モニタリング モードを設定できる機能が導入されました。 高速フェールオーバー モニタリング モードでは、アクティブ モニタリングとパッシブ モニタリングを使用して、すべての出口が継続的にプローブされます。 高速フェールオーバー モニタリング モードのプローブ頻度は、他のモニタリング モードよりも低く設定できます。これにより、より迅速なフェールオーバー機能が可能になります。 高速フェールオーバー モニタリングは、すべてのタイプのアクティブ プローブ（ICMP エコー、ジッター、TCP 接続、および UDP エコー）で使用できます。 高速フェールオーバー モニタリングの設定の詳細については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。
- EIGRP mGRE DMVPN 統合：PfR EIGRP 機能によって、ルート親チェックを EIGRP データベース上で実施することで、EIGRP に基づく PfR ルート制御機能が導入されます。 また、ハブツースポーク ネットワーク設計に準拠する mGRE Dynamic Multipoint VPN（DMVPN）導入のサポートも追加します。 EIGRP ルート制御および mGRE DMVPN サポートの詳細については、「パフォーマンス ルーティングの mGRE DMVPN ハブアンドスポーク サポートを使用した EIGRP ルートの制御」モジュールを参照してください。
- OER 音声トラフィックの最適化：PfR 音声トラフィックの最適化機能によって、音質メトリック、ジッター、および平均オピニオン評点（MOS）に基づく音声トラフィックのアウトバウンド最適化のサポートが提供されます。 ジッターおよび MOS は、音声トラフィック向けの重要な定量的品質メトリックであり、これらの音質メトリックは PfR アクティブ プローブを使用して測定します。 ポリシー ルールおよびポート ベースのプレフィックス学習を設定する方法の詳細については、「アクティブ プローブを使用した PfR 音声トラフィック最適化」モジュールを参照してください。

PfR 境界ルータの運用

PfR は、Cisco IOS コマンドライン インターフェイス（CLI）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マスターコントローラ（MC）と境界ルータ（BR）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。

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、プレフィッ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、プレフィックス 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。

PfR 境界ルータ専用機能の設定方法

PFR 境界ルータの設定

このタスクを実行して PfR 境界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境界ルータで実行する必要があります。最初に、境界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（境界ルータとマスター 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。

境界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。

境界ルータ プロセスを一時的にディセーブルにするには、**shutdown** コマンドを PfR 境界ルータ コンフィギュレーション モードで使用します。 **shutdown** コマンドを入力することで、アクティブな境界ルータ 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。 イネーブルの場合、**shutdown** コマンドは実行コンフィギュレーション ファイルに表示されます。

はじめる前に

- PfR マスター コントローラの設定タスクを実行して、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、境界ルータとの通信を確立します。 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 これらのイメージで境界ルータとして使用されている Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。
- 各境界ルータには、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。
- 各境界ルータには、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。
- 各境界ルータには、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 コントローラと境界ルータとの通信に対してだけ使用されます。 各境界ルータでは、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。

（注）
- 境界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 つ以上の境界ルータが導入された場合、各境界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。 • パスワードを入力します（要求された場合）。
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 コントローラと境界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。

	コマンドまたはアクション	目的
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 境界ルータ コンフィギュレーション モードを開始して、ルータを境界ルータとして設定します。 • 境界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。
ステップ 9	**local** *type number* 例： `Router(config-pfr-br)# local GigabitEthernet 0/0/0`	PfR 境界ルータのローカル 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。
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 管理境界ルータ 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。

	コマンドまたはアクション	目的
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。

次の作業

ネットワークがスタティック ルーティングだけを使用するように設定されている場合、追加の設定は必要ありません。境界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働している必要があります。 その他の PfR のカスタマイズに関する情報を含むモジュールへのリンクについては、「その他の関連資料」の項を参照してください。

PfR 境界ルータ情報の表示

PfR の機能のほとんどはマスター コントローラ上で設定されますが、境界ルータがパフォーマンス情報を実際に収集し、多数の **show** コマンドを境界ルータ上で実行できます。 この作業のコマンドは、アプリケーション トラフィックが通過する境界ルータ上で入力されます。 **show** コマンドは、任意の順番で入力できます。

手順の概要

1. **enable**
2. **show pfr border**
3. **show pfr border active-probes**
4. **show pfr border passive prefixes**
5. **show pfr border routes {bgp | cce | eigrp [parent]| rwatch | static }**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr border**
PfR 境界ルータ接続および PfR 制御されたインターフェイスに関する情報を表示します。

例：

```
Router# show pfr border

OER BR 10.1.1.3 ACTIVE, MC 10.1.1.1 UP/DOWN: UP 00:57:55,
  Auth Failures: 0
  Conn Status: SUCCESS, PORT: 3949
  Exits
  Et0/0           INTERNAL
  Et1/0           EXTERNAL
```

ステップ 3 **show pfr border active-probes**

境界ルータまたはアクティブプローブを実行中の境界ルータを含む、所定のプレフィックスおよび現在のプローブ状態に対するターゲットのアクティブ プローブ割り当てを表示します。 次に、それぞれが異なるプレフィックスに対して設定されている 3 つのアクティブ プローブの例を示します。 ターゲット ポート、発信元 IP アドレス、および出口インターフェイスが出力に表示されています。

例：

```
Router# show pfr border active-probes

OER Border active-probes
Type      = Probe Type
Target    = Target IP Address
TPort     = Target Port
Source    = Send From Source IP Address
Interface = Exit interface
Att       = Number of Attempts
Comps   = Number of completions
N - Not applicable
Type     Target          TPort Source          Interface           Att   Comps
udp-echo 10.4.5.1           80 10.0.0.1        Et1/0                 1       0
tcp-conn 10.4.7.1           33 10.0.0.1        Et1/0                 1       0
echo     10.4.9.1            N 10.0.0.1        Et1/0                 2       2
```

ステップ 4 **show pfr border passive prefixes**

このコマンドは、PfR の監視対象プレフィックスおよびトラフィック フローについて NetFlow によって収集されたパッシブ測定情報を表示するのに使用されます。 次の出力は、**show pfr border passive prefixes** コマンドが実行された境界ルータについて NetFlow によってパッシブ モニタリングが行われたプレフィックスを示します。

例：

```
Router# show pfr border passive prefixes

OER Passive monitored prefixes:
Prefix          Mask   Match Type
10.1.5.0        /24     exact
```

ステップ 5 **show pfr border routes {bgp | cce | eigrp [parent]| rwatch | static }**

このコマンドは、境界ルータ上の PfR 制御対象ルートに関する情報を表示するために使用します。 次に、境界ルータ上の EIGRP 制御対象ルートと、EIGRP ルーティング テーブルにある親ルートに関する情報を表示する例を示します。 この例の出力では、PfR によって制御される 10.1.2.0/24 プレフィックスが示されます。 このコマンドは、EIGRP ルーティング テーブルで親ルートが特定された場合に、親ルートの検索と既存の親ルートへのルート変更を表示するときに使用されます。

例：

```
Router# show pfr border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact
Flags Network            Parent            Tag
CE    10.1.2.0/24        10.0.0.0/8        5000
```

PfR 境界ルータ専用機能の設定例

PfR マスター コントローラの設定例

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。

（注） この設定は、マスター コントローラ上で実施します。 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S に含まれます。マスター コントローラ設定は使用できません。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。

```
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 の境界ルータおよび 10.200.2.2 の境界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 制御境界ルータ 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 GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 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 GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-pfr-mc)# exit
```

PfR 境界ルータの設定例

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、境界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 GigabitEthernet 1/0/0
Router(config-pfr-br)# master 192.168.1.1 key-chain PFR
Router(config-pfr-br)# end
```

関連情報

マスター コントローラと境界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、境界ルータ専用機能に関する項、「ベーシック パフォーマンス ルーティングの設定」モジュール、または「関連資料」の項に記載されているその他の関連資料で、Cisco IOS XE でサポートされている機能を参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール

関連項目	マニュアル タイトル
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR 境界ルータ専用機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *2* : *PfR* 境界ルータ専用機能の機能情報

機能名	リリース	機能情報
OER 境界ルータ専用機能	Cisco IOS XE Release 2.6.1、Cisco IOS XE Release 3.1S	パフォーマンス ルーティング（PfR）によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上での境界ルータ（BR）専用機能のサポートが導入されました。境界ルータ専用機能をサポートするソフトウェア イメージでは、マスター コントローラ設定は使用できません。 この状況で境界ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M を実行するルータでなければなりません。他のプラットフォーム上の境界ルータ専用機能と異なり、Cisco ASR 1000 シリーズ ルータでは境界ルータ パッシブ モニタリング機能をアクティブ モニタリング機能と同様にフルに提供できます。 PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 この機能により、次のコマンドが導入または変更されました。**show pfr border**、**show pfr border active-probes**、**show pfr border passive prefixes**、**show pfr border routes**。

パフォーマンス ルーティング コンフィギュレーション ガイド、**Cisco IOS XE Release 3S**（**Cisco ASR 1000**）

第 3 章

パフォーマンス ルーティングの理解

このモジュールでは、パフォーマンス ルーティング（PfR）がどのように動作するかを説明し、ユーザが自身のネットワークにこのテクノロジーを実装する方法を理解できるようにします。設定後、PfRテクノロジーは一連のフェーズを通過します。これらのフェーズはトラフィック クラスのプロファイリングで始まり、トラフィック クラスの測定、トラフィック クラスへのポリシーの適用、ポリシーの条件に合わせたトラフィック クラスの制御を経て、最後にトラフィック クラス最適化の結果が検証されます。

（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、『Optimized Edge Routing Configuration Guide』を参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンスルーティングを理解するための前提条件

- 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 Cisco IOS XE Release 3.1S および 3.2S イメージで境界ルータとして使用されている Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラ設定はサポートされます。
- PfR フェーズを理解するには、PfR の動作原理と基本的な PfR ネットワーク コンポーネントのセットアップ方法について概要を把握しておく必要があります。 詳細については、「Configuring Basic Performance Routing」モジュールを参照してください。
- 参加するすべてのデバイスでシスコ エクスプレス フォワーディング（CEF）を有効にする必要があります。 その他のスイッチング パスは、ポリシーベース ルーティング（PBR）でサポートされている場合でもサポートされません。

パフォーマンス ルーティングを理解するための概要

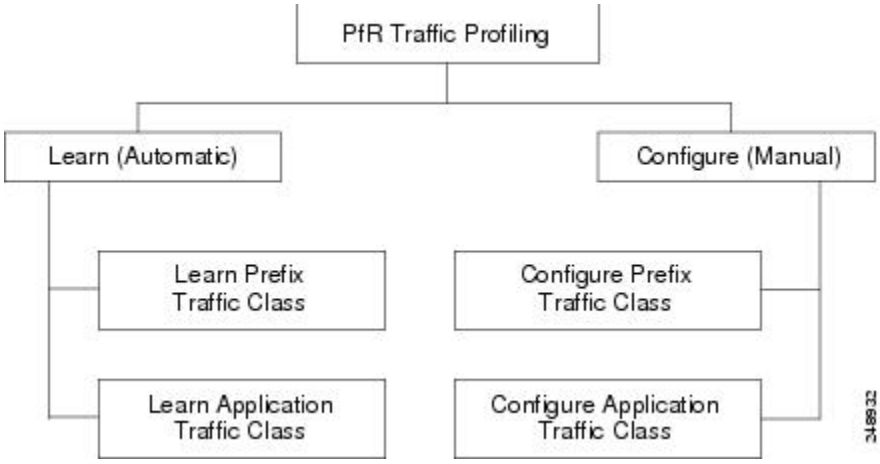
プロファイル フェーズの概念

トラフィック クラスのプロファイリングの概要

トラフィックを最適化する前に、PfR は境界ルータを通過するトラフィックからトラフィック クラスを判断する必要があります。トラフィック ルーティングを最適化するには、全トラフィックのサブセットを識別する必要があります。これらのトラフィック サブセットをトラフィック クラスと呼びます。 トラフィック クラスのエントリのリストには、監視対象トラフィック クラス（MTC）リストという名前が付けられています。デバイスを経由したトラフィックを自動的に学習するか、トラフィック クラスを手動で設定することによって、MTC リスト内のエントリのプロファイリングを行うことができます。学習されたトラフィック クラスと設定されたトラフィック クラスの両方が、同時に MTC リストに存在する場合があります。 PfR プロファイル フェーズに

は、学習メカニズムと設定メカニズムの両方が含まれます。 PfR トラフィック クラスのプロファイリング プロセスの全体構造とコンポーネントは次の図で確認できます。

図 *4*：*PfR* トラフィック クラスのプロファイリング プロセス



このフェーズの最終的な目的は、ネットワークを通過するトラフィックのサブセットを選択することです。 このトラフィックのサブセット（MTC リスト内のトラフィック クラス）は、使用可能な最良のパフォーマンス パスに基づいてルーティングする必要のあるトラフィックのクラスを表します。

自動トラフィック クラス学習

PfR は、境界ルータを通過するトラフィックを監視しながら、トラフィック クラスを自動的に学習します。 目的はトラフィックのサブセットを最適化することですが、このトラフィックの正確なパラメータをすべて把握できるわけではないので、PfR にはトラフィックを自動的に学習し、MTC リストに入力することによってトラフィック クラスを作成する方法が用意されています。初回リリース以降、複数の機能が PfR に追加され、自動トラフィック クラス学習プロセスの機能は強化されています。

自動トラフィック クラス学習プロセスには、現在 3 つのコンポーネントがあります。 1 つめのコンポーネントではプレフィックスベースのトラフィック クラスの自動学習、2 つめのコンポーネントではアプリケーションベースのトラフィック クラスの自動学習が規定されています。3 つめのコンポーネントでは、学習リストを使用してプレフィックスベースとアプリケーションベースの両方のトラフィック クラスを分類する方法が規定されています。 この 3 つのコンポーネントについては、次の項で説明します。

PfR を使用したプレフィックス トラフィック クラスの学習

NetFlow Top Talker 機能を使用して、最大のアウトバウンド スループットまたは最大の遅延時間に基づいてプレフィックスを自動的に学習するように PfR マスター コントローラを設定できます。 スループットの学習では、最大のアウトバウンド トラフィック ボリュームを生成するプレフィックスを判定します。 スループット プレフィックスは高い順にソートされます。 遅延学習

では、ラウンドトリップ応答時間（RTT）が最大のプレフィックスを判定し、これらのプレフィックスの RTT を低減するために、最大遅延プレフィックスを最適化します。 遅延プレフィックスは、遅延時間の長い順にソートされます。

PfR は、次の 2 種類のプレフィックスを自動的に学習できます。

- 外部プレフィックス：外部プレフィックスは、社外で割り当てられたパブリック IP プレフィックスとして定義されています。 外部プレフィックスは他のネットワークから受信します。
- 内部プレフィックス：内部プレフィックスは、社内で割り当てられたパブリック IP プレフィックスとして定義されています。 内部プレフィックスは、企業ネットワーク内部で設定されたプレフィックスです。

BGP インバウンド最適化機能に、内部プレフィックスを学習する機能が追加されました。 BGP を使用すると、PfR は内部プレフィックスを選択し、自律システム外のプレフィックスから自律システム内のプレフィックス宛てに送信されるトラフィックに対する最良入口選択をサポートできます。 以前のリリースでは、外部プレフィックスだけがサポートされていました。 PfR でサポートされる内部プレフィックスの詳細については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

自動プレフィックス学習は、PfR Top Talker/Top Delay 学習コンフィギュレーション モードで設定します。 PfR マスター コントローラ コンフィギュレーション モードからこのモードに移行するには、**learn**（PfR）コマンドを使用します。 自動プレフィックス学習がイネーブルの場合、境界ルータ上でプレフィックスとその遅延またはスループット特性が測定されます。 プレフィックスベースのトラフィック クラスのパフォーマンス測定値はマスター コントローラにレポートされ、学習済みプレフィックスは MTC リストに保存されます。

組み込みの NetFlow 機能を使用してトラフィック フローを監視することで、境界ルータ上でプレフィックスが学習されます。 すべての着信および発信トラフィック フローが監視されます。 デフォルトでは上位 100 フローが学習されますが、各学習サイクルにつき最大 2,500 フローを学習するようにマスター コントローラを設定できます。

学習したプレフィックスをタイプ（BGP、または非 BGP（スタティック））に基づいて集約するように、マスター コントローラを設定できます。プレフィックスは、プレフィックス長に基づいて集約できます。 デフォルトでは、/24 プレフィックス長を使用してトラフィック フローが集約されます。 プレフィックスの集約は、単一のホスト ルート（/32）から主要なネットワーク アドレス範囲にいたるまで、ネットワークの任意のサブセットまたはスーパーセットを含めるように設定できます。 集約された各プレフィックスに対し、最大 5 個のホスト アドレスを選択してアクティブ プローブ ターゲットとして使用できます。 プレフィックスの集約は、PfR Top Talker/Top Delay 学習コンフィギュレーション モードで **aggregation-type**（PfR）コマンドを使用して設定します。

PfR を使用したアプリケーション トラフィック クラスの学習

PfR はレイヤ 3 プレフィックスを学習でき、プロトコルまたはポート番号などのレイヤ 4 オプションはフィルタとしてプレフィックスベースのトラフィック クラスに追加できます。プロトコルとポート番号を使用して、特定のアプリケーション トラフィック クラスを識別できます。プロトコルおよびポート番号パラメータは、プレフィックスのコンテキストの中だけで監視され、マスター

コントローラ データベース（MTC リスト）には送信されません。 そのあと、特定のトラフィックを伝送するプレフィックスが、マスター コントローラによって監視されます。 PfR アプリケーション トラフィック クラスの学習は、プロトコルとポート番号のほか、DiffServ コード ポイント（DSCP）値もサポートしており、これらのレイヤ 4 オプションは MTC リストに入力されます。

PfR による DSCP 値、ポート、およびプロトコルの学習

PfR では、DSCP 値、ポート番号、またはプロトコルごとにアプリケーション トラフィックをフィルタリングして集約できます。 トラフィック クラスは、プロトコル、ポート番号、および DSCP 値で構成されるキーの組み合わせによって定義されます。 不要なトラフィックをフィルタリングする機能と、必要なトラフィックを集約する機能が追加されました。 プロトコル、ポート番号、DSCP 値などの情報は、プレフィックス情報と共にマスター コントローラ データベースに送信されるようになりました。 この新しい機能により、PfR によるアプリケーション トラフィックのアクティブ モニタリングおよびパッシブ モニタリングの両方が可能になりました。 新しい CLI とアクセス リストを使用して、アプリケーション トラフィック クラスを自動的に学習するように PfR を設定できます。

学習リスト コンフィギュレーション モード

PfR は、トラフィック クラスの学習を簡略化するために、学習リスト コンフィギュレーション モードをサポートしています。 学習リストは、学習したトラフィック クラスを分類する手段です。 各学習リストでは、プレフィックス、アプリケーションの定義、フィルタ、および集約パラメータなど、トラフィック クラスを学習するためのさまざまな基準を設定できます。 トラフィック クラスは、PfR によって各学習リスト基準に基づいて自動的に学習されます。各学習リストには、シーケンス番号が設定されます。 シーケンス番号によって、適用される学習リスト基準の順番が決定します。 学習リストごとに異なる PfR ポリシーを適用できます。以前のリリースではトラフィック クラスを分類することはできず、1 つの PfR ポリシーが、学習されたすべてのトラフィック クラスに適用されていました。

学習リスト コンフィギュレーション モードでは、**traffic-class** コマンドを使用してトラフィック クラスの学習が簡略化されます。 自動的に学習される 4 種類のトラフィック クラスのプロファイリングを行うことができます。

- 送信先プレフィックスに基づいたトラフィック クラス
- アクセス リストを使用してカスタム アプリケーションの定義を示すトラフィック クラス
- 送信先プレフィックスを定義するオプションのプレフィックス リスト付きのスタティック アプリケーション マッピング名に基づいたトラフィック クラス
- 送信先プレフィックスを定義するオプションのプレフィックス リスト付きの NBAR アプリケーション マッピング名に基づいたトラフィック クラス

学習リストごとに指定できる **traffic-class** コマンドのタイプは 1 つだけです。**throughput**（PfR）コマンドと **delay**（PfR）コマンドも、学習リスト内で同時に使用することはできません。

PfR を使用したスタティック アプリケーション マッピング

スタティック アプリケーション マッピング機能に、キーワードを使用してアプリケーションを定義できる機能が追加され、アプリケーションベースのトラフィック クラスの設定が簡略化されました。 PfR では、よく知られているアプリケーションと固定ポートを使用します。複数のアプリケーションを同時に設定することもできます。 スタティック アプリケーション マッピングの詳細については、パフォーマンス ルーティングを使用したスタティック アプリケーション マッピング機能を参照してください。

NBAR を使用した PfR アプリケーション マッピング

PfR では、NBAR を使用してアプリケーションベース トラフィック クラスをプロファイリングする機能がサポートされます。 ネットワークベース アプリケーション認識（NBAR）は、Web ベースやその他の動的な TCP/UDP ポート割り当てを使用する分類困難なアプリケーションおよびプロトコルを含む、多様なプロトコルおよびアプリケーションを認識して分類する分類エンジンです。 PfR では NBAR を利用して、プロトコルまたはアプリケーションを認識し、分類します。分類されたトラフィック クラスは、PfR アプリケーション データベースに追加され、パッシブ モニタリングおよびアクティブ モニタリングの対象となります。 NBAR を使用した PfR アプリケーション マッピングの詳細については、NBAR/CCE アプリケーション認識を使用したパフォーマンス ルーティング機能を参照してください。

トラフィック クラスの手動設定

モニタリングや後続の最適化用にトラフィック クラスを作成するよう、PfR を手動で設定することができます。 自動学習では通常、デフォルトのプレフィックス長 /24 が使用されますが、手動設定では正確なプレフィックスを定義することができます。 手動のトラフィック クラス設定プロセスには、2 つのコンポーネントがあります。1 つはプレフィックスベースのトラフィック クラスの手動設定、もう 1 つはアプリケーションベースのトラフィック クラスの手動設定です。これらのコンポーネントについては次の項で説明します。

PfR を使用したプレフィックス トラフィック クラスの設定

PfR モニタリングの対象となるプレフィックスまたはプレフィックス範囲を選択するには、IP プレフィックス リストを設定します。 そのあと PfR マップで match 句を設定し、IP プレフィックス リストを MTC リストにインポートします。 PfR マップは IP ルート マップと似ています。 IP プレフィックス リストは **ip prefix-list** コマンドを使用して設定し、PfR マップはグローバル コンフィギュレーション モードで **pfr-map** コマンドを使用して設定します。

PfR では、プレフィックス リスト構文は通常のルーティングとは若干異なる方法で動作します。**ge** キーワードは使用されません。**le** キーワードは、包含プレフィックスだけを指定するために PfR によって使用されます。プレフィックス リストを使用して、正確なプレフィックスを指定することもできます。

マスター コントローラは、デフォルト ルートを含む任意の長さの、完全に一致するプレフィックスを監視し、制御できます。 完全に一致するプレフィックスが指定される場合、PfR は、この完全に一致するプレフィックスだけを監視します。

マスター コントローラは、**le** キーワードと 32 に設定された *le-value* 引数を使用して包含プレフィックスを監視および制御できます。 PfR は、設定されたプレフィックスおよびより限定されたプレフィックス（たとえば、10.0.0.0/8 le 32 プレフィックスを設定すると、10.1.0.0/16 プレフィックスおよび 10.1.1.0/24 プレフィックスを含みます）を同じ出口で監視し、この情報をルーティング情報ベース（RIB）に記録します。

（注） PfR の一般的な導入では、包含プレフィックス オプションは慎重に使用してください。なぜなら、監視および記録するプレフィックスの量が増える可能性があるからです。

deny 文が含まれた IP プレフィックス リストを使用すると、学習済みトラフィック クラスのプレフィックスまたはプレフィックス長を除外するようにマスター コントローラを設定できます。 最良のパフォーマンスを得るには、最も低い PfR マップ シーケンス内で deny プレフィックス リスト シーケンスを割り当てる必要があります。 マスター コントローラの設定では、アクセス リストを使用して不要なトラフィックをフィルタリングするよう境界ルータに指示することもできます。

（注） deny 文が含まれた IP プレフィックス リストは、学習済みのトラフィック クラスだけに適用できます。

次の 2 種類のプレフィックスを使用して、IP プレフィックス リストを使用した PfR モニタリングを手動で設定できます。

- 外部プレフィックス：外部プレフィックスは、社外で割り当てられたパブリック IP プレフィックスとして定義されています。 外部プレフィックスは他のネットワークから受信します。
- 内部プレフィックス：内部プレフィックスは、社内で割り当てられたパブリック IP プレフィックスとして定義されています。 内部プレフィックスは、企業ネットワーク内部で設定されたプレフィックスです。

BGP インバウンド最適化機能に、内部プレフィックスを手動で設定する機能が追加されました。 BGP を使用すると、内部プレフィックスを選択するように PfR を設定して、自律システム外のプレフィックスから自律システム内のプレフィックス宛てに送信されるトラフィックに対する最良の入口選択をサポートできます。 以前のリリースでは、外部プレフィックスだけがサポートされていました。

PfR でサポートされる内部プレフィックスの詳細については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

PfR を使用したアプリケーション トラフィック クラスの設定

PfR は、PfR プロファイル フェーズにおけるレイヤ 3 プレフィックスの手動設定をサポートしています。 ポリシーベース ルーティング（PBR）用にアプリケーション アウェア ルーティングもサポートされます。 アプリケーション アウェア ルーティングでは、名前付き拡張 IP アクセス コントロール リスト（ACL）を使用してレイヤ 3 宛先アドレスを指定するほか、IP パケット ヘッ

ダーの値に基づいて特定のアプリケーションのトラフィックを選択できます。 サポートされるのは名前付き拡張 ACL だけです。 拡張 ACL は permit 文を使用して設定されたあと、PfR マップで参照されます。 プロトコルとポート番号を使用して、特定のアプリケーション トラフィック クラスを識別できます。ただし、プロトコルおよびポート番号パラメータは、プレフィックスのコンテキストの中だけで監視され、MTC リストには送信されません。 特定のアプリケーション トラフィックを伝送するプレフィックスだけが、マスター コントローラによってプロファイルされます。 アプリケーション アウェア ルーティングがサポートされたことにより、アプリケーション トラフィックのアクティブ モニタリングがサポートされました。アプリケーション トラフィックのパッシブ モニタリングもサポートされています。 アプリケーション トラフィック クラスは、DSCP値、プロトコル、およびポート番号を使用して定義できます。 MTC リストには、プレフィックスのほか、DSCP 値、ポート番号、プロトコルも保存されます。

学習リスト コンフィギュレーション モードでは、PfR マップ コンフィギュレーション モードの **match traffic-class** コマンドを使用して、トラフィック クラスの設定を簡略化します。 手動で設定する 4 種類のトラフィック クラスのプロファイリングを行うことができます。

- 送信先プレフィックスに基づいたトラフィック クラス
- アクセス リストを使用してカスタム アプリケーションの定義を示すトラフィック クラス
- スタティック アプリケーション マッピング名と送信先プレフィックスを定義するためのプレフィックス リストに基づくトラフィック クラス
- NBAR アプリケーション マッピング名と送信先プレフィックスを定義するためのプレフィックス リストに基づくトラフィック クラス

PfR マップごとに指定できる **match traffic-class** コマンドのタイプは 1 つだけです。

一連の既知のアプリケーションにはスタティック ポートが定義されており、キーワードを入力するとそれぞれのアプリケーションを定義できます。 スタティック アプリケーション マッピングの詳細については、パフォーマンス ルーティングを使用したスタティック アプリケーション マッピング機能を参照してください。

PfR では、NBAR を使用してアプリケーション ベース トラフィック クラスをプロファイリングする機能がサポートされます。 NBAR は、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。たとえば、ダイナミック TCP/UDP ポート割り当てを使用する Web ベースや他の分類が困難なアプリケーションとプロトコルなどです。 PfR では NBAR を利用して、プロトコルまたはアプリケーションを認識し、分類します。分類されたトラフィック クラスは、PfR アプリケーション データベースに追加され、パッシブ モニタリングおよびアクティブ モニタリングの対象となります。 NBAR を使用した PfR アプリケーション マッピングの詳細については、NBAR/CCE アプリケーション認識を使用したパフォーマンス ルーティング機能を参照してください。

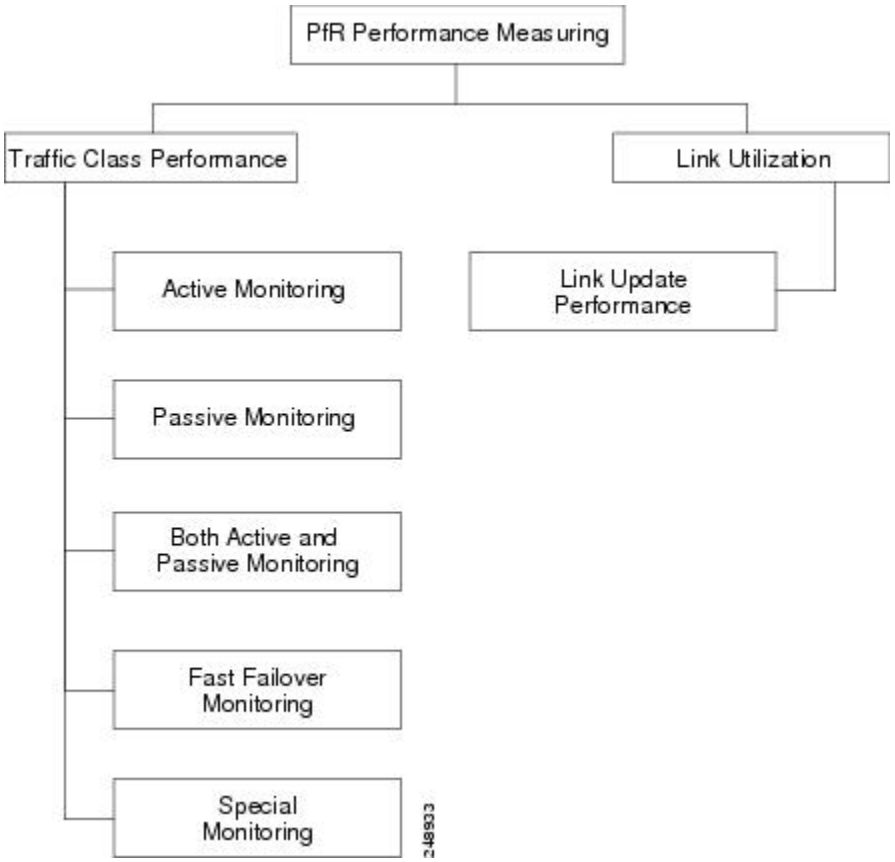
測定フェーズの概念

トラフィック クラス パフォーマンス測定の概要

PfR 測定フェーズは、トラフィック クラス エントリが Monitored Traffic Class（MTC）リストに入力される PfR プロファイル フェーズに続く、PfR パフォーマンス ループにおける 2 番目のステップです。 MTC リストにトラフィック クラス エントリが入力されると、PfR はこれらのトラフィック クラス エントリのパフォーマンス メトリックを測定する必要があります。 ここでいうモニタリングは、一定の時間間隔で定期的に行われ、測定値としきい値が比較される測定処理として定義されています。 PfR は、アクティブおよびパッシブ モニタリング手法を使用してトラフィック クラスのパフォーマンスを測定しますが、デフォルトではリンクの使用率も測定します。 学習済みおよび設定済みのトラフィック クラスを監視するように、マスター コントローラを設定することができます。 境界ルータはパッシブおよびアクティブ モニタリング統計情報を収集し、この情報をマスター コントローラに送信します。 MTC リスト内の各トラフィック クラス エントリにパフォーマンス メトリック測定値が関連付けられると、PfR 測定フェーズは終了します。

PfR 測定フェーズの全体構造とコンポーネントは次の図で確認できます。

図 *5*：*PfR* パフォーマンス測定プロセス



PfR は、トラフィック クラスとリンクの両方のパフォーマンスを測定しますが、トラフィック クラスまたはリンクをモニタリングする前に、その状態を確認します。 PfR は、トラフィック クラスの状態遷移図に従って動作するポリシー デシジョン ポイント（PDP）を使用します。

トラフィック クラスまたはリンクの状態を判定したら、PfR は次に示すパフォーマンス測定プロセスのいずれかを開始できます。

トラフィック クラス パフォーマンス測定手法

PfR は、次の 3 つのトラフィック クラス パフォーマンス測定手法を使用します。

- パッシブ モニタリング：トラフィックが NetFlow 機能を使用してデバイスを通過する間に、トラフィック クラス エントリのパフォーマンス メトリックを測定します。
- アクティブ モニタリング：トラフィック クラスをできる限り忠実に再現して合成トラフィックのストリームを作成し、その合成トラフィックのパフォーマンス メトリックを測定します。 合成トラフィックのパフォーマンス メトリック測定結果は、MTC リスト内のトラフィック クラスに適用されます。 アクティブ モニタリングでは、統合された IP サービス レベル契約（SLA）機能が使用されます。
- アクティブ モニタリングとパッシブ モニタリングの両方：ネットワーク内のトラフィック フローをより正確に把握するために、アクティブ モニタリングとパッシブ モニタリングを組み合わせます。

高速フェールオーバー モニタリング モードは、アクティブおよびパッシブ モニタリング モードのもうひとつの組み合わせです。 高速フェールオーバー モニタリング モードでは、アクティブ モニタリングとパッシブ モニタリングを使用して、すべての出口が継続的にプローブされます。 高速フェールオーバーモニタリングモードがイネーブルの場合、プローブの頻度を他のモニタリング モードよりも低く設定すると、より迅速なフェールオーバー機能を実現できます。

明示的な NetFlow または IP SLA 設定は必要なく、NetFlow および IP SLA のサポートは自動的にイネーブルになります。 1 つのトラフィック クラスに対し、アクティブおよびパッシブの両方のモニタリング手法を使用できます。

マスター コントローラが定義され、PfR 機能がイネーブルになると、マスター コントローラはデフォルトによりアクティブ モニタリングとパッシブ モニタリングの両方を使用します。 すべてのトラフィック クラスは、統合 NetFlow 機能を使用してパッシブに監視されます。 ポリシー違反のトラフィック クラスは、IP SLA 機能を使用してアクティブに監視されます。 マスター コントローラは、パッシブモニタリングだけ、アクティブモニタリングだけ、パッシブおよびアクティブモニタリング、または、高速フェールオーバーモニタリングを使用するように設定できます。 各種モードの主な違いは次の表で確認できます。

表 *3*：モード比較表

比較パラメータ	アクティブモード	パッシブ モード	複合モード	高速フェールオーバー モード
アクティブ/IP SLA	Yes	No	Yes	Yes

比較パラメータ	アクティブモード	パッシブ モード	複合モード	高速フェールオーバー モード
パッシブ/NetFlow	No	Yes	Yes	Yes
代替パスのモニタリング	オンデマンド	オンデマンド	オンデマンド	常時
最良のフェールオーバー時間	10 秒	1 分以内	1.1 分以内	3 秒
ラウンドトリップ遅延のサポート	Yes	Yes	Yes	Yes
損失に対するサポート	ジッタープローブ限定	TCP トラフィック限定	TCP トラフィック限定	TCP トラフィックおよびジッタープローブ限定
到達可能性のサポート	Yes	TCP トラフィック限定	TCP トラフィック限定	Yes
ジッターのサポート	Yes	No	No	Yes
MOS のサポート	Yes	No	No	Yes

パッシブ モニタリング

Cisco IOS PfR は、Cisco IOS ソフトウェアの統合テクノロジーである NetFlow を使用して、トラフィック クラスごとにパッシブ モニタリング統計情報を収集、集約します。 PfR 管理ネットワークが作成されると、デフォルトによりパッシブ モニタリングとアクティブ モニタリングが共にイネーブルになります。 パッシブ モニタリングは、**mode monitor passive** コマンドを使用して明示的にイネーブルにすることもできます。 Netflow はフローベースのモニタリングおよびアカウンティング システムで、パッシブ モニタリングがイネーブルになると、デフォルトにより境界ルータの Netflow サポートがイネーブルになります。

パッシブ モニタリングは既存のトラフィックだけを使用し、追加のトラフィックは生成されません。 境界ルータは、パッシブ モニタリング統計情報を収集し、1 分間に約 1 回の頻度でマスター コントローラに情報をレポートします。 トラフィックが境界ルータの外部インターフェイスを通過しない場合、データはマスター コントローラにレポートされません。 しきい値の比較はマスター コントローラで実行されます。 パッシブ モニタリングでは、プレフィックス、ポート、プロトコル、および DSCP 値で定義されたトラフィック クラスがサポートされます。

PfR はパッシブ モニタリングを使用して、すべてのトラフィック クラスについて次のメトリックを測定します。

- 遅延：PfR は所定のプレフィックスについて、TCP フローの平均遅延を測定します。 遅延とは、TCP 同期メッセージが送信されてから TCP 受信確認が受信されるまでの、ラウンドトリップ応答時間（RTT）の測定値です。
- パケット損失：PfR は各 TCP フローの TCP シーケンス番号をトラッキングすることによってパケット損失を測定します。 PfR は、最も大きい TCP シーケンス番号をトラッキングすることで、パケット損失を推定します。 後続のパケットが前よりも小さいシーケンス番号で受信されると、PfR はパケット損失のカウンタを増やします。 パケット損失は、100 万パケットあたりの損失パケット数で測定されます。
- 到達可能性：PfR は、TCP 受信確認を受信しないまま繰り返し送信された TCP 同期メッセージをトラッキングして、到達可能性を測定します。
- スループット：PfR は、所定の時間間隔における各トラフィック クラスの総バイト数と総パケット数を測定することで、スループットを測定します。

（注） すべてのトラフィック クラスが監視されますが、遅延、損失、および到達可能性に関する情報は TCP トラフィック フローに限定して取得されます。 スループット統計情報は、すべての非 TCP トラフィック フローについて取得されます。

プレフィックスに加えて DSCP 値、ポート番号、プロトコルも境界ルータからマスター コントローラに送信されます。 収集されたパッシブ モニタリング統計情報は、プレフィックス履歴バッファに保存されます。このバッファは、トラフィック フローが継続的かどうかに応じて、少なくとも 60 分間の情報を格納できます。 PfR はこの情報を使用して、プレフィックスがデフォルトまたはユーザ定義のポリシーに準拠しているかどうかを判断します。 トラフィック クラスのトラフィックは、ネットワーク内の 1 台の伝送デバイスを通過するので、代替パスの分析は行われません。 トラフィック クラスがポリシー違反（OOP）になり、パッシブ モニタリング モードだけがイネーブルの場合、そのトラフィック クラスは別のポイントに移動され、良好または最良の出口が見つかるまで測定が繰り返されます。 トラフィック クラスが OOP になり、パッシブおよびアクティブの両方のモニタリング モードがイネーブルの場合、すべての出口でアクティブ プローブが実行され、最良または良好な出口が選択されます。

アクティブ モニタリング

PfR パッシブ モニタリング手法によってネットワーク デバイスで過度のオーバーヘッドが発生する場合、または PfR パッシブ モニタリング モードを使用してトラフィック クラスのパフォーマンス メトリックを測定できない場合は、PfR アクティブ モニタリング手法が実行されます。 アクティブ モニタリングでは、トラフィック クラスをできる限り忠実に再現する合成トラフィックのストリームが作成されます。 合成トラフィックのパフォーマンス メトリックが測定され、その結果が MTC リストのトラフィック クラス エントリに適用されます。 アクティブ モニタリングでは、プレフィックス、ポート、プロトコル、および DSCP 値で定義されたトラフィック クラスがサポートされます。

PfR はアクティブ モニタリングを使用して、すべてのトラフィック クラスについて次のメトリックを測定します。

- 遅延：PfR は所定のプレフィックスについて、TCP、UDP、および ICMP フローの平均遅延を測定します。 遅延とは、TCP 同期メッセージが送信されてから TCP 受信確認が受信されるまでの、ラウンドトリップ応答時間（RTT）の測定値です。
- 到達可能性：PfR は、TCP 受信確認を受信しないまま繰り返し送信された TCP 同期メッセージをトラッキングして、到達可能性を測定します。
- ジッター：ジッターはパケット間の遅延がばらつくことを指します。 PfR は、複数のパケットをターゲット アドレスと所定のターゲット ポート番号に送信し、宛先に到着したパケット間の遅延を測定することで、ジッターを測定します。
- MOS：平均オピニオン評点（MOS）は、標準ベースの音声品質測定手法です。 ITU などの標準化団体によって、P.800（MOS）および P.861（Perceptual Speech Quality Measurement（PSQM））という 2 つの重要な勧告が作成されています。 P.800 は、音声品質の平均オピニオン評点を算出する方法の定義に関するものです。 MOS スコアの範囲は、最低の音声品質を表す 1 から最高を表す 5 までです。 MOS 4 は、「トール品質」音声と見なされます。

Cisco ネットワーク デバイスでの合成トラフィックの作成は、Cisco IOS IP SLA プローブを使用するとアクティブになります。 PfR は IP SLA 機能と統合され、IP SLA プローブを使用してトラフィック クラスをアクティブに監視します。 アクティブ モニタリングがイネーブルの場合、マスター コントローラは境界ルータに対し、一連のターゲット IP アドレスにアクティブ プローブを送信するよう指示します。 境界ルータは、1 つのトラフィック クラスにつき最大 5 個のターゲット ホスト アドレスにプローブ パケットを送信し、分析のためプローブ結果をマスター コントローラに送信します。

アクティブ プローブ モニタリングの期間は、最新の 5 個のプローブ結果で構成される短期、および最新の 60 個のプローブ結果で構成される長期と定義されます。

PfR で使用される IP SLA アクティブ プローブ タイプ

IP SLA は Cisco IOS ソフトウェアの組み込み機能で、これを使用すると IP アプリケーションおよびサービスの IP サービス レベルの分析、生産性の改善、運用コストの削減、ネットワークの輻輳や停止の低減などが可能になります。 IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。 Cisco ルータで使用できる IP SLA Responder を宛先デバイス上でイネーブルにすると、測定データの精度が向上します。 IP SLA の詳細については、『IP SLAs Configuration Guide』を参照してください。

設定可能なアクティブ プローブのタイプは次のとおりです。

- ICMP エコー：ターゲット アドレスに ping が送信されます。 アクティブ プローブが自動的に生成されると、PfR はデフォルトにより ICMP エコープローブを使用します。 ICMP エコープローブの設定には、ターゲット デバイスからの大きな協力を必要としません。 しかし、プローブを繰り返し行うと、ターゲット ネットワーク内で侵入検知システム（IDS）アラームが発生することがあります。 自身の管理制御下にないターゲット ネットワークで IDS が設定されている場合には、ターゲット ネットワークの管理者に通知することを推奨します。
- ジッター：ジッター プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 設定されるポート番号に関係なく、ターゲット デバイスの

リモート レスポンダはイネーブルにする必要があります。 ジッター プローブ使用時のアクティブ モニタリング用に、損失ポリシーがサポートされています。

- TCP 接続：TCP 接続プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 TCP メッセージの設定で、既知の番号である TCP ポート番号 23 以外のポート番号を使用するように指定されている場合は、リモート レスポンダをイネーブルにする必要があります。
- UDP エコー：UDP エコー プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 設定されるポート番号に関係なく、ターゲット デバイスのリモート レスポンダはイネーブルにする必要があります。

監視対象トラフィック クラスの DSCP フィールドが 0 以外の値に設定されている場合、PfR はデフォルトにより、DSCP 値を持つプローブ パケットをマークします。

トラフィック クラスに対するアクティブ プローブの作成

トラフィック クラスに対してアクティブ プローブを作成するには、プローブ タイプを特定し、そのトラフィック クラスにプローブ ターゲットを割り当てる必要があります。 PfR は、次のいずれかの手法を使用してプローブ タイプを特定します。

- 学習済みプローブ：NetFlow トップ トーカーの学習メカニズムを使用してトラフィック クラスが学習されると、アクティブ プローブが自動的に生成されます。 各トラフィック クラスに対して 5 つのターゲットが学習され、デフォルトによりアクティブ プローブが ICMP エコー プローブとして設定されます。
- 設定済みプローブ：プローブ タイプ、ターゲット アドレス、およびポートを必要に応じて指定することで、マスター コントローラでアクティブ プローブを設定することもできます。設定済みトラフィック クラスは、任意の IP SLA アクティブ プローブを使用するように設定できます。

PfR は次のいずれかの手法を使用して、トラフィック クラスにプローブ ターゲットを割り当てます。

- 最長一致：デフォルトでは、PfR は MTC リスト内で最長の照合プレフィックスを持つトラフィック クラスにプローブ ターゲットを割り当てます。 これをデフォルト プローブ割り当てと呼びます。
- 強制割り当て：PfR マップを使用して IP SLA プローブを設定できます。プローブの結果は、PfR マップに関連付けられた特定のトラフィック クラスに割り当てられます。 このようなアクティブ プローブ結果の割り当てを、強制ターゲット プローブ割り当てと呼びます。

アクティブ プローブは境界ルータから発信され、外部インターフェイスを経由して伝送されます（外部インターフェイスは、最適化されたプレフィックスの優先ルートである場合とそうでない場合があります）。 指定されたターゲットに対して外部インターフェイス経由のアクティブ プローブを作成する場合は、その外部インターフェイスを介してターゲットに到達できる必要があります。 指定されたターゲットの到達可能性をテストするために、PfR は BGP およびスタティック ルーティング テーブルで、所定のターゲットと外部インターフェイスのルート ルックアップを実行します。 Protocol Independent Route Optimization（PIRO）は、PfR で任意の IP ルーティング

情報ベース（RIB）の親ルート（完全一致ルート、またはそれより一致度が低いルート）を検索できる機能を導入しました。 まず BGP ルーティング テーブルが検索され、次にスタティック テーブル、最後に RIB が検索されます。

アクティブモニタリングモードでは、すべての境界ルータでプローブがアクティブになり、特定のトラフィック クラスにとって最良のパフォーマンス パスが検索されます。 トラフィック クラスが OOP にならない限り、そのトラフィック クラスのアクティブ プローブが再度アクティブ化されることはありません。

デフォルトでは、PfR が使用するアクティブ プローブの頻度は 60 秒に設定されています。 2 つのプローブ間の時間間隔を短く設定することで、ポリシーごとにアクティブ プローブの頻度を増やすことができます。 プローブの頻度を増やすと応答時間が短縮され、音声トラフィックの場合は、MOS 低カウント率の近似値をより正確に求めることができます。

PfR アクティブ プローブ ソース アドレス

PfR は、アクティブ プローブのソース アドレスを設定する機能をサポートしています。 デフォルトでは、アクティブ プローブはプローブを送信する PfR 外部インターフェイスのソース IP アドレスを使用します。 アクティブ プローブ ソース アドレス機能は、境界ルータで設定されます。 このコマンドが設定されると、指定されたインターフェイスのプライマリ IP アドレスがアクティブ プローブ ソースとして使用されます。 アクティブ プローブのソース インターフェイス IP アドレスは、プローブ応答が指定したソース インターフェイスに必ず戻されるようにするために、一意である必要があります。 インターフェイスに IP アドレスが設定されていない場合、アクティブ プローブは生成されません。インターフェイスがアクティブプローブのソースとして設定された後で IP アドレスが変更されると、アクティブ プローブは停止し、新しい IP アドレスで再開します。 インターフェイスがアクティブ プローブのソースとして設定された後で IP アドレスが削除されると、アクティブプローブは停止します。有効なプライマリ IP アドレスが設定されるまで再開しません。

アクティブ プローブを使用した PfR 音声トラフィック最適化

PfR では、遅延、到達可能性、ジッター、平均オピニオン評点（MOS）などの音質メトリックを基準とする、アクティブ プローブを使用した音声トラフィックのアウトバウンド最適化がサポートされます。

音声トラフィック最適化の詳細については、「アクティブプローブを使用した PfR 音声トラフィック最適化」モジュールを参照してください。

結合モニタリング

ネットワーク内のトラフィック フローをより正確に把握するために、アクティブおよびパッシブの両方のモニタリングを組み合わせるように Cisco IOS PfR を設定することもできます。 両方の PfR モニタリング モードを結合する場合、いくつかのシナリオが考えられます。

一例を挙げると、トラフィック クラスを学習するにはそれらのトラフィック クラスをパッシブに監視しますが、トラフィック クラスを制御するには代替パスのパフォーマンス メトリックも測定する必要があります。 ネットワーク内で実際に代替パスを通過するトラフィックがない場合は、アクティブ プローブを使用して代替パス パフォーマンス メトリックを測定できます。 PfR は、5

つのターゲットでトラフィック クラスを学習し、アクティブ プローブを使用してすべての代替パスをプローブすることにより、このプロセスを自動化します。

高速フェールオーバー モニタリング

高速モニタリングでは、すべての出口を継続的に監視する（probe-all）ようにアクティブ プローブが設定され、パッシブ モニタリングもイネーブルになります。 高速フェールオーバー モニタリングは、すべてのタイプのアクティブ プローブ（ICMP エコー、ジッター、TCP 接続、および UDP エコー）で使用できます。 **mode monitor fast** コマンドがイネーブルの場合、プローブの頻度を他のモニタリング モードよりも低く設定すると、より迅速なフェールオーバー機能を実現できます。 プローブ頻度を低く設定した高速モニタリング中にポリシー違反状態が発生すると、3 秒以内にルートが変更されます。 高速モニタリング中に出口が OOP になると、選択された最良の出口が動作可能になり、OOP出口からのルートは最良のポリシー準拠出口に移動されます。高速モニタリングは、継続的なプローブによって多くのオーバーヘッドが発生する、非常にアグレッシブなモードです。 高速モニタリングは、パフォーマンスに影響されやすいトラフィックだけに使用することを推奨します。 たとえば音声コールは、パフォーマンスの問題や輻輳が発生したリンクに大きく影響されます。しかし、高速モニタリング モードを使用すると、数秒でコールを検出して再ルーティングすることができます。

（注） 高速モニタリング モードでは、学習済みプレフィックスと同様に、プローブ ターゲットが学習されます。ネットワーク内で多数のプローブをトリガーしないようにするには、トラフィックがパフォーマンスに影響されやすいリアルタイム アプリケーションと重要アプリケーションにのみ、高速モニタリング モードを使用します。

リンク使用率測定手法

リンク使用率のしきい値

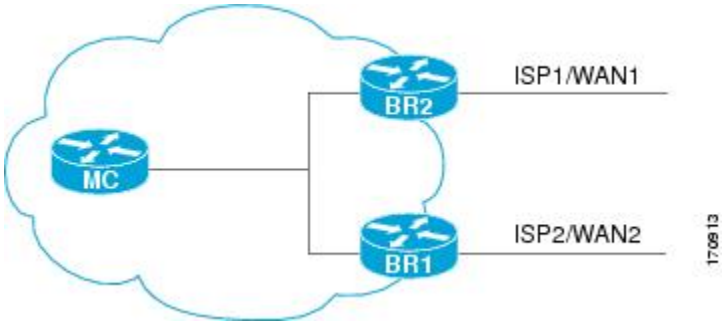
境界ルータに外部インターフェイスが設定されると、PfR は自動的に外部リンクの使用率を監視します（外部リンクは境界ルータ上のインターフェイスで、通常はWANにリンクしています）。デフォルトでは、境界ルータは 20 秒ごとにリンクの使用率をマスター コントローラにレポートします。出力（送信済み）と入力（受信済み）の両方のトラフィック使用率の値がマスターコントローラにレポートされます。出口または入口リンクの使用率がデフォルトしきい値である 75 % を超えている場合、その出口または入口リンクはOOP状態であり、PfR はトラフィック クラス用の代替リンクを検出するためにモニタリング プロセスを開始します。 リンク使用率のしきい値は、毎秒あたりのキロバイト数（kbps）で表す絶対値またはパーセンテージとして手動で設定できます。

リンク使用率範囲

また、PfR では、すべてのリンクに対する使用率の範囲を計算するよう設定することもできます。出力（送信済み）と入力（受信済み）の両方のトラフィック使用率の値がマスター コントローラにレポートされます。 次の図に、個別の ISP 経由でインターネットに接続する出口リンクを持つ

2つの境界ルータを示します。 マスター コントローラは、一方の境界ルータ（次の図の BR1 または BR2）のどのリンクをトラフィック クラスによって使用するのかを決定します。

図 *6*：*PfR* ネットワーク図



PfR 範囲機能は、確実にトラフィックの負荷を分散するために、出口または入口リンクが相互に相対的な使用率の範囲内に収まるよう動作します。 範囲は割合で指定されます。この値はマスターコントローラ上で設定され、そのマスターコントローラで管理されている境界ルータ上のすべての出口リンクまたは入口リンクに適用されます。 たとえば、範囲が 25 % として指定され、（上の図の）BR1 の出口リンクの使用率が 70 % で、（上の図の）BR2 の出口リンクの使用率が 40 % に下がった場合、2 つの出口リンクの間の割合の範囲が 25 % を上回るので、PfR は、BR1 の出口リンクを使用する一部のトラフィック クラスを移動して、トラフィック負荷を均等にしようとします。（上の図の）BR1 が入口リンクとして設定されている場合は、使用率の値が送信済みトラフィックではなく受信済みトラフィックに関するものでない限り、出口リンクの場合と同じ方法でリンク使用率範囲が計算されます。

（注） リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

ポリシー適用フェーズの概念

ポリシー適用フェーズの概要

PfR ポリシー適用フェーズは、トラフィック クラスを識別するプロファイル フェーズと、MTC リスト内の各トラフィック クラス エントリを監視してパフォーマンス メトリックを測定する測定フェーズに続く、PfR パフォーマンス ループにおける 3 番目のステップです。 ポリシー適用フェーズでは、測定されたパフォーマンス メトリックを既知のまたは設定されたしきい値と比較し、トラフィックが所定のサービス レベルを満たしているか、あるいは何らかの措置が必要かを判断します。 パフォーマンス メトリックがしきい値に適合していない場合、PfR はトラフィック クラスを移動するか、他の状態に遷移するかを決定します。

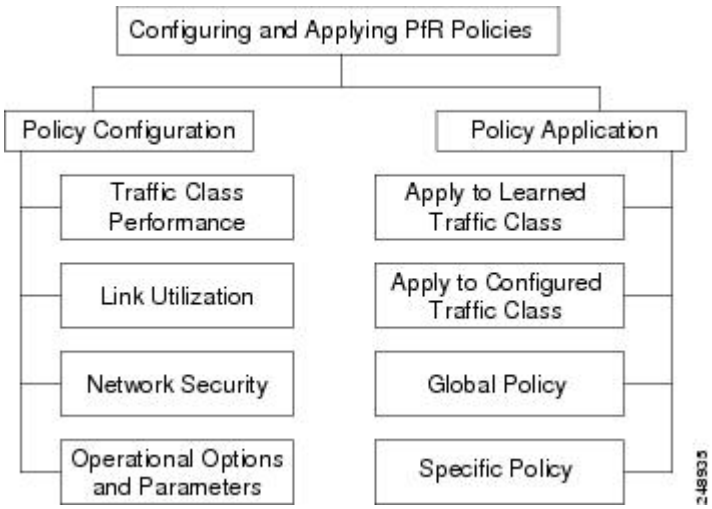
PfR ポリシーは、目的が明示されたルールであり、次の項目が含まれます。

- 範囲
- 処理
- トリガー イベントまたは条件

たとえば、特定のトラフィック クラス エントリに送信されるパケットの遅延を 100 ミリ秒以下で維持するようにポリシーを設定することができます。 この場合、範囲とは特定のトラフィック クラス エントリに送信されるネットワーク トラフィックであり、処理はルーティング テーブルの変更、トリガー イベントはこのトラフィックで測定された 100 ミリ秒を超える遅延です。 PfR がトラフィックを制御するよう PfR 制御フェーズで設定されるまでは、処理が実行されない場合があります。 プロファイル、測定、およびポリシー適用フェーズでは、PfR はデフォルトにより観察モードで実行されます。

PfR ポリシー適用フェーズでは、ポリシーの設定と適用が可能です。 異なるタイプの PfR ポリシーを設定できます。次の図を参照してください。特定の PfR パラメータおよびオプションをポリシーに含めることができます。 このマニュアルでは、パラメータとは微調整ができる設定可能要素であり、オプションとはイネーブルまたはディセーブルにする設定可能要素を指します。 PfR ポリシーを設定したら、そのポリシーを学習済みトラフィック クラスまたは設定済みトラフィック クラスに適用できます。 PfR ポリシーは、すべてのトラフィック クラスを対象としてグローバルに適用することも、一部のトラフィック クラスだけに適用することもできます。

図 *7*：*PfR* ポリシー適用フェーズの構造



上の図には、3 種類の PfR ポリシーといくつかの設定可能な動作オプションおよびパラメータが示されています。 各ポリシータイプ、パラメータ、またはオプションの詳細を確認するには、次のリンクを使用してください。

PfR ポリシーの設定後は、上の図に示すように、すべてのトラフィック クラスを対象とするグローバル ベースで、または一部のトラフィック クラスを対象に、ポリシーを学習済みトラフィック クラスまたは設定済みトラフィック クラスに適用できます。

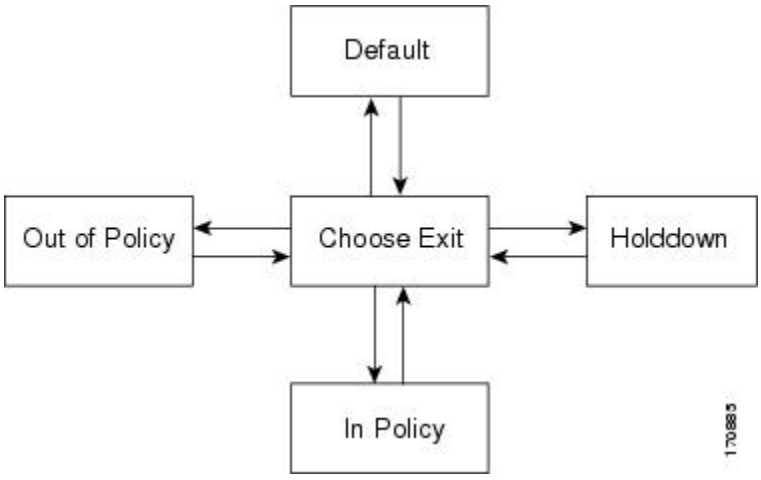
トラフィック クラスに複数のポリシー パラメータを設定する場合、複数のポリシーが重複する可能性があります。 実行するポリシーの競合を回避するために、PfR は解決機能を使用します。これは、大半のポリシー タイプにプライオリティを設定できる柔軟なメカニズムです。

PfR ポリシー デシジョン ポイント

トラフィック クラスのパフォーマンス メトリックをデフォルトまたは設定されたしきい値と比較する PfR ポリシーを実行する際、トラフィック クラスの状態が変更される場合があります。 PfR は、次の図に示すトラフィック クラスの状態遷移図に従って動作するポリシー デシジョン ポイント（PDP）を使用します。 次の図の状態遷移図には次の状態が含まれています。

- デフォルト：PfR の制御下にないとき、トラフィック クラスはデフォルト状態です。 中央のポリシー データベースである MTC に最初に追加されたとき、トラフィック クラスはデフォルト状態にあります。 トラフィック クラスは、パフォーマンス測定値、タイマー、およびポリシーの設定に応じてデフォルト状態から遷移します。
- 出口選択：これは、PDP がトラフィック クラスの現在の状態をポリシーの設定と比較し、そのトラフィック クラスに最適の出口を選択するための一時的な状態です。 PfR は現在の出口を通過するトラフィック クラスを維持しようとしますが、デフォルト状態の場合と同様に、パフォーマンス測定値、タイマー、およびポリシーの設定によって、マスター コントローラは出口リンク選択プロセス中にトラフィック クラスをこの状態に移動させる可能性があります。 トラフィック クラスは、新しい出口に移動されるまでは出口選択状態にあります。
- ホールドダウン：マスター コントローラが、プローブを使用して監視するためにトラフィック クラスを転送するよう境界ルータに要求すると、トラフィック クラスはホールドダウン状態になります。 このトラフィック クラスが使用している出口が到達不能と宣言されない限り、選択されたトラフィック クラスに関する測定値はホールドダウン タイマーが終了するまで収集されます。 出口が到達不能な場合、トラフィック クラスは出口選択状態に戻ります。

図 *8*：*PfR* トラフィック クラス状態遷移図



- ポリシー準拠：パフォーマンス測定値がデフォルトまたはユーザ定義のポリシー設定と比較され、出口が選択されると、トラフィック クラスはポリシー準拠状態になります。 ポリシー準拠状態のトラフィック クラスは、デフォルトまたはユーザ定義の設定に適合する出口から転送されます。 マスター コントローラは引き続きトラフィック クラスを監視しますが、周期タイマーが終了するか、測定コレクタからポリシー違反メッセージが受信され、トラフィック クラスが出口選択状態に戻るまで、処理は行われません。

（注） 観察モードの実行中、プレフィックスがポリシー準拠状態になるのは、そのプレフィックスに選択された出口が現在の出口である場合だけです。

- ポリシー違反（OOP）：デフォルトまたはユーザ定義のポリシーに準拠したトラフィック クラスを転送する出口がない場合、トラフィック クラスはポリシー違反状態になります。 トラフィック クラスがこの状態にある間、バックオフ タイマーがこの状態からの遷移を制御します。 トラフィック クラスがポリシー違反状態になるたびに、そのトラフィック クラスのこの状態における経過時間が増加します。 トラフィック クラスがポリシー準拠状態になると、そのトラフィック クラスのタイマーがリセットされます。 すべての出口リンクがポリシー違反の場合、マスター コントローラは使用可能な最良の出口を選択することもあります。

トラフィック クラス パフォーマンス ポリシー

PfR トラフィック クラス パフォーマンス ポリシーは、トラフィック クラスのパフォーマンス特性を管理する一連のルールです。トラフィック クラスは、ネットワーク アドレス（プレフィックス）の場合と、プロトコル、ポート番号、DSCP 値などのアプリケーション基準の場合があります。 ネットワーク アドレスは、ネットワーク内の各エンドポイント（10.1.1.1/32 など）またはサブネット全体（10.0.0.0/8 など）を参照できます。 PfR ポリシーで管理できる主なパフォーマンス特性は次のとおりです。

これらのパフォーマンス特性は、到達可能性を除き、従来のルーティング プロトコル メトリックの構造では管理できません。 Cisco PfR は、指定されたパスで宛先に到達できるかどうかを自動的に検証することで、到達可能性の（ルーティング テーブルに特定のルートを確保するという）概念を拡大します。 Cisco PfR では、ネットワーク管理者はトラフィック フローを管理するための新しく強力なツールセットを使用できます。

到達可能性

到達可能性は、PfR がトラフィック クラス エントリから許可する到達不能ホストの相対割合（%）、または 100 万フローあたりの到達不能数（fpm）に基づく絶対最大数として指定されます。 到達不能ホストの絶対数または相対割合がユーザ定義またはデフォルトの値を超える場合、PfR そのはトラフィック クラス エントリをポリシー違反と見なし、代替出口リンクを探します。

到達可能性のパラメータを設定するには、**unreachable**（PfR）コマンドを使用します。 このコマンドには **relative** と **threshold** という 2 つのキーワードがあります。 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。 到達不能ホストの相対割合は、短期測定値およ

び長期測定値の比較に基づいています。 短期測定値には、5 分以内に到達できないホストの割合が反映されます。 長期測定値には、60 分以内に到達できないホストの割合が反映されます。 この値の計算には次の式が使用されます。

到達不能ホストの相対割合 = ((短期割合 - 長期割合) / 長期割合) * 100

マスター コントローラは、割合で表されるこれら 2 つの値の差異を測定します。 この割合がユーザ定義またはデフォルトの値を超えると、トラフィック クラスエントリはポリシー違反と見なされます。 たとえば、長期測定で 10 台、短期測定で 12 台のホストが到達不能な場合、到達可能ホストの相対割合は 20 % です。

threshold キーワードは、到達不能ホストの絶対最大数の設定に使用します。 この最大数は、fpm に基づく到達不能な実際のホスト数に基づいています。

遅延

遅延（レイテンシともいう）は、パケットが送信元デバイスから送信されて宛先デバイスに到着するまでの遅れとして定義されています。 遅延は、一方向遅延またはラウンドトリップ遅延として測定されます。 レイテンシの最大の原因は、ネットワーク伝送遅延です。

PfR は、音声トラフィックに関する遅延パフォーマンス特性の定義をサポートしています。 ラウンドトリップ遅延は、通話能力に影響し、平均オピニオン評点（MOS）の計算に使用されます。 一方向遅延は、ネットワーク問題の診断に使用されます。 200 ミリ秒の遅延に気づいた発信者は、パケット遅延のため、相手の応答中に話そうとすることがあります。 ITU-T G.114 で規定されている電話業界標準では、一方向遅延の最大値を 150 ミリ秒以下にするよう推奨しています。 一方向遅延が 150 ミリ秒を超えると、音声品質に影響が出ます。 300 ミリ秒以上のラウンドトリップ遅延が発生すると、話者同士が同時に発話してしまうことがあります。

パケット損失

パケット損失は、インターフェイスの障害、パケットのルーティング先の間違い、またはネットワークの輻輳によって発生する可能性があります。

音声トラフィックのパケット損失はサービスの低下を招き、発信者には音声が途切れて聞こえます。 パケット損失の平均値が低くても、音声品質は短期間の連続するパケット損失の影響を受ける場合があります。

ジッター

PfR は、ジッター パフォーマンス特性の定義をサポートしています。 ジッターはパケット間の遅延がばらつくことを指します。 複数のパケットが発信元から宛先に連続的に送信された場合、たとえば 10 ms 間隔で送信された場合、ネットワークが理想的に動作していれば、宛先は 10 ms 間隔でパケットを受信します。 しかし、ネットワーク内に遅延（キューイング、代替ルートを介した受信など）が存在する場合、パケット間の到着遅延は、10 ms より大きい場合も、10 ms より小さい場合もあります。 この例を使用すると、正のジッター値は、パケットが 10 ms を超える間隔で到着することを示します。 パケットが 12 ms 間隔で到着する場合、正のジッターは 2 ms です。 パケットが 8 ms 間隔で到着する場合、負のジッターは 2 ms です。 VoIP のように遅延の影響を受けやすいネットワークの場合、ジッター値は正と負のいずれであっても望ましくなく、理想的なジッター値は 0 です。

平均オピニオン評点（MOS）

PfR は、MOS パフォーマンス特性の定義をサポートしています。すべての要因が音声品質に影響を与えるので、音声品質の測定方法については多くの人々が疑問を持っています。 ITU などの標準化団体によって、P.800（MOS）および P.861（Perceptual Speech Quality Measurement（PSQM））という 2 つの重要な勧告が作成されています。 P.800 は、音声品質の平均オピニオン評点を算出する方法の定義に関するものです。 MOS スコアの範囲は、最低の音声品質を表す 1 から最高を表す 5 までです。 MOS 4 は、「トール品質」音声と見なされます。

ジッターと MOS パフォーマンス特性は、遅延やパケット損失だけでなく PfR ポリシーでも設定でき、IP ネットワークでの電話品質の判断に利用できます。

PfR リンク ポリシー

PfR リンク ポリシーは、PfR が管理する外部リンクに適用される一連のルールです（外部リンクは、ネットワーク エッジにある境界ルータのインターフェイスです）。 リンク ポリシーでは、目的とするリンクのパフォーマンス特性を定義します。 トラフィック クラス パフォーマンス ポリシーのように、リンクを使用する個々のトラフィック クラスエントリのパフォーマンスを定義するのではなく、リンク ポリシーではリンク全体のパフォーマンスを定義します。 リンク ポリシーは、出口（出力）リンクと入口（入力）リンクに適用できます。リンク ポリシーで管理されるパフォーマンス特性は次のとおりです。

- トラフィック負荷（使用率）
- 範囲
- コスト

トラフィックの負荷

トラフィック負荷（使用率とも呼ばれます）ポリシーは、特定のリンクで伝送できるトラフィック量に関する上限しきい値で構成されます。 Cisco IOS PfR は、トラフィック クラスごとの負荷分散をサポートします。 境界ルータに外部インターフェイスが設定されると、境界ルータはデフォルトにより、20 秒ごとにリンク使用率をマスター コントローラに報告します。 出口リンクおよび入口リンクのトラフィック負荷しきい値は PfR ポリシーとして設定できます。 出口または入口リンク使用率が、設定されたしきい値またはデフォルトしきい値である 75％を超えている場合、その出口または入口リンクは OOP 状態であり、PfR はトラフィック クラス用の代替リンクを検出するためにモニタリング プロセスを開始します。 リンク使用率のしきい値は、キロビット毎秒（kbps）で表す絶対値またはパーセンテージとして手動で設定できます。 各インターフェイスの負荷使用率ポリシーは、マスター コントローラで境界ルータを設定する際に設定します。

ヒント　負荷分散を設定する場合は、**load-interval**（PfR）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、外部インターフェイスでのインターフェイス負荷計算の間隔を 30 秒に設定することを推奨します。デフォルトの計算間隔は300秒です。負荷計算は、インターフェイス コンフィギュレーション モードの境界ルータで設定します。 この設定は必須ではありませんが、Cisco IOS PfR ができる限り迅速に負荷分散に対応できるよう、これを設定しておくことを推奨します。

範囲

範囲ポリシーは、確実にトラフィックの負荷が分散されるよう、すべてのリンクを相互に相対的な一定の使用率の範囲内で維持するために定義します。 たとえば、ネットワークに複数の出口リンクがあり、いずれかのリンクを優先する財務上の理由がない場合、最善の選択はすべてのリンクに負荷を均一に分散することです。従来のルーティングプロトコルによる負荷共有では、必ずしも均一に負荷が分散されるわけではありません。なぜなら、負荷共有はフローベースであり、パフォーマンスまたはポリシー ベースではないからです。 Cisco PfR 範囲機能を使用すると、一連のリンクにおけるトラフィック使用率が所定の割合の範囲内で相互に維持されるように PfR を設定できます。 リンク間の差異が大きくなりすぎると、PfR は使用可能なリンク間にトラフィック クラスを分散し、リンクをポリシー準拠状態に戻そうとします。 デフォルトでは、マスター コントローラは PfR が管理するすべてのリンクに対して最大範囲使用率を 20 % に設定しますが、使用率の範囲は最大割合値を使用して設定できます。 出口リンクおよび入口リンクの使用率範囲は PfR ポリシーとして設定できます。

（注）　リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

コスト

コストベース最適化を使用すると、ネットワーク内の各出口リンクの金銭的コスト（ISP サービス レベル契約（SLA））に基づいてポリシーを設定できます。 PfR コストベース最適化を実装するには、帯域幅使用率の費用効果が最も高い出口リンクからトラフィックを送信し、なおかつ目的とするパフォーマンス特性は維持するようにマスター コントローラを設定します。

コストベース最適化は、固定または階層的な課金方法を使用して課金されるリンクに適用でき、コストベースのロードバランシングも実行できます。設定の詳細は、「パフォーマンス ルーティング コスト ポリシーの設定」モジュールを参照してください。

PfR リンクのグループ化

パフォーマンス ルーティング - リンク グループ機能に、出口リンクのグループを PfR 用の優先リンク セットまたはフォールバック リンク セットとして定義し、PfR ポリシーで指定されたトラ

フィック クラスを最適化する際に使用できるようにする機能が導入されました。 現在PfRは、ポリシーで指定されたプリファレンスと、指定リンク外のパスでのトラフィック クラスのパフォーマンス（到達可能性、遅延、損失、ジッター、MOSなどのパラメータを使用）に基づいて、トラフィック クラスに最良のリンクを選択しています。 最良リンクの選択では、帯域幅の使用率、コスト、リンクの範囲を考慮することもできます。 リンクのグループ化に使用される手法では、1つ以上のトラフィック クラスに対する優先リンクをPfR ポリシーで指定し、プライマリ リンク グループと呼ばれる優先リンクのリストにある最良リンクを介してトラフィック クラスがルーティングされるようにします。プライマリ グループに所定のポリシーとパフォーマンス要件を満たすリンクがない場合は、フォールバック リンク グループを指定することもできます。 プライマリ グループ リンクを使用できない場合、トラフィック クラスはフォールバック グループ内の最良リンクを介してルーティングされます。 最良のリンクを特定するために、PfR はプライマリ グループとフォールバック グループの両方をプローブします。

（注） リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

PfR リンクのグループ化の詳細については、「パフォーマンス ルーティング リンク グループ」モジュールを参照してください。

PfR ネットワーク セキュリティ ポリシー

PfR には、ネットワークの不正使用の防止またはネットワーク内外での攻撃軽減のためにネットワーク セキュリティ ポリシーを設定する機能があります。 ブラック ホール ルーティングまたはシンクホール ルーティング手法を使用するようにPfR を設定すると、ネットワーク攻撃による影響を軽減できます。 ブラック ホール ルーティングとは、パケットをヌル インターフェイスに転送する、つまりパケットを「ブラック ホール」にドロップするプロセスです。シンクホール ルーティングでは、パケットはネクスト ホップに転送され、そこで保存、分析、またはドロップされます。 シンクホール ルーティングはハニーポット ルーティングとも呼ばれます。

PfR ポリシーの動作オプションおよびパラメータ

特定のタイプの PfR ポリシーに加え、PfR ポリシーの動作パラメータまたはオプションも設定可能です。 動作パラメータとはタイマーであり、動作オプションはさまざまな動作モードで構成されます。 詳細については、次の項を参照してください。

PfR タイマー パラメータ

PfR ポリシーの動作パラメータとして、次の 3 種類のタイマーを設定できます。

バックオフ タイマー

バックオフ タイマーは、マスター コントローラがポリシー違反のトラフィック クラスエントリを保留する移行期間を調整するために使用されます。 マスターコントローラは、この移行期間だけ待機してから、ポリシー準拠の出口を検索します。 最小、最大、および任意のステップ タイマー値を設定できます。

ホールドダウン タイマー

ホールドダウン タイマーは、トラフィック クラス エントリのルート ダンプニング タイマーを設定して、代替出口が選択可能になるまで新しい出口を使用する最小期間を設定します。 マスターコントローラは、急速な状態の変化によってトラフィック クラスエントリのフラッピングが発生するのを防ぐために、トラフィック クラスエントリがポリシー違反状態になっても、ホールドダウン タイマー期間中はそのエントリを他の出口に移動しません。 トラフィック クラス エントリがホールドダウン状態の間、PfR はポリシーの変更を実施しません。 トラフィック クラス エントリは、デフォルトまたは設定された期間中、ホールドダウン状態で維持されます。 ホールドダウン タイマーの期限が切れると、PfR は、パフォーマンスおよびポリシー設定に基づいて最良の出口を選択します。 ただし、トラフィック クラス エントリの現在の出口が到達不能になった場合は、ただちにルート変更がトリガーされます。

周期タイマー

周期タイマーは、トラフィック クラスエントリが現在の出口でポリシー準拠状態であっても、さらに良好なパスを検出するために使用されます。 周期タイマーが終了すると、マスター コントローラはトラフィック クラス エントリの現在の出口を確認します。現在の測定値とプライオリティに基づいてさらに良好な出口がある場合、トラフィック クラスエントリは新しいポリシー準拠出口リンクに移動されます。

PfR タイマーの調整を行う際は、新しい設定値が残り時間よりも少ないと、既存の設定はただちに新しいタイマー設定に置き換えられることに注意してください。 値が残り時間よりも多い場合、既存タイマーが期限切れになるか、リセットされると、新しい設定が適用されます。

（注） 極端なタイマー設定を行うと、出口リンクまたはトラフィック クラス エントリがポリシー違反状態になることがあります。

PfR モード オプション

PfR ポリシーの動作オプションとして、次の 3 種類のモード オプションを設定できます。

モニタ モード

モニタ モード オプションでは、PfR モニタリングの設定をイネーブルにします。 ここでいうモニタリングは、一定の時間間隔で定期的に行われ、測定値としきい値が比較される測定処理として定義されています。 PfR は、アクティブおよびパッシブ モニタリング手法を使用してトラフィック クラスのパフォーマンスを測定しますが、デフォルトでは出口リンクの使用率も測定します。

ルート モード

ルート モード オプションでは、3 つの PfR ルート制御ポリシー設定のうちいずれか 1 つを指定します。 ルート モード制御は PfR の自動ルート制御をイネーブルにし、ルート モード メトリックは PfR ルート プロトコルに関する設定を指定し、ルート観察モードではルート制御についての助言が行われますが、処理は何も実行されません。 デフォルトでは、PfR がイネーブルになると、観察モードのモニタリングもイネーブルになります。 観察モードでは、マスター コントローラはデフォルトおよびユーザ設定のポリシーに基づいてトラフィック クラスと出口リンクを監視し、ネットワークの状態と必要な決定事項をレポートします。ただし、変更は何も実施されません。観察モードは、PfR がネットワークに積極的に導入される前に、その機能の効果を検証するために使用されます。

PfR 境界ルータで異なる種類のルーティング プロトコルが動作している場合（たとえば、ある境界ルータでは BGP、別のルータでは EIGRP）、mode route コマンドで **protocol** と **pbr** キーワードを設定して、ダイナミック PBR を使用して宛先だけのトラフィック クラスを制御できるようにする必要があります。 **no mode route protocol pbr** コマンドを入力すると、まず、宛先だけのトラフィック クラスが制御されない設定になり、次に、BGP、EIGRP、スタティック、PBR の順に、トラフィック クラスを制御する 1 つのプロトコルを使用して、PfR がデフォルトの動作に戻ります。

出口選択モード

出口選択モード オプションでは、出口選択の設定をイネーブルにします。 ポリシー準拠のトラフィック クラス エントリは、パフォーマンス メトリックの測定値がデフォルトまたは定義済みのしきい値を超えず、トラフィック クラス エントリが現在のパス上にあると定義されます。 この場合、現在のネットワーク パスでトラフィック クラス エントリのポリシー準拠状態が維持されるので、PfR は代替出口リンクを検索しません。 このタイプの設定は、**mode select-exit good** コマンドを使用してアクティブ化されます。このコマンドは、**mode**（PfR）コマンドが指定されていない場合のデフォルトです。 PfR で最良パフォーマンス パスを選択するシナリオはほかにもあります。 このタイプの設定は、**mode select-exit best** コマンドを使用してアクティブ化されます。この場合、トラフィック クラス エントリが現在のパスでポリシー準拠状態である間に、PfR は代替パスのパフォーマンス メトリックを測定します。 さらに良好なパスが検出されると、PfR は現在のパスを移動します。 ただし、最初に最良のパスが選択された場合は、周期タイマーが設定されていない限り、PfR は代替パスの検索を開始しません。 周期タイマーが終了すると、マスター コントローラはトラフィック クラス エントリの現在の出口を確認します。現在の測定値とプライオリティに基づいてさらに良好な出口がある場合、トラフィック クラス エントリは新しいポリシー準拠出口リンクに移動されます。 PfR でいつでも最良パフォーマンス パスが選択されるようにする必要がある場合は、周期タイマーと **mode select-exit best** コマンドを使用します。

出口選択モード オプションにはもうひとつ使用方法があります。 **mode select-exit good** コマンドの動作中に、PfR によってトラフィック クラス エントリに対するポリシー準拠の出口が検出されなかった場合、PfR はそのトラフィック クラス エントリを制御解除状態にします。 **mode select-exit best** コマンドの動作中に、PfR によってトラフィック クラス エントリに対するポリシー準拠の出口が検出されなかった場合、PfR は OOP 出口リンクの中からそのトラフィック クラス エントリにとって最良の出口を選択します。

PfR ポリシーの適用

PfR ポリシーは、学習済みまたは設定済みのトラフィック クラスに適用できます。 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 PfR ポリシーが直接設定されている場合は、その PfR ポリシーをグローバルに適用できます。 すべてのトラフィック クラスはグローバル ポリシーを継承します。 ただし、トラフィック クラスのサブセットにポリシーを適用したい場合は、特定のポリシーを設定できます。 特定の PfR ポリシーは、プレフィックス リストまたはアクセス リストと一致する特定のトラフィック クラスだけに適用されます。 特定のポリシーは、同じポリシーが特定のポリシーによって上書きされない限り、グローバル ポリシーを継承します。 PfR ポリシーは、プレフィックスだけに適用できすることができます。あるいは、アプリケーション トラフィック クラスを定義するトラフィック クラスに PfR ポリシーを適用し、プレフィックス、プロトコル、ポート番号、および DSCP 値を含めることもできます。 特定のポリシーを学習済みまたは設定済みトラフィック クラスに適用するには、PfR マップ設定を使用します。

PfR ポリシー用 PfR マップの設定

PfR マップはルート マップと似ていますが、大きく異なる点があります。 PfR マップの目的は、match 句を使用して学習済みまたは設定済みトラフィック クラスを選択してから、set 句を使用して PfR ポリシー設定を適用することです。 ルート マップのようにシーケンス番号を使用して PfR マップを任意で設定することはできますが、評価されるのはシーケンス番号が最も小さい PfR マップだけです。 PfR マップとルート マップの動作の違いはここにあります。 重要な違いは次の 2 点です。

- 各シーケンスに対して設定できるのは、1 つの match 句だけです。 1 つの PfR マップ シーケンスに複数の match 句を設定しようとすると、エラー メッセージが表示されます。
- PfR マップの設定に permit 文または deny 文は使用しません。 ただし、IP プレフィックス リストで permit 文または deny 文を設定し、そのプレフィックス リストを PfR マップに適用すると、IP トラフィック フローに許可または拒否シーケンスを設定できます。

（注） match precedence のプライオリティは PfR マップではサポートされません。

適切に一致すると、PfR マップに set 句の設定が適用されます。 PfR set 句を使用して、バックオフ タイマー、パケット遅延、ホールドダウン タイマー、パケット損失、周期タイマー、解決設定、到達不能ホスト、traceroute レポートなどのポリシー パラメータを設定できます。

PfR マップによって適用されたポリシーはただちに有効になります。 PfR マップ設定は、**show running-config** コマンドの出力で確認できます。 PfR ポリシー設定は、**show pfr master policy** コマンドの出力で確認できます。 これらのポリシーは、PfR マップと一致する、または PfR マップを通過するトラフィック クラスだけに適用されます。

PfR ポリシーを適用するポリシー ルールの設定

policy-rules（PfR）コマンドを使用すると、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、シーケンス番号を使用して PfR マップを選択し設定を適用できます。これにより、定

義済み PfR マップ間での切り替えを容易に実行できます。 ポリシーの設定に使用できる PfR マップは 1 度に 1 つだけですが、多数の PfR マップを定義することができます。

複数の PfR ポリシーに対するプライオリティ解決

1 つのトラフィック クラス エントリまたはトラフィック クラスのセットに複数のポリシー基準を設定する場合、複数のポリシーが重複する可能性があります。 実行するポリシーの競合を回避するために、PfR は解決機能を使用します。これは、PfR ポリシーにプライオリティを設定できる柔軟なメカニズムです。 各ポリシーには一意の値が割り当てられ、最低値が設定されているポリシーが最高プライオリティ ポリシーとして選択されます。 デフォルトでは、PfR は最高プライオリティを遅延ポリシーに割り当て、その次に使用率ポリシーに割り当てます。 いずれかのポリシーにプライオリティ値を割り当てると、デフォルト設定は上書きされます。 ポリシー競合解決を設定するには、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 **resolve**（PfR）コマンドを使用するか、PfR マップ コンフィギュレーション モードで **set resolve**（PfR）コマンドを使用します。

PfR ポリシー競合解決のための分散設定

PfR 解決を設定する際、定義済みのポリシーに許容分散を設定することもできます。 分散では、平均遅延が割合で設定されます。平均遅延とは、1 つの出口に対するすべてのトラフィック クラスまたは特定のポリシー トラフィック クラスが、定義されたポリシー値と異なっていてもそれと同等と見なされる範囲です。 たとえば、最良の出口リンク（遅延の面から見て最良の出口）でのトラフィック クラス エントリの遅延が 80 ミリ秒（ms）で、10 % の分散が設定されている場合、その他の出口リンクで同じトラフィック クラス エントリの遅延が 80 ～ 88 ms の範囲内であれば、それらの出口リンクは最良の出口リンクと同等であると見なされます。

PfR で分散がどのように使用されるかを理解するために、3 つの出口リンクでトラフィック クラス エントリの遅延およびジッターに次のパフォーマンス値が設定された場合を見てみましょう。

- 出口 A：遅延 80 ms、ジッター 3 ms
- 出口 B：遅延 85 ms、ジッター 1 ms
- 出口 C：遅延 100 ms、ジッター 5 ms

このトラフィック クラス エントリには、次の PfR ポリシー競合解決が適用されます。

```
delay priority 1 variance 10
jitter priority 2 variance 10
```

PfR は、プライオリティ値が最も低いポリシー（この例では遅延ポリシー）を探して最良の出口を判断します。 遅延値が最も低いのは出口 A です。ただし、出口 B の遅延値は 85 で、これは出口 A における遅延値の 10 % 分散の範囲内です。 したがって、出口 A と出口 B は遅延値上では同等であると見なされます。 出口 C は、遅延値が高すぎるため無視されます。 次のプライオリティ ポリシーはジッターで、ジッター値が最も低いのは出口 B です。 出口 A のジッター値は出口 B のジッター値の 10 % 分散の範囲内にないので、PfR は、トラフィック クラス エントリの唯一最良の出口として出口 B を選択します。

（注） 分散は、コストまたは範囲ポリシーには設定できません。

施行フェーズの概念

PfR 施行フェーズの概要

PfR 学習フェーズでトラフィック クラスをプロファイリングし、測定フェーズでトラフィック クラスのパフォーマンス メトリックを測定し、トラフィックが所定のサービス レベルを満たしている場合はポリシー フェーズでネットワーク ポリシーを使用して、Monitored Traffic Class（MTC）リストにあるトラフィック クラス エントリの測定済みパフォーマンス メトリックを既知または設定済みのしきい値にマッピングしたら、PfR パフォーマンス ループにおける次のステップは施行フェーズです。

デフォルトでは、PfR は観察モードで動作します。PfR 学習、測定、およびポリシー適用フェーズのマニュアルでは、PfR が観察モードであることを前提としています。観察モードでは、マスター コントローラはデフォルトおよびユーザ設定のポリシーに基づいてトラフィック クラスと出口リンクを監視し、ポリシー違反（OOP）イベントなどネットワークの状態と必要な決定事項をレポートします。ただし、変更は何も実施されません。 PfR 施行フェーズは、観察モードではなく制御モードで動作します。制御モードは、**mode route control** コマンドを使用して明示的に設定する必要があります。 制御モードでは、マスター コントローラは境界ルータからの情報を観察モードと同じ方法で統合します。ただし、PfR 管理ネットワークのルーティングを変更してポリシー決定を実施するために、境界ルータにコマンドが返されます。

次のいずれかの状況が発生すると、PfR はルート変更を開始します。

- トラフィック クラスが OOP になる。
- 出口リンクが OOP になる。
- 周期タイマーが終了し、出口選択モードが最良のモードとして設定される。

PfR 施行フェーズでは、マスター コントローラは目的のパフォーマンス特性と一致するポリシー準拠のトラフィック クラスを継続的に監視し、それらのトラフィック クラスがポリシー準拠のまま維持されるようにします。 OOP のトラフィック クラスと出口をポリシー準拠にする場合だけ、それらのトラフィック クラスと出口が変更されます。 ネットワークで目的のパフォーマンス レベルを実現するには、マスター コントローラによるポリシー決定に影響を与える可能性のある設定オプションを認識しておく必要があります。

PfR の導入時に考慮すべきもうひとつの設定上の問題は、極端な遅延または損失ポリシーが定義され、出口リンクへの加入も過剰な場合、PfR がトラフィック クラスをポリシー準拠状態にできないと判断する可能性があるということです。 この場合マスター コントローラは、トラフィック クラスが OOP のままであっても、パフォーマンス ポリシーに最も厳密に適合するリンクを選択するか、PfR 制御からプレフィックスを削除します。 PfR は、使用可能な帯域幅を最大限活用できるようにすることを目的としていますが、加入過多の帯域幅の問題は解決できません。

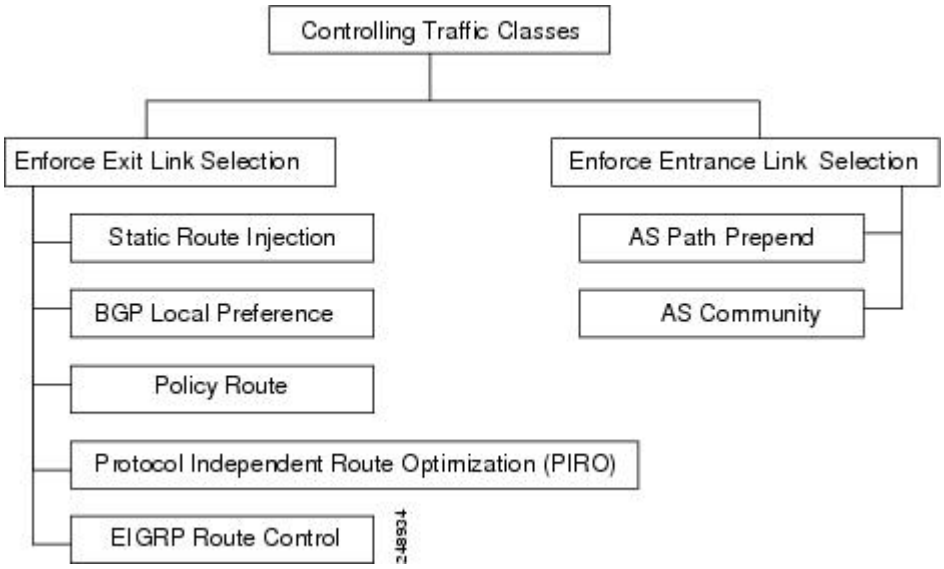
PfR 制御モードがイネーブルになり、設定オプションが検討されたら、次のステップでは PfR で実施されるトラフィック クラス制御の手法を検証します。

PfR トラフィック クラス制御手法

PfR マスター コントローラが、OOP トラフィック クラスまたは出口リンクに対して何らかの措置が必要であると判断した場合、ルーティング メトリックまたは BGP 属性を変更したり、ルートマップを使用するポリシーベースのルーティングを導入したりして、トラフィックが別のリンクを使用するようにするための手法がいくつかあります。トラフィック クラスに関連付けられたトラフィックがプレフィックスだけで定義されている場合は、BGP ルートまたはスタティック ルートの導入など、従来のルーティング制御メカニズムを使用できます。 この制御は、再配布後にネットワーク全体で有効になります。なぜなら、より良好なメトリックを持つルーティング プロトコルに導入されたプレフィックスは、そのプレフィックスのトラフィックを境界ルータに誘導するからです。トラフィック クラスに関連付けられたトラフィックがプレフィックスとその他のパケット一致基準または（たとえばアプリケーション トラフィック）によって定義されている場合、従来のルーティングを使用してそのアプリケーション トラフィックを制御することはできません。 この場合は、ネットワーク全体ではなくデバイス固有の制御が行われます。 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、リモート境界ルータはシングル 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。

出口または入口リンクの選択でグループ化されたさまざまなトラフィック クラス制御手法を次の図に示します。

図 *9*：トラフィック クラス制御手法



PfR 出口リンク選択制御手法

出口選択にはパフォーマンス ルーティングのロード バランシングに関する 1 つの原理が当てはまるので、出口リンク選択制御手法を導入するにあたっては、この原理を理解する必要があります。PfR では、限定度の高いルートはデフォルト ルートとして設定しない限り、親ルートとして扱われません。

親ルートの検索時、ソフトウェアでは指定されたプレフィックスを含む最も限定度の高いルートの検出が試みられます。また、ソフトウェアでは、そのルートが予想される出口をポイントしていることが確認されます。 限定度の高いスタティック ルートが 2 つ以上存在する場合、それぞれのルートで予想される出口があるかどうかが検査されます。 予想される出口が見つかった場合、プローブが作成されます。

たとえば、次のような設定があるとします。

```
ip route 10.4.0.0 255.255.0.0 172.17.40.2
ip route 0.0.0.0 0.0.0.0 serial 6/0
```

プレフィックス 10.4.1.0/24 およびターゲット 10.4.1.1 のプローブは、シリアル インターフェイス 6/0 を使用する出口上には作成されません。この理由は、10.4.1.1 を含む最も限定度の高いルートは 172.17.40.2 への出口になっているためです。 両方の出口にトラフィックのロード バランスを行う場合の解決法は、限定度の高いルートのデフォルト ルートを作成することです。次に例を示します。

```
ip route 10.4.0.0 255.255.0.0 172.17.40.2
ip route 10.4.0.0 255.255.0.0 serial 6/0
```

または

```
ip route 0.0.0.0 0.0.0.0 serial 6/0
ip route 0.0.0.0 0.0.0.0 172.17.40.2
```

変更後の設定では、172.17.40.2 への出口用とシリアル インターフェイス 6/0 を使用する出口用に 2 つのプローブが作成されます。

PfR では、次の手法を使用して出口リンク選択を実施します。

スタティック ルートの挿入

PfR マスター コントローラは、一時的なスタティック ルートを挿入して、特定の境界ルータを優先出口リンクとして強制的に使用させることができます。 これらのスタティック ルートはルータのメモリ内に一時的に存在し、永続的な設定には意図的に保存されません。マスター コントローラが境界ルータでスタティック ルートを挿入するための手法はいくつかあります。 既存のスタティック ルートは、より良好なルーティング メトリックを持つ新しいスタティック ルートで上書きされます。境界ルータ上にデフォルト ルート（またはあいまいなルート）がある場合、マスター コントローラは監視対象のトラフィック クラス用に特定のスタティック ルートを追加できます。このスタティック ルートは既存のデフォルト ルートよりも優先されます。 最後に、マスター コントローラでは分割プレフィックスとして知られる方法も使用できます。

分割プレフィックスは、追加されたより具体的なルートを参照します。このルートは、あいまいなルートよりも優先されます。 たとえば、境界ルータに 10.10.10.0/24 のルートがすでにある場合、10.10.10.128/25 のスタティック ルートを追加すると、新たに挿入されたルートを使用してアドレス 10.10.10.129 ～ 10.10.10.254 も転送されます。 大規模ネットワークのサブセットを監視す

るように設定されている場合、PfRは既存のルーティングテーブルに適切なルートを追加します。PfR は分割プレフィックスを使用して、既存プレフィックスのサブセットをより適切な出口リンクにリダイレクトできます。分割プレフィックスは、内部 BGP（iBGP）ルートとスタティックルートの両方で使用できます。

ルーティング プロトコル テーブルに既存ルートがない場合、PfR はルートを挿入しません。 特定タイプのルートを挿入する前に、PfR は BGP またはスタティック テーブル内にルートが存在し、プレフィックスと既存リンクへのポイントが含まれていることを確認します。 このルートはデフォルト ルートの場合もあります。

BGP 制御手法

PfR では 2 つの BGP 手法を使用して、最良の出口パスを強制的に使用させます。手法のひとつは BGP ルートの挿入、もうひとつは BGP ローカル プリファレンス属性の変更です。

トラフィック クラスに関連付けられているトラフィックがプレフィックスだけで定義されている場合、マスターコントローラはBGPルートをBGPテーブルに挿入するよう境界ルータに指示し、そのトラフィックで他のリンクが使用されるようにすることができます。 PfR で挿入されたすべてのルートは自律システムのローカル ルートのままであり、外部BGPピアと共有されることはありません。 この動作が確実に実行されるようにするため、PfR は BGP ルートを挿入する際、そのルートに no-export コミュニティを設定します。 この処理は自動的に実行されるので、ユーザが設定する必要はありません。 ただし、現在これらのルートには特殊なマーキングがあるため、内部 BGP ピアと情報を共有するには追加設定が必要です。 各 iBGP ピアに対し、send コミュニティ設定を指定する必要があります。 境界ルータは挿入されたルートの最良出口を認識していますが、さらにこの情報をネットワークに再配布する必要が生じる場合があります。

PfR は、トラフィック クラスの制御にも BGP ローカル プリファレンスを使用します。 BGP ローカル プリファレンス（Local_Pref）は BGP プレフィックスに適用される任意の属性で、ルート選択時にそのルートに対するプリファレンスの程度を指定します。 Local_Pref は BGP プレフィックスに適用される値であり、Local_Pref の値が高いほど、そのルートは同等のルートよりも優先されます。 マスター コントローラはいずれかの境界ルータに対し、トラフィック クラスに関連付けられたプレフィックスまたはプレフィックスのセットに Local_Pref 属性を適用するよう指示します。 そのあと境界ルータは、Local_Pref 値をすべての内部 BGP ピアと共有します。 Local_Pref は自律システムのローカルでは重要な値ですが、外部 BGP ピアとは共有されません。 iBGP 再コンバージェンスが完了すると、プレフィックスの Local_Pref が最も高いルータが、ネットワークからの出口リンクになります。

（注） デフォルトの BGP ルーティングに 5000 以上のローカル プリファレンス値が設定されている場合は、**mode**（PfR）コマンドを使用してそれよりも高い BGP ローカル プリファレンス値を PfR で設定する必要があります。

EIGRP ルート制御

PfR EIGRP mGRE DMVPN ハブアンドスポーク サポート機能により、PfR で EIGRP ルートを制御できるようになりました。 この機能がイネーブルになると、PfR プレフィックスおよびルートを制御するために、既存の BGP およびスタティック ルート データベースだけでなく EIGRP データ

ベースでも親ルートがチェックされます。 詳細については、「パフォーマンス ルーティングの mGRE DMVPN ハブアンドスポーク サポートを使用した EIGRP ルートの制御」モジュールを参照してください。

ポリシーベースのルーティング制御

PfR は、ポリシーベースのルーティングを使用してアプリケーション トラフィックを制御できます。 PfR ポリシーの一環として PfR マップで定義されたトラフィックと照合することで、特定の PfR 境界ルータを通過するアプリケーション トラフィックを識別できます。 **match ip address**（PfR）コマンドは、拡張 ACL をサポートするように強化されました。 拡張 ACL は PfR マップで参照されます。各 PfR マップ シーケンスには単一の match 句を設定できます。 set 句は、一致したトラフィックに独立した PfR ポリシーを適用するために設定されます。このトラフィックは、監視対象のプレフィックスのサブセットです。アプリケーションのポリシー ルーティングを強制するために、PfR ポリシーはすべての境界ルータに適用されます。 一致したトラフィックは、ポリシー パラメータに適合する PfR 外部インターフェイスを介してポリシー ルーティングされます。

アプリケーション トラフィックの識別と制御には、プレフィックスのほか DSCP 値、ポート番号、およびプロトコルも使用できます。 DSCP 値、プロトコル、およびポート番号は、境界ルータによってマスター コントローラに送信され、MTC リストに入力されます。

Protocol Independent Route Optimization（PIRO）

PIRO が導入され、PfR でトラフィック クラスを識別および制御できるようになりました。 PIRO より前に、PfR は、BGP またはスタティック ルート データベースで親ルート（完全一致ルート、またはそれより一致度が低いルート）を持つトラフィック クラスのパスを最適化します。 PIRO を使用して、PfR は親ルートの IP ルーティング情報ベース（RIB）を検索できます。これにより、OSPF や IS-IS などの内部ゲートウェイ プロトコル（IGP）を含む任意の IP ルーティング環境に PfR を導入することができます。

詳細については、「PfR Protocol Independent Route Optimization」モジュールを参照してください。

PfR 入口リンク選択の制御テクニック

PfR BGP インバウンド最適化機能に、インバウンド トラフィックを操作する機能が追加されました。 ネットワークは ISP への eBGP アドバタイズメントを使用して、内部プレフィックスの到達可能性をインターネットにアドバタイズします。 同じプレフィックスが複数の ISP にアドバタイズされると、そのネットワークはマルチホーム状態になります。 PfR BGP インバウンド最適化は、マルチホームのネットワークで最も効果的に機能します。ただしこの最適化は、同じ ISP に対して複数の接続を持つネットワークでも使用できます。 BGP インバウンド最適化を実装するために、PfR は eBGP アドバタイズメントを操作して、内部プレフィックス宛てのトラフィックに対して最良入口選択を反映させます。 最良入口選択は、複数の ISP に接続しているネットワークだけに効果があります。

PfR 入口リンク選択制御手法の詳細については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

確認フェーズの概念

確認フェーズの概要

PfR パフォーマンス ループの最終フェーズでは、PfR 制御フェーズで実施された処理によってトラフィック フローが実際に変更され、トラフィック クラスまたはリンクのパフォーマンスがポリシー準拠状態に移行するかどうかを確認します。 PfR は NetFlow を使用して、自動的にルート制御を確認します。 マスター コントローラは、新しいリンク インターフェイスからのトラフィック クラスの Netflow アップデートを予想しているので、以前のパスからの Netflow アップデートは無視します。 2 分後に Netflow アップデートが表示されない場合、マスター コントローラはトラフィック クラスをデフォルト状態にします。 PfR の制御下にないとき、トラフィック クラスはデフォルト状態です。

PfR で使用される NetFlow 確認に加え、PfR がネットワーク内で変更を開始したことを確認する方法がさらに 2 つあります。

- syslog レポート：主要な PfR の状態変更をすべてユーザに通知するようにロギング コマンドを設定できます。syslog レポートを実行すると、PfR で変更が行われたことを確認できます。マスター コントローラは双方向トラフィックを予想しており、トラフィック クラスに関連付けられた特定のプレフィックスに関する区切りつき syslog レポートでこれを確認できます。
- PfR show コマンド：PfR show コマンドを使用して、ネットワークで変更が行われたこと、トラフィック クラスがポリシー準拠状態であることを確認できます。 監視対象のプレフィックスのステータスを表示するには、**show pfr master prefix** コマンドを使用します。 このコマンドの出力には、現在の出口インターフェイス、プレフィックス遅延、出力および入力インターフェイスの帯域幅、指定された境界ルータを送信元とするパス情報が含まれます。 境界ルータ上で PfR によって制御されているルートに関する情報を表示するには、**show pfr border routes** コマンドを使用します。 このコマンドは、BGP またはスタティック ルートに関する情報を表示できます。

関連情報

このモジュールで説明する概念を実行する設定タスクと設定例については、「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。 その他のパフォーマンス ルーティング モジュールおよび機能の詳細については、「関連資料」の項を参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンスルーティングを理解するための機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *4*：パフォーマンス ルーティングを理解するための機能情報

機能名	リリース	機能の設定情報
OER 境界ルータ専用機能	Cisco IOS XE Release 3.1.S	境界ルータ専用機能は Cisco IOS XE Release 3.1S で導入されました。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降のリリースを実行するルータでなければなりません。 この機能により、次のコマンドが導入または変更されました。 **show pfr border passive cache**。

機能名	リリース	機能の設定情報
ASR 1000 用 PfR マスター コントローラのサポート	Cisco IOS XE Release 3.3.S	ASR 1000 用 PfR マスター コントローラのサポートにより、マスター コントローラのサポートが導入されました。以前は、境界ルータのサポートのみ使用可能でした。この機能により、他のプラットフォームで使用できる PfR 機能の大部分がイネーブルになりました。

パフォーマンス ルーティング コンフィギュレーション ガイド、**Cisco IOS XE Release 3S**（**Cisco ASR 1000**）

第 4 章

アドバンスドパフォーマンスルーティングの設定

パフォーマンス ルーティング（PfR）マスター コントローラおよび境界ルータの設定後（「ベーシック パフォーマンス ルーティングの設定」モジュールを参照）に PfR のすべての最適化機能をアクティブ化するには、追加設定が必要です。 このモジュールには、PfR の各フェーズを表すタスクおよび設定例が記載されているので、PfR の各フェーズの高度なオプションの一部の設定方法を理解し、確認できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

アドバンスドパフォーマンスルーティングの設定の前提条件

- このモジュールでは、マスター コントローラおよび境界ルータが Cisco IOS XE Release 3.3S 以降で稼働していることを前提としています。
- このモジュールのタスクを設定する前に、「ベーシック パフォーマンス ルーティングの設定」モジュールを使用して、マスター コントローラおよび少なくとも 2 台の境界ルータを設定する必要があります。
- このモジュールのタスクを設定する前に、「パフォーマンス ルーティングの理解」モジュールに記載の概念についての知識が必要です。
- ネットワークでルーティング プロトコル ピアリングを確立するか、スタティック ルーティングを設定してから、ルート制御モードをイネーブルにする必要があります。

境界ルータで内部ボーダー ゲートウェイ プロトコル（iBGP）を設定した場合は、BGP ピアリングを確立してネットワーク全体に一貫して適用するか、Interior Gateway Protocol（IGP）に再配布する必要があります。 Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Intermediate System-to-Intermediate System（IS-IS）、またはルーティング情報プロトコル（RIP）の各 IGP がサポートされています。

ネットワークに IGP が導入されている場合、**redistribute** コマンドを使用してスタティック ルートの再配布を設定する必要があります（ただし、iBGP が設定されている場合は除きます）。 IGP またはスタティック ルーティングが、PfR 管理のネットワーク全体に一貫して適用され、境界ルータがネットワークの一貫したビューを持つことも必要です。

注意 PfR スタティック ルートを IGP に再配布する際は、慎重に行う必要があります。 PfR によって挿入されるルートは IGP のルートよりも限定度の高いルートになる傾向にあります。これらのルートは PfR 境界ルータが出発点であるかのように表示されます。 ルーティング ループを回避するためには、再配布された PfR スタティック ルートが、PfR 境界ルータまたは他のルータによって WAN 上でアドバタイズされないようにする必要があります。 PfR スタティック ルートがアドバタイズされないようにするために、ルート フィルタリングおよびスタブ ネットワーク設定を使用できます。 PfR スタティック ルートが PfR 外部インターフェイスを終端とするルータに再配布された場合、ルーティング ループが発生することがあります。

アドバンスド パフォーマンス ルーティングの概要

アドバンスド PfR を設定するには、次の概念を理解する必要があります。

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、MOS スコア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 サービス レベル契約（SLA）（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。

アドバンスド パフォーマンス ルーティングの導入

アドバンスド PfR は、Cisco IOS コマンドライン インターフェイス（CLI）設定を使用して Cisco ルータ上で設定されます。 PfR 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 モードで通信が行われるパフォーマンス ルーティング プロトコルが含まれています。 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、境界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。

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。

アドバンスドPfRでは、次の各PfRフェーズに対応するために設定タスクを行う必要があります。

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ルーティング情報ベース（RIB）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、ポリシー違反（OOP）イベントになります。 結果は相対的に（実際の平均値からの偏差）、またはしきい値ベースで（値の下限または上限、または両方の組み合わせ）比較されます。

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、プレフィッ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。 プレフィッ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ッ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ッ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。

プレフィッ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、プレフィッ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、リモート境界ルータはシングル 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 アクティブ プローブのターゲットへの到達可能性

アクティブ プローブは境界ルータをソースとし、外部インターフェイスを介して送信されます（外部インターフェイスは、最適化されたプレフィックスの優先ルートである場合も、ない場合もあります）。指定されたターゲットに対して外部インターフェイス経由のアクティブプローブを作成する場合は、その外部インターフェイスを介してターゲットに到達できる必要があります。指定されたターゲットの到達可能性をテストするために、PfR は BGP およびスタティック ルーティングテーブルで、所定のターゲットと外部インターフェイスのルートルックアップを実行します。

ICMP エコー プローブ

ICMP エコー プローブの設定には、ターゲット デバイスからの大きな協力を必要としません。 しかし、プローブを繰り返し行うと、ターゲット ネットワーク内で侵入検知システム（IDS）アラームが発生することがあります。 自身の管理制御下にないターゲット ネットワークで IDS が設定されている場合には、ターゲット ネットワークの管理エンティティに通知することを推奨します。

アクティブ モニタリングがイネーブルの場合には、次のデフォルトが適用されます。

- トラフィック クラスが学習済みまたは集約されている場合、境界ルータは、アクティブ プローブを行うために最大 5 個のホスト アドレスをトラフィック クラスから収集します。
- アクティブ プローブは、1 分間に 1 回送信されます。
- ICMP プローブは、学習済みのトラフィック クラスをアクティブに監視するために使用されます。

ジッター

ジッターはパケット間の遅延がばらつくことを指します。 複数のパケットが発信元から宛先に連続的に送信された場合、たとえば 10 ms 間隔で送信された場合、ネットワークが理想的に動作していれば、宛先は 10 ms 間隔でパケットを受信します。 しかし、ネットワーク内に遅延（キューイング、代替ルートを介した受信など）が存在する場合、パケット間の到着遅延は、10 ms より大きい場合も、10 ms より小さい場合もあります。 この例を使用すると、正のジッター値は、パケットが 10 ms を超える間隔で到着することを示します。 パケットが 12 ms 間隔で到着する場合、正のジッターは 2 ms です。パケットが 8 ms 間隔で到着する場合、負のジッターは 2 ms です。 Voice over IP（VoIP）など遅延に影響されやすいネットワークでは、正のジッター値は望ましくありません。0 のジッター値が理想的です。

MOS

平均オピニオン評点（MOS）は、PfR アクティブ プローブを使用して測定可能な音声トラフィック向けの定量的な品質メトリックです。 すべての要因が音声品質に影響を与えるので、音声品質の測定方法については多くの人々が疑問を持っています。 ITU などの標準化団体によって、P.800（MOS）および P.861（Perceptual Speech Quality Measurement（PSQM））という 2 つの重要な勧告が作成されています。 P.800 は、音声品質の平均オピニオン評点を算出する方法の定義に関するものです。 MOS スコアの範囲は、最低の音声品質を表す 1 から最高を表す 5 までです。 MOS 4 は、「トール品質」音声と見なされます。

アドバンスド パフォーマンス ルーティングの設定方法

ここでは、次のタスクについて説明します。

プロファイリング フェーズのタスク

次のタスクは、PfR プロファイリング フェーズの要素の設定方法を示します。

アクセス リストを使用して自動的に学習されたアプリケーション トラフィック クラスの学習リストの定義

アクセス リストを使用して PfR で自動的に学習されたトラフィック クラスを含む学習リストを定義して、カスタマイズされたアプリケーション トラフィック クラスを作成するには、マスター コントローラで次のタスクを実行します。 次のタスクでは、カスタム アプリケーション トラフィック クラスを定義するアクセス リストが作成されます。 アクセス リスト内のエントリごとに 1 つのアプリケーションが定義されます。 次に学習リストが定義され、アクセス リストが適用されます。集約方法が設定されます。 **count**（PfR）コマンドを使用すると、LEARN_USER_DEFINED_TC という名前の学習リストに対する 1 回の学習セッションで 50 個のトラフィック クラスを学習できます。この学習リストに指定できるトラフィック クラスの最大数は 90 です。 マスター コントローラは、フィルタリング対象トラフィックの最高遅延に基づいてトップ プレフィックスを学習するように設定され、その結果得られたトラフィック クラスが PfR アプリケーション データベースに追加されます。

学習リストは PfR マップを使用してアクティブ化されます。このタスクの最後の方の手順では、このタスクで定義した学習リストをアクティブ化しカスタム トラフィック クラスを作成するための、PfR マップの設定方法を示します。

プレフィックス リストを使用して自動的に学習されたプレフィックスベースのトラフィック クラスの学習リストの定義例については、「例：自動的に学習されたプレフィックスベースのトラフィック クラスの学習リストの定義」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
5. 必要に応じて、追加のアクセス リスト エントリについてステップ 4 を繰り返します。
6. **exit**
7. **pfr master**
8. **learn**
9. **list seq** *number* **refname** *refname*
10. **count** *number* **max** *max-number*
11. **traffic-class access-list** *access-list-name* [**filter** *prefix-list-name*]
12. **aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask*
13. **delay**
14. **exit**
15. ステップ 14 を 2 回繰り返し、グローバル コンフィギュレーション モードに戻ります。
16. **pfr-map** *map-name sequence-number*
17. **match traffic-class access -list** *access-list-name*
18. **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。 • パスワードを入力します（要求された場合）。
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	**ip access-list** {**standard** | **extended**} *access-list-name* 例： `Router(config)# ip access-list extended USER_DEFINED_TC`	IP アクセス リストを名前で定義します。 • PfR は、名前付きアクセス リストだけをサポートします。 • 例では、USER_DEFINED_TC という名前の拡張 IP アクセス リストが作成されます。

	コマンドまたはアクション	目的
ステップ 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] 例： `Router(config-ext-nacl)# permit tcp any any 500`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • 例では、任意の宛先または送信元から、および宛先ポート番号 500 からのすべての伝送制御プロトコル（TCP）トラフィックを識別するように設定されます。この特定の TCP トラフィックが最適化されます。 （注） 次のタスクに適用される構文だけが記載されています。詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。
ステップ 5	必要に応じて、追加のアクセス リスト エントリについてステップ 4 を繰り返します。	--
ステップ 6	**exit** 例： `Router(config-ext-nacl)# exit`	（任意）拡張アクセス リスト 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 7	**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、マスター コントローラとして Cisco ルータを設定し、マスター コントローラ ポリシーおよびタイマー設定を設定します。
ステップ 8	**learn** 例： `Router(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、トラフィック クラスを自動的に学習します。
ステップ 9	**list seq** *number* **refname** *refname* 例： `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_USER_DEFINED_TC`	PfR 学習リストを作成し、学習リスト コンフィギュレーション モードを開始します。 • 学習リスト基準が適用される順番の決定に使用されるシーケンス番号を指定するには、**seq** キーワードおよび *number* 引数を使用します。 • 学習リストの参照名を指定するには、**refname** キーワードおよび *refname* 引数を使用します。 • 例では、LEARN_USER_DEFINED_TC という名前の学習リストが作成されます。

	コマンドまたはアクション	目的
ステップ 10	**count** *number* **max** *max-number* 例： `Router(config-pfr-mc-learn-list)# count 50 max 90`	PfR 学習セッション中に学習されるトラフィック クラスの数を設定します。 • 1 つの学習セッション中に、指定した学習リストについて学習されるトラフィック クラスの数を指定するには、*number* 引数を使用します。 • すべての学習セッション中に、指定した学習リストについて学習されるトラフィック クラスの最大数を指定するには、**max** キーワードおよび *max-number* 引数を使用します。 • 例では、LEARN_USER_DEFINED_TC という名前のリストについて各学習セッションで 50 個のトラフィック クラスが学習され、この学習リストについて合計で最大 90 個のトラフィック クラスが学習されるように指定されます。
ステップ 11	**traffic-class access-list** *access-list-name* [**filter** *prefix-list-name*] 例： `Router(config-pfr-mc-learn-list)# traffic-class access-list USER_DEFINED_TC`	アクセス リストを使用して PfR トラフィック クラスを定義します。 • トラフィック クラスを定義するための基準を含むアクセス リストを指定するには、*access-list-name* 引数を使用します。 • 例では、USER_DEFINED_TC という名前のアクセス リストが使用されて、トラフィック クラスが作成されます。
ステップ 12	**aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask* 例： `Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	（任意）トラフィック フロー タイプに基づいて学習済みのプレフィックスを集約するように、マスター コントローラを設定します。 • **bgp** キーワードは、BGP ルーティング テーブル内のエントリに基づいてプレフィックスを集約するように設定します。 このキーワードは、BGP ピアリングがネットワーク内でイネーブルの場合に使用されます。 • **non-bgp** キーワードは、スタティック ルートに基づいて学習済みのプレフィックスを集約するように設定します。 このキーワードが入力された場合、BGP ルーティング テーブル内のエントリは無視されます。 • **prefix-length** キーワードは、指定したプレフィックス長に基づいて集約するように設定します。 この引数に設定できる値の範囲は、1 ～ 32 のプレフィックス マスクです。 • このコマンドが指定されない場合、デフォルトの集約が、/24 のプレフィックス長に基づいて実行されます。

	コマンドまたはアクション	目的
		• 例では、/24 のプレフィックス長に基づいて、プレフィックス長の集約が設定されます。
ステップ 13	**delay** **例**： `Router(config-pfr-mc-learn-list)# delay`	最高遅延時間に基づいたプレフィックス学習をイネーブルにします。 • *Top Delay* プレフィックスは、最高遅延時間から最低遅延時間の順にソートされます。 • 例では、最高遅延に基づいたプレフィックス学習が設定されます。 （注） 学習リスト内での自動 PfR 学習を設定するには、**delay**（PfR）コマンドまたは **throughput**（PfR）コマンドのいずれかを指定できますが、これらのコマンドは、学習リスト コンフィギュレーション モードでは同時に使用できません。
ステップ 14	**exit** **例**： `Router(config-pfr-mc-learn-list)# exit`	（任意）学習リスト コンフィギュレーション モードを終了し、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 15	ステップ 14 を 2 回繰り返し、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 16	**pfr-map** *map-name sequence-number* **例**： `Router(config)# pfr-map ACCESS_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • permit シーケンスは最初に IP アクセス リストに定義してから、ステップ 17 で **match traffic-class access-list** コマンドを使用して適用します。 • 例では、ACCESS_MAP という名前の PfR マップが作成されます。
ステップ 17	**match traffic-class access -list** *access-list-name* **例**： `Router(config-pfr-map)# match`	PfR マップを使用して、トラフィック クラスの作成に使用される一致基準として、アクセス リストを手動で設定します。 • 例では、USER_DEFINED_TC という名前の IP アクセス リストで定義されている宛先アドレスを使用して、トラフィック クラスが定義されます。

	コマンドまたはアクション	目的
	`traffic-class access-list USER_DEFINED_TC`	
ステップ 18	**end** 例： `Router(config-pfr-mc-learn-list)# end`	学習リスト 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。

プレフィックス リストを使用した、プレフィックス ベースのトラフィック クラスの手動選択

送信先プレフィックスだけに基づいてトラフィック クラスを手動で選択するには、マスター コントローラで次のタスクを実行します。次のタスクは、トラフィック クラスに選択する送信先プレフィックスが判明している場合に実行します。 送信先プレフィックスを定義するために IP プレフィックス リストが作成され、PfR マップを使用してこのトラフィック クラスのプロファイリングが行われます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. 必要に応じて、追加のプレフィックス リスト エントリに対し、ステップ 3 を繰り返します。
5. **pfr-map** *map-name sequence-number*
6. **match traffic-class prefix-list** *prefix-list-name*
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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} 例： `Router(config)# ip prefix-list PREFIX_TC permit 172.16.1.0/24`	送信先プレフィックスベースのトラフィック クラスを指定するために、プレフィックス リストを作成します。 • 例では、トラフィック クラスに選択される 172.16.1.0/24 送信先プレフィックスを指定する、PREFIX_TC という名前のプレフィックス リストが作成されます。
ステップ 4	必要に応じて、追加のプレフィックス リスト エントリに対し、ステップ 3 を繰り返します。	--
ステップ 5	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map PREFIX_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • permit シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 6 で **match traffic-class prefix-list** コマンドを使用して適用します。 • 例では、PREFIX_MAP という名前の PfR マップが作成されます。
ステップ 6	**match traffic-class prefix-list** *prefix-list-name* 例： `Router(config-pfr-map)# match traffic-class prefix-list PREFIX_TC`	PfR マップを使用して、トラフィック クラスの作成に使用される一致基準として、プレフィックス リストを手動で設定します。 • 例では、PREFIX_TC という名前の IP プレフィックス リストで定義された宛先アドレスを使用してトラフィック クラスが定義されます。
ステップ 7	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

トラフィック クラスおよび学習リストの情報の表示とリセット

トラフィック クラスおよび学習リストの情報を表示し、任意で一部のトラフィック クラス情報をリセットするには、次の作業を実行します。 これらのコマンドは、学習リストが設定されてトラフィック クラスが自動的に学習された後で、またはPfRマップを使用してトラフィック クラスが手動で設定されたときに入力できます。 コマンドは、任意の順番で入力できます。すべてのコマンドは、省略可能です。

手順の概要

1. **enable**
2. **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
3. **show pfr master learn list** [*list-name*]
4. **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

手順の詳細

ステップ1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ2 **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
このコマンドは、学習済みのトラフィック クラス、またはPfR学習リスト コンフィギュレーション モードで手動設定されたトラフィック クラスに関する情報を表示するために使用されます。

例：

```
Router# show pfr master traffic-class

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix          Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
        PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
        ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
```

```
--------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
               #          OOPOLICY       32          10.11.1.3  Gi0/0/0      BGP
               N        N        N        N        N        N        N      IBwN
             130      134        0        0        N        N
```

ステップ 3 **show pfr master learn list** [*list-name*]

このコマンドは、設定された PfR 学習リストの 1 つまたはすべてを表示するために使用されます。 この例では、2 つの学習リストに関する情報が表示されます。

例：

```
Router# show pfr master learn list

Learn-List LIST1 10
   Configuration:
    Application: ftp
    Aggregation-type: bgp
    Learn type: thruput
    Policies assigned: 8 10
   Stats:
    Application Count: 0
    Application Learned:
 Learn-List LIST2 20
   Configuration:
    Application: telnet
    Aggregation-type: prefix-length 24
    Learn type: thruput
    Policies assigned: 5 20
   Stats:
    Application Count: 2
    Application Learned:
     Appl Prefix 10.1.5.0/24 telnet
     Appl Prefix 10.1.5.16/28 telnet
```

ステップ 4 **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

このコマンドは、PfR の制御対象トラフィック クラスをマスター コントローラ データベースからクリアするために使用されます。 次の例では、Telnet アプリケーションおよび 10.1.1.0/24 プレフィックスによって定義されたトラフィック クラスがクリアされます。

例：

```
Router# clear pfr master traffic-class application telnet 10.1.1.0/24
```

測定フェーズのタスク

次のタスクは、PfR 測定フェーズの要素の設定方法を示します。

アウトバウンド トラフィックの PfR リンク使用率の変更

PfR の出口（アウトバウンド）リンク使用率のしきい値を変更するには、マスター コントローラで次のタスクを実行します。 境界ルータ用外部インターフェイスが設定されると、PfR は、境界

ルータ上の外部リンク使用率を 20 秒ごとに自動的に監視します。 使用率はマスター コントローラに報告されます。使用率が 75% を超えると、PfR はこのリンク上のトラフィック クラス用に別の出口リンクを選択します。 キロバイト/秒（kbps）単位の絶対値または割合を指定できます。

着信トラフィックの測定の設定については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **max-xmit-utilization** {**absolute** *kbps* | **percentage** *value*
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Router(config-pfr-mc)# border 10.1.1.2`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界ルータを識別するために、IP アドレスを設定します。 • PfR の管理対象ネットワークを作成するには、少なくとも 1 台の境界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境界ルータは、最大 10 台です。

	コマンドまたはアクション	目的
		（注） 境界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、既存の境界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 5	**interface** *type number* **external** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	PfR 管理の外部インターフェイスとして境界ルータを設定し、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 モードを開始します。 • 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つの外部境界ルータ インターフェイスが必要です。 各境界ルータでは、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。 （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 6	**max-xmit-utilization** {**absolute** *kbps* | **percentage** *value* 例： `Router(config-pfr-mc-br-if)# max-xmit-utilization absolute 500000`	単一の PfR 管理の出口リンクの最大使用率を設定します。 • PfR 管理の出口リンクでの絶対最大使用率を kbps 単位で指定するには、**absolute** キーワードおよび *kbps* 引数を使用します。 • 出口リンクの使用割合を指定するには、**percentage** キーワードおよび *value* 引数を使用します。
ステップ 7	**end** 例： `Router(config-pfr-mc-br-if)# end`	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 モードを終了し、特権 EXEC モードに戻ります。

PfR 出口リンクの使用率範囲の変更

すべての境界ルータで出口リンクの最大使用率範囲のしきい値を変更するには、マスター コントローラで次のタスクを実行します。 デフォルトでは、PfR は境界ルータ上の外部リンクの使用率を 20 秒ごとに自動監視し、境界ルータがマスター コントローラに使用率を報告します。 すべて

の出口リンク間の使用率範囲が20%を超えると、マスターコントローラは、一部のトラフィッククラスを別の出口リンクに移動させることによって、トラフィック負荷の均等化を試みます。 最大使用率の範囲は、割合として設定されます。

PfR は、最大使用率の範囲を使用して、出口リンクがポリシーに準拠しているかどうかを判断します。 PfR は、過剰使用されている、またはポリシー違反の出口から、ポリシー準拠の出口にトラフィック クラスを移動することによって、すべての出口リンクでアウトバウンド トラフィックを均等化します。

（注） リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

着信トラフィックの測定の設定については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max-range-utilization percent** *maximum*
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 4	**max-range-utilization percent** *maximum* 例： `Router(config-pfr-mc)# max-range-utilization percent 25`	すべての PfR 管理の出口リンクに最大使用率の範囲を設定します。 • すべての出口リンク間の最大使用率の範囲を指定するには、**percent** キーワードおよび *maximum* 引数を使用します。 • この例では、境界ルータ上のすべての出口リンク間の最大使用率の範囲が 25% 以内になるように設定されます。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR パッシブ モニタリングの設定および確認

PfR 管理のネットワークが作成されているが、パッシブ モニタリングがディセーブルになることもある場合、PfR は、デフォルトでパッシブ モニタリングをイネーブルにします。 パッシブ モニタリングを設定してから、パッシブ モニタリングが実行されていることを確認するには、次のタスクを使用します。 マスター コントローラで最初の 5 つの手順を実行し、次に境界ルータに移動して、監視対象プレフィックスまたはアプリケーション トラフィック フローについて NetFlow で収集されたパッシブ測定情報を表示します。 **show** コマンドは、アプリケーション トラフィックが通過する境界ルータで入力します。 **show** コマンドは、任意の順番で入力できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode monitor** {**active** | **both**| **fast**| **passive**}
5. **end**
6. いずれかの境界ルータに移動します。
7. **enable**
8. **show pfr border passive cache** {**learned**[**application**| **traffic-class**]}
9. **show pfr border passive prefixes**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **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。

例：

```
Router# configure terminal
```

ステップ 3 **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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

例：

```
Router(config)# pfr master
```

ステップ 4 **mode monitor** {**active** | **both**| **fast**| **passive**}
PfR マスター コントローラでルート モニタリングまたはルート制御を設定します。 アクティブ モニタリング、パッシブ モニタリング、またはアクティブ モニタリングとパッシブ モニタリングの両方を設定するには、**monitor** キーワードを使用します。 パッシブ モニタリングは、**both** キーワードまたは **passive** キーワードのいずれかが指定されている場合にイネーブルになります。 この例では、パッシブ モニタリングがイネーブルになります。

例：

```
Router(config-pfr-mc)# mode monitor passive
```

ステップ 5 **end**
PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Router(config-pfr-mc)# end
```

ステップ 6 いずれかの境界ルータに移動します。

ステップ 7 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 8 **show pfr border passive cache** {**learned**[**application**| **traffic-class**]}

このコマンドは、PfR の監視対象プレフィックスおよびトラフィック フロー用の境界ルータから NetFlow によって収集されたリアルタイムのパッシブ測定情報を表示するために使用します。次の例では、PfR で学習した監視対象アプリケーション トラフィック クラスに関する測定情報の表示に、learned キーワードおよびapplicationキーワードを使用しています。音声トラフィックに関するこの例では、音声アプリケーション トラフィックは、ユーザ データグラム プロトコル（UDP）、DSCP 値 ef、および範囲 3000 ～ 4000 のポート番号により特定されます。

例：

```
Router# show pfr border passive cache learned application
OER Learn Cache:
    State is enabled
    Measurement type: throughput, Duration: 2 min
    Aggregation type: prefix-length, Prefix length: 24
    4096 oer-flows per chunk,
    8 chunks allocated, 32 max chunks,
    5 allocated records, 32763 free records, 4588032 bytes allocated
Prefix          Mask     Pkts  B/Pk  Delay Samples   Active
Prot  Dscp  SrcPort          DstPort
Host1           Host2           Host3           Host4           Host5
dport1          dport2          dport3          dport4          dport5
10.1.3.0         /24     873     28      0       0      13.3
17      ef [1, 65535]       [3000, 4000]
10.1.3.1        0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0
3500             0                0               0               0
10.1.1.0         /24    7674     28      0       0      13.4
17      ef [1, 65535]       [3000, 4000]
10.1.1.1        0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0
3600             0                0               0               0
```

ステップ 9 **show pfr border passive prefixes**

このコマンドは、PfR の監視対象プレフィックスおよびトラフィック フローについて NetFlow によって収集されたパッシブ測定情報を表示するのに使用されます。 次の出力は、**show pfr border passive prefixes** コマンドが実行された境界ルータについて NetFlow によってパッシブ モニタリングが行われたプレフィックスを示します。

例：

```
Router# show pfr border passive prefixes
OER Passive monitored prefixes:
Prefix          Mask   Match Type
10.1.5.0        /24     exact
```

最長一致ターゲット割り当てを使用した PfR アクティブ プローブの設定

最長一致ターゲット割り当てを使用してアクティブ プローブを設定するには、マスター コントローラで次のタスクを実行します。 アクティブ モニタリングは、**mode monitor active** コマンドまたは **mode monitor both** コマンドを使用した場合にイネーブルになります。アクティブ プローブのタイプは、**active-probe**（PfR）コマンドを使用して指定します。 アクティブ プローブは、特定のホストまたはターゲット アドレスを使用して設定し、このアクティブ プローブはボード ルータをソースとします。 アクティブ プローブのソース外部インターフェイスは、最適化されたプレフィックスの優先ルートである場合も、ない場合もあります。この例では、アクティブモニタリングとパッシブ モニタリングの両方がイネーブルであり、ターゲット IP アドレスの 10.1.5.1 は、インターネット制御プロトコル（ICMP）のエコー（ping）メッセージを使用してアクティブに監視されます。 次のタスクでは、IP SLA Responder をイネーブルにする必要はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode monitor** {**active** | **both** | **passive**}
5. **active-probe** {**echo** *ip-address* | **tcp-conn** *ip-address* **target-port** *number* | **udp-echo** *ip-address* **target-port** *number*}
6. **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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**mode monitor** {**active**	**both**	**passive**}	PfR マスター コントローラでルート モニタリングを設定します。

	コマンドまたはアクション	目的
	例： `Router(config-pfr-mc)# mode monitor both`	• アクティブ モニタリング、パッシブ モニタリング、またはその両方を設定するには、**monitor** キーワードを使用します。 • 例では、アクティブ モニタリングとパッシブ モニタリングの両方をイネーブルにします。
ステップ 5	**active-probe** {**echo** *ip-address* | **tcp-conn** *ip-address* **target-port** *number* | **udp-echo** *ip-address* **target-port** *number*} 例： `Router(config-pfr-mc)# active-probe echo 10.1.5.1`	ターゲット プレフィックスのアクティブ プローブを設定します。 • アクティブ プローブは、パッシブ モニタリングだけを行った場合よりも正確にターゲットプレフィックスの遅延およびジッターを測定します。 • アクティブ プローブには、特定のホストまたはターゲット アドレスを設定する必要があります。 • アクティブプローブは、PfR 管理の外部インターフェイスをソースとします。 この外部インターフェイスは、最適化されたプレフィックスの優先ルートである場合も、ない場合もあります。 • UDP エコー プローブを設定する場合、または 23 以外のポート番号で設定される TCP 接続プローブを設定する場合には、ターゲット デバイス上で対応するポート番号を持つリモート レスポンダを設定する必要があります。 リモート レスポンダは、**ip sla monitor responder** グローバル コンフィギュレーション コマンドで設定します。
ステップ 6	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

強制ターゲット割り当てを使用した PfR 音声プローブの設定

PfR ジッター プローブを使用してアクティブ モニタリングをイネーブルにするには、次のタスクを実行します。 この例では、監視対象トラフィックは音声トラフィックであり、アクセスリストを使用して識別されます。 アクティブ音声プローブは、通常の最長一致割り当てのターゲットではなく、PfR の強制ターゲットを割り当てられます。 このタスクでは、PfR プローブ頻度の変更方法も示します。

ソースデバイスで PfR ジッタープローブを設定する前に、ターゲットデバイス（動作のターゲット）で IP SLA Responder をイネーブルにする必要があります。 IP SLA Responder を使用できるのは、Cisco IOS ソフトウェアベースのデバイスだけです。 IP SLA Responder が稼働するネットワーク デバイスで次のタスクを開始します。

（注） IP SLA Responder が稼働するデバイスは、PfR 用に設定されている必要はありません。

はじめる前に

次のタスクを続行する前に、アクセス リストを定義する必要があります。 アクセス リストの例およびアクティブ プローブを使用した音声トラフィックの設定の詳細については、「アクティブ プローブを使用した PfR 音声トラフィック最適化」ソリューション モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. PfR マスター コントローラになっているネットワーク デバイスに移動します。
6. **enable**
7. **configure terminal**
8. **pfr master**
9. **mode monitor** {**active** | **both** | **passive**}
10. **exit**
11. **pfr-map** *map-name sequence-number*
12. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
13. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*]
14. **set probe frequency** *seconds*
15. **set jitter threshold** *maximum*
16. **set mos** {**threshold** *minimum* **percent** *percent*}
17. **set delay** {**relative** *percentage* | **threshold** *maximum*}
18. **end**
19. **show pfr master active-probes** [**appl**| **forced**]

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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip sla monitor responder** 例： `Router(config)# ip sla monitor responder`	IP SLA Responder をイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル 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 5	PfR マスター コントローラになっているネットワーク デバイスに移動します。	--
ステップ 6	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 7	**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 8	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 9	**mode monitor {active | both | passive}** 例： `Router(config-pfr-mc)# mode monitor active`	PfR マスター コントローラでルート モニタリングを設定します。 • アクティブ モニタリング、パッシブ モニタリング、またはその両方を設定するには、**monitor** キーワードを使用します。 • 例では、アクティブ モニタリングが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 10	**exit** 例： `Router(config-pfr-mc)# exit`	PfR マスター コントローラ コンフィギュレーション モードを終了し、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	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map TARGET_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 12 で **match ip address**（PfR）コマンドを使用して適用します。 • 例では、TARGET_MAP という名前の PfR マップが作成されます。
ステップ 12	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} 例： `Router(config-pfr-map)# match ip address access-list VOICE_ACCESS_LIST`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。 • 例では、VOICE_ACCESS_LIST という名前の IP アクセス リストが、PfR マップ内の一致基準として設定されます。
ステップ 13	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*] 例： `Router(config-pfr-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	set 句エントリを作成して、アクティブ プローブのターゲット プレフィックスを割り当てます。 • 4 種類のプローブ タイプ（echo、jitter、tcp-conn、または udp-echo）のうち 1 つを指定するには、*probe-type* 引数を使用します。 • 指定したタイプのプローブを使用して監視されるプレフィックスのターゲット IP アドレスを指定するには、*ip-address* 引数を使用します。 • アクティブ プローブの宛先ポート番号を指定するには、**target-port** キーワードおよび *number* 引数を使用します。 • **codec** キーワードおよび *codec-name* 引数を使用するのは、ジッター プローブ タイプだけです。 平均オピニオン評点（MOS）の計算に使用されるコーデック値を指定します。 コーデック値は、g711alaw、g711ulaw、または g729a のいずれかを指定します。

	コマンドまたはアクション	目的
		• 例では、set 句エントリを作成し、ジッターを使用してアクティブに監視するプレフィックスのターゲット IP アドレスと特定のポート番号を指定しています。
ステップ 14	**set probe frequency** *seconds* 例： `Router(config-pfr-map)# set probe frequency 10`	set 句エントリを作成して、PfR アクティブ プローブの頻度を設定します。 • 指定した IP プレフィックスのアクティブ プローブ モニタリングの間隔を秒単位で設定するには、*seconds* 引数を使用します。 • 例では、アクティブ プローブ頻度を 10 秒に設定する set 句を作成しています。
ステップ 15	**set jitter threshold** *maximum* 例： `Router(config-pfr-map)# set jitter threshold 20`	set 句エントリを作成して、ジッターしきい値を設定します。 • 最大ジッター値をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックのジッターしきい値を 20 に設定する set 句を作成しています。
ステップ 16	**set mos** {**threshold** *minimum* **percent** *percent*} 例： `Router(config-pfr-map)# set mos threshold 4.0 percent 30`	set 句エントリを作成して、代替出口を選択するかどうかの判断に使用される MOS しきい値および割合値を設定します。 • 最低 MOS 値を設定するには **threshold** キーワードを使用します。 • MOS しきい値を下回る MOS 値の割合を設定するには **percent** キーワードを使用します。 • PfR は、5 分間隔で記録された MOS しきい値を下回る MOS 値の割合を計算します。 この割合値が、設定した割合値またはデフォルト値を上回る場合、マスター コントローラは代替出口リンクを検索します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックのしきい値 MOS 値を 4.0 に設定し、割合値を 30% に設定する set 句を作成しています。
ステップ 17	**set delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay threshold 100`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。相対遅延割合は、短期測定値および長期測定値の比較に基づいています。

	コマンドまたはアクション	目的
		• 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 100 ミリ秒に設定する set 句を設定しています。
ステップ 18	**end** 例： `Router(config-pfr-map)# end`	PfR マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 19	**show pfr master active-probes** [**appl**| **forced**] 例： `Router# show pfr master active-probes forced`	PfR マスター コントローラ上のアクティブ プローブに関する接続情報およびステータス情報を表示します。 • このコマンドからの出力には、アクティブ プローブのタイプおよび宛先、アクティブ プローブのソースである境界ルータ、アクティブ プローブに使用されるターゲット プレフィックス、およびプローブが学習済みだったか、または設定済みだったかが表示されます。 • 出力をフィルタリングして、マスター コントローラによって最適化されるアプリケーションに関する情報を表示するには、**appl** キーワードを使用します。 • 割り当てられたすべての強制ターゲットを表示するには、**forced** キーワードを使用します。 • 例では、強制ターゲット割り当てで設定された音声トラフィック用に生成されたアクティブ プローブに関する接続情報およびステータス情報が表示されます。

例

次に、**show pfr master active-probes forced** コマンドからの出力例を示します。 出力はフィルタリングされ、強制ターゲット割り当てで設定された音声トラフィック用に生成されたアクティブ プローブに関する接続情報およびステータス情報だけが表示されます。

```
Router# show pfr master active-probes forced
OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
```

```
The following Forced Probes are running:
Border          State    Policy            Type     Target          TPort
10.20.20.2      ACTIVE   40                jitter   10.20.22.1      3050
10.20.21.3      ACTIVE   40                jitter   10.20.22.4      3050
```

高速フェールオーバー用 PfR 音声プローブの設定

PfR ジッター プローブを使用して高速モニタリングをイネーブルにするには、次のタスクを実行します。 高速フェールオーバー モニタリング モードでは、アクティブ モニタリングとパッシブ モニタリングを使用して、すべての出口が継続的にプローブされます。 高速フェールオーバー モニタリング モードのプローブ頻度は、他のモニタリング モードよりも低く設定できます。これにより、より迅速なフェールオーバー機能が可能になります。 高速フェールオーバー モニタリングは、すべてのタイプのアクティブ プローブ（ICMP エコー、ジッター、TCP 接続、および UDP エコー）で使用できます。

高速フェールオーバー モニタリングは、パフォーマンス上の問題または輻輳したリンクに非常に影響されやすいトラフィック クラス向けに設計されています。音声トラフィックは、ドロップされたリンクに非常に影響されやすいトラフィックです。この例では、高速フェールオーバー モードがイネーブルになり、IP プレフィックス リストを使用して監視対象の音声トラフィックが識別されます。高速フェールオーバー モードで発生するオーバーヘッドを削減するために、アクティブ音声プローブが PfR の強制ターゲットに割り当てられます。 PfR プローブ頻度は、2 秒に設定されます。タスク テーブルの後の例の項では、タスクの手順で指定されたプレフィックスのポリシー設定を表示するために **show pfr master prefix** コマンドが使用されています。また、ロギング出力では高速フェールオーバーが設定されていることを示されています。

（注） 高速モニタリング モードでは、学習済みプレフィックスと同様に、プローブ ターゲットが学習されます。 ネットワーク内で多数のプローブをトリガーしないようにするには、トラフィックがパフォーマンスに影響されやすいリアルタイム アプリケーションと重要アプリケーションにのみ、高速モニタリング モードを使用します。

ソース デバイスで PfR ジッター プローブを設定する前に、ターゲット デバイス（動作のターゲット）で IP SLA Responder をイネーブルにする必要があります。 IP SLA Responder を使用できるのは、Cisco IOS ソフトウェアベースのデバイスだけです。 IP SLA Responder が稼働するネットワーク デバイスで次のタスクを開始します。

（注） IP SLA Responder が稼働するデバイスは、PfR 用に設定されている必要はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. PfR マスター コントローラになっているネットワーク デバイスに移動します。
6. **enable**
7. **configure terminal**
8. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
9. 必要に応じて、追加のプレフィックス リスト エントリについてステップ 4 を繰り返します。
10. **pfr-map** *map-name sequence-number*
11. **match traffic-class prefix-list** *prefix-list-name*
12. **set mode monitor** {**active** | **both**| **fast**| **passive**}
13. **set jitter threshold** *maximum*
14. **set mos** {**threshold** *minimum* **percent** *percent*}
15. **set delay** {**relative** *percentage* | **threshold** *maximum*}
16. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*]
17. **set probe frequency** *seconds*
18. **end**
19. **show pfr master prefix** [*prefix*[**detail**| **policy**| **traceroute**[*exit-id*| *border-address*| **current**]]]

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。 • パスワードを入力します（要求された場合）。
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	**ip sla monitor responder** 例： `Router(config)# ip sla monitor responder`	IP SLA Responder をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル 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 5	PfR マスター コントローラになっているネットワーク デバイスに移動します。	--
ステップ 6	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 7	**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 8	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} 例： `Router(config)# ip prefix-list VOICE_FAIL_LIST permit 10.1.0.0/24`	IP プレフィックス リストを作成します。 • ここで指定する IP プレフィックス リストは PfR マップで使用され、トラフィック クラスの宛先 IP アドレスを指定します。 • 例では、VOICE_FAIL_LIST という名前の IP プレフィックス リストが作成され、PfR で 10.1.0.0/24 プレフィックスのプロファイリングが行われます。
ステップ 9	必要に応じて、追加のプレフィックス リスト エントリについてステップ 4 を繰り返します。	—
ステップ 10	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map FAST_FAIL_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、FAST_FAIL_MAP という名前の PfR マップが作成されます。

	コマンドまたはアクション	目的
ステップ 11	**match traffic-class prefix-list** *prefix-list-name* 例： `Router(config-pfr-map)# match traffic-class prefix-list VOICE_FAIL_LIST`	PfR マップ内のトラフィック クラス一致基準として IP プレフィックス リストを参照します。 • 例では、VOICE_FAIL_LIST という名前の IP プレフィックス リストが、PfR マップ内の一致基準として設定されます。
ステップ 12	**set mode monitor** {**active** | **both**| **fast**| **passive**} 例： `Router(config-pfr-map)# set mode monitor fast`	set 句エントリを作成して、PfR マスター コントローラでルート モニタリングを設定します。 • アクティブ モニタリング、パッシブ モニタリング、またはその両方を設定するには、**monitor** キーワードを使用します。 • 継続的なアクティブ モニタリングおよびパッシブ モニタリングがイネーブルである高速フェールオーバー モニタリング モードを設定するには、**fast** キーワードを使用します。 • 例では、高速フェールオーバー モニタリングがイネーブルになります。
ステップ 13	**set jitter threshold** *maximum* 例： `Router(config-pfr-map)# set jitter threshold 12`	set 句エントリを作成して、ジッターしきい値を設定します。 • 最大ジッター値をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックのジッターしきい値を 12 に設定する set 句が作成されます。
ステップ 14	**set mos** {**threshold** *minimum* **percent** *percent*} 例： `Router(config-pfr-map)# set mos threshold 3.6 percent 30`	set 句エントリを作成して、代替出口を選択するかどうかの判断に使用される MOS しきい値および割合値を設定します。 • 最低 MOS 値を設定するには **threshold** キーワードを使用します。 • MOS しきい値を下回る MOS 値の割合を設定するには **percent** キーワードを使用します。 • PfR は、5 分間隔で記録された MOS しきい値を下回る MOS 値の割合を計算します。 この割合値が、設定した割合値またはデフォルト値を上回る場合、マスター コントローラは代替出口リンクを検索します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックのしきい値 MOS 値を 3.6 に設定し、割合値を 30% に設定する set 句が作成されます。

	コマンドまたはアクション	目的
ステップ 15	**set delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay relative 50`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。 相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの相対遅延割合を 50% に設定する set 句が作成されます。
ステップ 16	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] [**dscp** *value*] 例： `Router(config-pfr-map)# set active-probe jitter 10.120.120.1 target-port 20 codec g729a`	set 句エントリを作成して、アクティブ プローブのターゲット プレフィックスを割り当てます。 • 4 種類のプローブ タイプ（echo、jitter、tcp-conn、または udp-echo）のうち 1 つを指定するには、*probe-type* 引数を使用します。 • 指定したタイプのプローブを使用して監視されるプレフィックスのターゲット IP アドレスを指定するには、*ip-address* 引数を使用します。 • アクティブ プローブの宛先ポート番号を指定するには、**target-port** キーワードおよび *number* 引数を使用します。 • **codec** キーワードおよび *codec-name* 引数を使用するのは、ジッター プローブ タイプだけです。 平均オピニオン評点（MOS）の計算に使用されるコーデック値を指定します。 コーデック値は、g711alaw、g711ulaw、または g729a のいずれかを指定します。 • 例では、set 句エントリを作成し、ジッターを使用してアクティブに監視するプレフィックスのターゲット IP アドレスと特定のポート番号を指定しています。
ステップ 17	**set probe frequency** *seconds* 例： `Router(config-pfr-map)# set probe frequency 2`	set 句エントリを作成して、PfR アクティブ プローブの頻度を設定します。 • 指定した IP プレフィックスのアクティブ プローブ モニタリングの間隔を秒単位で設定するには、*seconds* 引数を使用します。 • 例では、アクティブ プローブ頻度を 2 秒に設定する set 句が作成されます。

	コマンドまたはアクション	目的
		（注） ステップ 12 で高速フェールオーバー モニタリング モードがイネーブルになっているため、ここでは、4 秒未満のプローブ頻度も設定可能です。
ステップ 18	**end** 例： `Router(config-pfr-map)# end`	PfR マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 19	**show pfr master prefix** [*prefix*[**detail**| **policy**| **traceroute**[*exit-id*| *border-address*| **current**]]] 例： `Router# show pfr master prefix 10.1.1.0/24 policy`	（任意）監視対象プレフィックスのステータスを表示します。 • *prefix* 引数は、IP アドレスおよびビット長マスクとして入力します。 • 指定したプレフィックスのポリシー情報を表示するには、**policy** キーワードを使用します。 • 例では、10.1.1.0/24 プレフィックスのポリシー情報が表示されます。

例

次の例は、policy キーワードを使用してプレフィックスを指定したときの **show pfr master prefix** コマンドからの出力です。このコマンドでは、10.1.1.0/24 プレフィックスに設定されたポリシーが表示されます。 mode monitor は fast に設定されています。したがって、select-exit は自動的に best に設定され、probe frequency を 2 に設定できます。

```
Router# show pfr master prefix 10.1.1.0/24 policy
* Overrides Default Policy Setting
pfr-map MAP 10
  sequence no. 8444249301975040, provider id 1, provider priority 30
    host priority 0, policy priority 10, Session id 0
  match ip prefix-lists: VOICE_FAIL_LIST
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
 *probe frequency 2
  mode route control
 *mode monitor fast
 *mode select-exit best
  loss relative 10
 *jitter threshold 12
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 10.120.120.1 target-port 20 codec g729a
```

アクティブ プローブのソース アドレスの設定

アクティブプローブのソースインターフェイスを指定するには、境界ルータで次のタスクを実行します。アクティブ プローブのソース インターフェイスは、境界ルータ上で設定します。PfR 境界ルータ コンフィギュレーション モードで、**active-probe address source**（PfR）を使用します。アクティブ プローブのソース インターフェイス IP アドレスは、プローブ応答が指定したソース インターフェイスに必ず戻されるようにするために、一意である必要があります。

デフォルトの動作は、次のとおりです。

- このコマンドがイネーブルではない、または**no**形式を入力した場合、ソースIPアドレスは、アクティブ プローブを送信するデフォルトのPfR外部インターフェイスから使用されます。
- インターフェイスに IP アドレスが設定されていない場合、アクティブ プローブは生成されません。
- インターフェイスがアクティブ プローブのソースとして設定された後で IP アドレスが変更されると、アクティブ プローブは停止し、新しい IP アドレスで再開します。
- インターフェイスがアクティブ プローブのソースとして設定された後で IP アドレスが削除されると、アクティブ プローブは停止します。有効なプライマリ IP アドレスが設定されるまで再開しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr border**
4. **active-probe address source interface** *type number*
5. **end**
6. **show pfr border active-probes**

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。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**pfr border** 例： `Router(config)# pfr border`	PfR 境界ルータ コンフィギュレーション モードを開始して、ルータを境界ルータとして設定します。
ステップ 4	**active-probe address source interface** *type number* 例： `Router(config-pfr-br)# active-probe address source interface GigabitEthernet 0/0/0`	境界ルータ上のインターフェイスをアクティブ プローブのソースとして設定します。 • 例では、GigabitEthernet 0/0/0 インターフェイスがソース インターフェイスとして設定されます。
ステップ 5	**end** 例： `Router(config-pfr-br)# end`	PfR 境界ルータ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**show pfr border active-probes** 例： `Router# show pfr border active-probes`	PfR 境界ルータ上のアクティブ プローブに関する接続情報およびステータス情報を表示します。 • このコマンドを使用すると、設定されたソース IP アドレスを確認できます。

ポリシー適用フェーズのタスク

次のタスクは、PfR ポリシー適用フェーズの要素の設定方法を示します。

PfR ポリシーの設定および学習済みトラフィック クラスへの適用

PfR ポリシーを設定し、学習済みトラフィック クラスに適用するには、マスター コントローラで次のタスクを実行します。 **pfr master** コマンドを使用して PfR マスター コントローラとしてルータを設定した後は、このタスクのほとんどのコマンドは省略可能です。 各ステップでは、グローバル ベースで学習済みトラフィック クラスに適用されるパフォーマンス ポリシーが設定されます。 この例では、PfR は、ポリシー準拠の最初の出口を選択するように設定されます。

次のタスクでは、一部の PfR タイマーが変更されます。 PfR タイマーの調整を行う際は、新しい設定値が残り時間よりも少ないと、既存の設定はただちに新しいタイマー設定に置き換えられることに注意してください。 値が残り時間よりも多い場合、既存タイマーが期限切れになるか、リセットされると、新しい設定が適用されます。

（注） 極端なタイマー設定を行うと、出口リンクまたはトラフィック クラス エントリがポリシー違反状態になることがあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **backoff** *min-timer max-timer* [*step-timer*]
5. **delay** {**relative** *percentage* | **threshold** *maximum*}
6. **holddown** *timer*
7. **loss** {**relative** *average* | **threshold** *maximum*}
8. **periodic** *timer*
9. **unreachable** {**relative** *average* | **threshold** *maximum*}
10. **mode select-exit** {**best** | **good**}}
11. **end**
12. **show pfr master policy** [*sequence-number*|*policy-name* | **default**]

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。 • パスワードを入力します（要求された場合）。
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	**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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**backoff** *min-timer max-timer* [*step-timer*] 例： `Router(config-pfr-mc)# backoff 400 4000 400`	（任意）バックオフ タイマーを設定して、ポリシー決定期間を調整します。 • 最低移行期間を秒単位で設定するには、*min-timer* 引数を使用します。 • トラフィック クラス エントリのポリシー要件を満たすリンクがない場合に PfR がポリシー違反トラフィック クラスを保持する最大期間を設定するには、*max-timer* 引数を使用します。 • *step-timer* 引数を使用すると、最大制限時間に達するまで最低タイマーの期限が切れるたびに時間を追加するように PfR を任意で設定できます。
ステップ 5	**delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-mc)# delay relative 80`	（任意）遅延しきい値を相対割合または絶対値で設定します。 • 相対遅延割合を設定するには **relative** キーワードを使用します。 相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 設定した遅延しきい値を超えると、プレフィックスはポリシー違反になります。 • 例では、相対平均に基づいて 80% の遅延しきい値が設定されます。
ステップ 6	**holddown** *timer* 例： `Router(config-pfr-mc)# holddown 600`	（任意）トラフィック クラス エントリのルート ダンプニング タイマーを設定して、代替出口が選択可能になる前に新しい出口の使用が必要な最低期間を設定します。 • トラフィック クラス エントリがホールドダウン状態の間は、PfR はルート変更を実行できません。 • ホールドダウン タイマーの期限が切れると、PfR は、パフォーマンスおよびポリシー設定に基づいて最良の出口を選択します。 • トラフィック クラス エントリの現在の出口が到達不能になると、PfR は、代替パスの検索プロセスを開始します。 • 例では、トラフィック クラスエントリのダンプニング タイマーが 600 秒に設定されます。
ステップ 7	**loss** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-mc)# loss relative 20`	（任意）PfR がトラフィック クラス エントリに許可する相対パケット損失または最大パケット損失を設定します。 • **relative** キーワードは、短期間のパケット損失割合および長期間のパケット損失割合の比較に基づいてパケットの相対割合を設定します。

	コマンドまたはアクション	目的
		• **threshold** キーワードは、絶対パケット数（百万パケットあたりのパケット数）を設定します。 • 例では、パケット損失の比較割合が 20% 以上の場合にマスター コントローラが新しい出口リンクを検索するように設定されます。
ステップ 8	**periodic** *timer* 例： `Router(config-pfr-mc)# periodic 300`	（任意）周期タイマーの期限が切れると、最良の出口リンクを定期的に選択するように PfR を設定します。 • このコマンドがイネーブルの場合、マスター コントローラが定期的に評価し、トラフィック クラスのポリシー決定を行います。 • 例では、周期タイマーが 300 秒に設定されます。 タイマーの期限が切れると、PfR は最良の出口またはポリシー準拠の最初の出口のいずれかを選択します。 （注） このタイマーの期限が切れたときに PfR がポリシー準拠の最初の出口を選択するか、利用可能な最良の出口を選択するかを決定するには、**mode select-exit** コマンドを使用します。
ステップ 9	**unreachable** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-mc)# unreachable relative 10`	（任意）到達不能ホストの最大数を設定します。 • このコマンドは、PfR がトラフィック エントリに許可する到達不能ホストの相対割合または最大数（100 万フローあたりのフロー数（fpm））を指定するために使用します。 到達不能ホストの絶対数または相対割合がユーザ定義の値またはデフォルト値を超える場合、PfR はトラフィック クラス エントリが OOP であると判断し、代替出口リンクを検索します。 • 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。 到達不能ホストの相対割合は、短期測定値および長期測定値の比較に基づいています。 • 到達不能ホストの絶対最大数を fpm に基づいて設定するには **threshold** キーワードを使用します。 • 例では、到達不能ホストの相対割合が 10% 以上の場合にトラフィック クラス エントリの新しい出口リンクを検索するように PfR が設定されます。
ステップ 10	**mode select-exit** {**best** | **good**}} 例： `Router(config-pfr-mc)# mode select-exit good`	パフォーマンスまたはポリシーに基づいて、出口リンクを選択できるようにします。 • マスター コントローラが、**best** キーワードが入力されたときに利用可能な最良の出口を選択するか、**good** キーワードが入力されたときにポリシー準拠の最初の出口を選択するかを設定するには **select-exit** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show pfr master policy** [*sequence-number*|*policy-name* | **default**] 例： `Router# show pfr master policy`	PfR マスター コントローラ上のポリシー設定を表示します。 • このコマンドの出力では、デフォルトのポリシーおよび任意で PfR マップに設定されているポリシーが表示されます。 • 指定した PfR マップ シーケンスのポリシー設定を表示するには *sequence-number* 引数を使用します。 • 指定した PfR ポリシー マップ名のポリシー設定を表示するには *policy-name* 引数を使用します。 • デフォルトのポリシー設定だけを表示するには、**default** キーワードを使用します。 • 例では、デフォルトのポリシー設定および次のタスクの設定によって更新されたポリシー設定が表示されます。

例

次に、**show pfr master policy** コマンドからの出力例を示します。 次のタスクの設定によって特定のポリシー設定が上書きされた部分を除いて、デフォルトのポリシー設定が表示されます。

```
Router# show pfr master policy
Default Policy Settings:
  backoff 400 4000 400
  delay relative 80
  holddown 600
  periodic 300
  probe frequency 56
  mode route observe
  mode monitor both
  mode select-exit good
  loss relative 20
  unreachable relative 10
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
 *tag 0
```

学習済みプレフィックスの PfR 最適化の防止

PfR が指定した学習済みプレフィックスを最適化しないようにするために PfR ポリシーを設定および適用するには、マスター コントローラで次のタスクを実行します。 次のタスクは、PfR 最適化から除外する一部のプレフィックスが判明しているものの、これらのプレフィックスが PfR で

自動的に学習される場合に便利です。次のタスクでは、IPプレフィックスリストは、最適化されない異なるプレフィックスに対する 2 つのエントリで設定されます。 PfR マップは、1 つのシーケンスの2つのエントリで設定されます。これによって、プレフィックスは学習されますが、PfR は、プレフィックス リストで指定したプレフィックスを最適化しなくなります。 PfR マップ エントリのシーケンス番号が逆方向になった場合、PfR はプレフィックスを学習し、プレフィックスの最適化を試みます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*}
4. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*}
5. **pfr-map** *map-name sequence-number*
6. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
7. **exit**
8. **pfr-map** *map-name sequence-number*
9. **match pfr learn** {**delay**| **inside**| **throughput**}
10. **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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*} 例： `Router(config)# ip prefix-list DENY_LIST deny 10.1.1.0/24`	IP プレフィックス リストを作成します。 • IP プレフィックス リストは、マスター コントローラによるモニタリング用のプレフィックスを手動で拒否する、または許可するために使用されます。 • IPプレフィックスリストで指定されたプレフィックスは、**match ip address**（PfR）コマンドで PfR マップにインポートされます。

	コマンドまたはアクション	目的
		• 例では、10.1.1.0/24 サブネットからのプレフィックスだけを拒否するエントリを含む IP プレフィックス リストが作成されます。
ステップ 4	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network / length*| **permit** *network / length*} 例： `Router(config)# ip prefix-list DENY_LIST deny 172.20.1.0/24`	IP プレフィックス リストを作成します。 • IP プレフィックス リストは、マスター コントローラによるモニタリング用のプレフィックスを手動で拒否する、または許可するために使用されます。 • IPプレフィックスリストで指定されたプレフィックスは、**match ip address**（PfR）コマンドで PfR マップにインポートされます。 • 例では、172.20.1.0/24 サブネットからのプレフィックスだけを拒否する IP プレフィックス エントリが作成されます。
ステップ 5	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map DENY_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 6 で **match ip address**（PfR）コマンドを使用して適用します。 • 例では、シーケンス番号が 10 の DENY_MAP という名前の PfR マップが作成されます。
ステップ 6	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} 例： `Router(config-pfr-map)# match ip address prefix-list DENY_LIST`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックス リストを参照します。 • 例では、DENY_LIST という名前のプレフィックス リストが、PfR マップ内の一致基準として設定されます。
ステップ 7	**exit** 例： `Router(config-pfr-map)# exit`	PfR マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map DENY_MAP 20`	PfR マップ エントリを入力します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 9 で **match ip address**（PfR）コマンドを使用して適用します。 • 例では、シーケンス番号が 20 の DENY_MAP という名前の PfR マップの PfR マップ エントリを作成します。
ステップ 9	**match pfr learn** {**delay**| **inside**| **throughput**} 例： `Router(config-pfr-map)# match pfr learn throughput`	学習済みの PfR プレフィックスに一致させるために、PfR マップ内で match 句エントリを作成します。 • PfR は、最高遅延または最高アウトバウンドスループットに基づいた内部プレフィックスまたはプレフィックスであるトラフィック クラスを学習するように設定できます。 • 例では、最高スループットに基づいて学習されたトラフィック クラスに一致する match 句エントリが作成されます。
ステップ 10	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

PfR マップ用ポリシー ルールの設定

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、PfR マップを選択し設定を適用するには、次のタスクを実行します。 **policy-rules**（PfR）コマンドを使用すると、定義済み PfR マップ間の切り替えを容易に実行できます。

はじめる前に

少なくとも 1 つの PfR マップを設定しなければ、ポリシー ルールのサポートはイネーブルにできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **policy-rules** *map-name*
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。 • パスワードを入力します（要求された場合）。
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	**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、グローバル プレフィックスおよび出口リンク ポリシーを設定します。
ステップ 4	**policy-rules** *map-name* 例： `Router(config-pfr-mc)# policy-rules TARGET_MAP`	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、PfR マップからマスター コントローラ コンフィギュレーションに設定を適用します。 • 新しい PfR マップ名でこのコマンドを再入力すると、以前の設定がただちに上書きされます。 この動作は、定義済みの PfR 間での迅速な選択および切り替えを可能にするように設計されています。 • 例では、TARGET_MAP という名前の PfR マップから設定が適用されます。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

複数 PfR ポリシーの競合解決の設定

PfR 解決機能を使用して、最初に実行される PfR ポリシーに関する競合を回避するためのプライオリティをポリシーに割り当てるには、次のタスクを実行します。 各ポリシーに一意の値が割り当てられ、最高値を設定されたポリシーが最高プライオリティとして選択されます。 デフォルトでは、遅延ポリシーに最高プライオリティが設定され、トラフィック負荷（使用率）ポリシーに 2 番目に高いプライオリティが設定されます。 いずれかのポリシーにプライオリティ値を割り当てると、デフォルト設定が上書きされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **resolve** {**cost priority** *value*| **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
5. ステップ 4 を繰り返して、必要な各 PfR ポリシーにプライオリティを割り当てます。
6. **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。 • パスワードを入力します（要求された場合）。
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	**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 モードを開始します。
ステップ 4	**resolve** {**cost priority** *value*| **delay priority** *value* **variance** *percentage*	**loss priority** *value* **variance** *percentage*	**range priority** *value*	**utilization priority** *value* **variance** *percentage*}	ポリシープライオリティを設定するか、ポリシーの競合を解決します。 • このコマンドは、同じプレフィックスに対して複数のポリシーが設定されている場合にプライオリティを設定するため

	コマンドまたはアクション	目的
	例： `Router(config-pfr-mc)# resolve loss priority 2 variance 10`	に使用されます。 このコマンドが設定されている場合、最高プライオリティのポリシーが選択されて、ポリシー決定を行います。 • プライオリティ値を指定するには、**priority** キーワードを使用します。 1という番号を設定すると、ポリシーに最高プライオリティが割り当てられます。 10 という番号を設定すると、最低プライオリティが割り当てられます。 • 各ポリシーには、異なるプライオリティ番号を割り当てる必要があります。 • ユーザ定義のポリシーに許容分散を設定するには、**variance** キーワードを使用します。 このキーワードでは、出口リンクまたはプレフィックスがユーザ定義のポリシー値と異なっても、まだ同等であると見なす許容割合が設定されます。 • 例では、損失ポリシーのプライオリティが、10%の分散で2に設定されます。 （注） 範囲またはコスト ポリシーには分散を設定できません。
ステップ 5	ステップ 4 を繰り返して、必要な各 PfR ポリシーにプライオリティを割り当てます。	--
ステップ 6	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

PfR マップを使用したブラック ホール ルーティングの設定

ヌルインターフェイスに転送されるパケット、つまり、「ブラック ホール」に廃棄されるパケットをフィルタリングするために PfR マップを設定するには、次のタスクを実行します。IP プレフィックスが、ネットワーク上の攻撃のソースとして識別されると、プレフィックス リストが設定されます。 BGP など一部のプロトコルでは、ブラック ホール ルートの再配布が許可されますが、他のプロトコルでは許可されません。

この省略可能なタスクを実行すると、ネットワーク上での攻撃を阻止したり、軽減したりできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length*| **permit** *network*/*length*}
4. **pfr-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set interface null0**
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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length*| **permit** *network*/*length*} 例： `Router(config)# ip prefix-list BLACK_HOLE_LIST seq 10 permit 10.20.21.0/24`	IP プレフィックス リストを作成します。 • IP プレフィックス リストは、PfR マスター コントローラでモニタリングするプレフィックスを手動で選択するために使用されます。 • マスター コントローラは、デフォルト ルートを含む任意の長さの、完全に一致するプレフィックスを監視し、制御できます。 完全に一致するプレフィックスが指定される場合、PfR は、この完全に一致するプレフィックスだけを監視します。 • IPプレフィックスリストで指定されたプレフィックスは、**match ip address**（PfR）コマンドを使用して PfR マップにインポートします。 • 例では、10.20.21.0/24 サブネットからのプレフィックスを許可する、BLACK_HOLE_LIST という名前の IP プレフィックス リストが作成されます。

	コマンドまたはアクション	目的
ステップ 4	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map BLACK_HOLE_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから前のステップで **match ip address**（PfR）コマンドを使用して適用します。 • 例では、BLACK_HOLE_MAP という名前の PfR マップが作成されます。
ステップ 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} 例： `Router(config-pfr-map)# match ip address prefix-list BLACK_HOLE_LIST`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。 • 例では、PfR マップ内の一致基準として BLACK_HOLE_LIST という名前の IP プレフィックス リストが、設定されます。
ステップ 6	**set interface null0** 例： `Router(config-pfr-map)# set interface null0`	set 句エントリを作成して、パケットをヌル インターフェイスに転送します（つまり、パケットが廃棄されます）。 • 例では、BLACK_HOLE_LIST プレフィックス リストに一致するパケットが廃棄されるように指定するための set 句エントリが作成されます。
ステップ 7	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

PfR マップを使用したシンクホール ルーティングの設定

PfR マップを設定して、ネクスト ホップに転送されるパケットをフィルタリングするには、次のタスクを実行します。ネクストホップは、パケットの保存、分析、または廃棄を実行できるルータです（シンクホールアナロジー）。IPプレフィックスがネットワーク上の攻撃のソースとして識別されると、プレフィックス リストが設定されます。

この省略可能なタスクを実行すると、ネットワーク上での攻撃を阻止したり、軽減したりできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*}
4. **pfr-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set next-hop** *ip-address*
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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*| **permit** *network/length*} 例： `Router(config)# ip prefix-list SINKHOLE_LIST seq 10 permit 10.20.21.0/24`	IP プレフィックス リストを作成します。 • IP プレフィックス リストは、PfR マスター コントローラでモニタリングするプレフィックスを手動で選択するために使用されます。 • マスター コントローラは、デフォルト ルートを含む任意の長さの、完全に一致するプレフィックスを監視し、制御できます。 完全に一致するプレフィックスが指定される場合、PfR は、この完全に一致するプレフィックスだけを監視します。 • IPプレフィックスリストで指定されたプレフィックスは、**match ip address**（PfR）コマンドを使用してPfRマップにインポートします。 • 例では、10.20.21.0/24 サブネットからのプレフィックスを許可する、SINKHOLE_LIST という名前の IP プレフィックス リストが作成されます。

	コマンドまたはアクション	目的
ステップ 4	**pfr-map** *map-name sequence-number* 例： `Router(config-pfr-mc)# pfr-map SINKHOLE_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから前のステップで **match ip address**（PfR）コマンドを使用して適用します。 • 例では、SINKHOLE_MAP という名前の PfR マップが作成されます。
ステップ 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} 例： `Router(config-pfr-map)# match ip address prefix-list SINKHOLE_LIST`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。 • 例では、PfR マップ内の一致基準として SINKHOLE_LIST という名前の IP プレフィックス リストが設定されます。
ステップ 6	**set next-hop** *ip-address* 例： `Router(config-pfr-map)# set next-hop 10.20.21.6`	パケットがネクスト ホップに転送されるように指定する set 句エントリを作成します。 • 例では、SINKHOLE_LISTプレフィックス リストに一致するパケットが 10.20.21.6 のネクスト ホップに転送されるように指定するための set 句エントリが作成されます。
ステップ 7	**end** 例： `Router(config)# end`	（任意）PfR マップ 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。

施行フェーズのタスク

次のタスクは、PfR ポリシーの設定および適用フェーズの要素の設定方法を示します。

アプリケーション トラフィックの制御

アプリケーショントラフィックを制御するには、マスターコントローラで次のタスクを実行する必要があります。次のタスクは、ポリシーベース ルーティング（PBR）を使用して、指定したアプリケーショントラフィック クラスをPfRで制御できるようにする方法を示します。アプリケーション アウェア ポリシー ルーティングを使用して、拡張 IP アクセス リストで permit 文を使用したフィルタリングが可能なアプリケーション トラフィックを設定します。

Telnet トラフィックなどのアプリケーション トラフィックは遅延に影響されやすいので、TCP 遅延が長い場合は、Telnetセッションの使用が困難になることがあります。次のタスクでは、Telnetトラフィックを許可するために拡張 IP アクセス リストが設定されます。 PfR マップは、192.168.1.0/24 ネットワークをソースとする Telnet トラフィックに一致させるために match 句を参照する拡張アクセス リストで設定されます。 PfR ルート制御がイネーブルになり、遅延ポリシーが設定されて、Telnet トラフィックが 30 ミリ秒以下の応答時間で出口リンクを経由して送信されるようになります。 この設定は、**show pfr master appl** コマンドを使用して確認します。

（注）
- 境界ルータは、シングルホップのピアである必要があります。
- 名前付き拡張 IP アドレス リストだけがサポートされます。
- アプリケーション トラフィックの最適化は、CEF スイッチング パス上での PfR だけでサポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*}
4. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*][**precedence** *precedence*][**tos** *tos*] [**ttl** *operator value*] [**log]**[**time-range** *time-range-name*][**fragments**]
5. **exit**
6. **pfr-map** *map-name sequence-number*
7. **match ip address** {*access-list name*| *prefix-list name*}
8. **set mode route control**
9. set delay {**relative** *percentage* | **threshold** *maximum*}
10. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
11. **end**
12. **show pfr master appl** [**access-list** *name*] [**detail**] | [**tcp** | **udp**] [*protocol-number*] [*min-port max-port*] [**dst** | **src**] [**detail** | **policy**]

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。 • パスワードを入力します（要求された場合）。
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	**ip access-list** {**standard** | **extended**} *access-list-name*} 例： `Router(config)# ip access-list extended TELNET_ACL`	拡張アクセス リストを作成し、拡張アクセス リスト コンフィギュレーション モードを開始します。 • 名前付きアクセス リストだけがサポートされます。
ステップ 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*][**precedence** *precedence*][**tos** *tos*] [**ttl** *operator value*] [**log**][**time-range** *time-range-name*][**fragments**] 例： `Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq telnet`	拡張アクセス リストを定義します。 • 任意のプロトコル、ポート、またはその他の IP パケット ヘッダー値を指定できます。 • 例では、192.168.1.0/24 ネットワークをソースとする Telnet トラフィックが許可されます。
ステップ 5	**exit** 例： `Router(config-ext-nacl)# exit`	拡張アクセス リスト 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 6	**pfr-map** *map-name sequence-number* 例： `Router(config# pfr-map BLUE`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。
ステップ 7	**match ip address** {*access-list name*| *prefix-list name*} 例： `Router(config-pfr-map)# match ip address access-list TELNET`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。 • 拡張 IP アクセス リストは、監視対象プレフィックスからトラフィックのサブセットをフィルタリングするために使用されます。

	コマンドまたはアクション	目的
ステップ 8	**set mode route control** 例： `Router(config-pfr-map)# set mode route control`	一致したトラフィックのルート制御を設定するために、set 句エントリを作成します。 • 制御モードでは、マスターコントローラが監視対象プレフィックスを分析し、ポリシーパラメータに基づいて変更を実行します。 • この例では、PfR 制御モードをイネーブルにする set 句を作成しています。
ステップ 9	set delay {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay threshold 30`	（任意）PfR が遅延しきい値を設定するように PfR マップを設定します。 • この例では、遅延ポリシーを設定しています。他のポリシーも設定できます。 • Telnet トラフィックの遅延しきい値が 30 ミリ秒に設定されます。
ステップ 10	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} 例： `Router(config-pfr-map)# set resolve delay priority 1 variance 20`	（任意）ポリシーを上書きするためにポリシー プライオリティを設定するように PfR マップを設定します。 • 解決ポリシーは、遅延ポリシーを 20% の分散の最高プライオリティに設定します。
ステップ 11	**end** 例： `Router(config-pfr-map)# end`	PfR マップ 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 12	**show pfr master appl** [**access-list** *name*] [**detail**] | [**tcp** | **udp**] [*protocol-number*] [*min-port max-port*] [**dst** | **src**] [**detail** | **policy**] 例： `Router# show pfr master appl tcp 23 23 dst policy`	（任意）PfR マスター コントローラによって監視され、制御されるアプリケーションに関する情報を表示します。

例

次の例では、ポート 23（Telnet）に基づいてフィルタリングされる TCP アプリケーション トラフィックを表示する、**show pfr master appl** コマンドの出力を示します。

```
Router# show pfr master appl tcp 23 23 dst policy

Prefix              Appl Prot       Port                 Port Type       Policy
-------------------------------------------------------------------------------
10.1.1.0/24         tcp             [23, 23]             src             10
```

確認フェーズのタスク

次のタスクは、PfR 確認フェーズの要素の設定方法を示します。

PfR ルート強制変更の手動確認

PfR は、NetFlow 出力を使用して、ネットワーク内のルート強制変更を自動的に確認します。 PfR は NetFlow メッセージを監視し、メッセージでルート強制変更を確認できない場合は、トラフィック クラスを制御しません。 PfR 施行フェーズで実行されたトラフィック制御が実際にトラフィック フローを変更し、OOP イベントをポリシー準拠に変更したことを手動で確認する場合は、この任意のタスクのステップを実行します。 すべてのステップは任意ですが、順番は任意ではありません。 これらのステップから得られる情報では、トラフィック クラスに関連付けられた特定のプレフィックスが、別の出口リンク インターフェイスまたは入口リンク インターフェイスに移動されたか、または PfR によって制御されているかを確認できます。 最初の 3 つのコマンドは、マスター コントローラで入力します。最後の 2 つのコマンドは、境界ルータで入力します。 他の PfR 表示コマンドの詳細については、『*Cisco IOS Optimized Edge Routing Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **show logging** [**slot** *slot-number* |**summary**]
3. **show pfr master prefix** *prefix* [**detail**]
4. 境界ルータに移動して、次のステップを開始します。
5. **enable**
6. **show pfr border routes** {**bgp** | **cce** | **eigrp** [**parent**] | **rwatch** | **static**}

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show logging** [**slot** *slot-number* |**summary**]

このコマンドは、システム ロギング（syslog）の状態および標準的なシステム ロギング バッファの内容を表示するために使用します。 省略可能な区切り文字を使用したこの例では、OOP であり、ルート変更が行われた 10.1.1.0 プレフィックスについての PfR メッセージが含まれるロギング バッファが示されます。

例：

```
Router# show logging | i 10.1.1.0

*Apr 26 22:58:20.919: %OER_MC-5-NOTICE: Discovered Exit for prefix 10.1.1.0/24, BR
10.10.10.1, i/f Gi0/0/1
*Apr 26 23:03:14.987: %OER_MC-5-NOTICE: Route changed 10.1.1.0/24, BR 10.10.10.1, i/f
Gi0/2/0, Reason Delay, OOP Reason Timer Expired
*Apr 26 23:09:18.911: %OER_MC-5-NOTICE: Passive REL Loss OOP 10.1.1.0/24, loss 133, BR
10.10.10.1, i/f Gi0/2/0, relative loss 23, prev BR Unknown i/f Unknown
*Apr 26 23:10:51.123: %OER_MC-5-NOTICE: Route changed 10.1.1.0/24, BR 10.10.10.1, i/f
Gi0/0/1, Reason Delay, OOP Reason Loss
```

ステップ 3 **show pfr master prefix** *prefix* [**detail**]

このコマンドは、監視対象プレフィックスの状態を表示するために使用します。 このコマンドからの出力には、送信元境界ルータ、現在の出口インターフェイス、プレフィックス遅延、出口インターフェイスの帯域幅、および入口インターフェイスの帯域幅に関する情報が含まれています。 この例では、出力で 10.1.1.0 プレフィックスのフィルタリングが行われ、現在ホールドダウン状態のプレフィックスが表示されます。 このステップでは、次のタスクに関連する構文だけを示します。

例：

```
Router# show pfr master prefix 10.1.1.0

Prefix          State   Time Curr BR     CurrI/F     Protocol
           PasSDly PasLDly  PasSUn  PasLUn PasSLos PasLLos
           ActSDly ActLDly  ActSUn  ActLUn   EBw   IBw
------------------------------------------------------------------------------
10.1.1.0/24   HOLDDOWN  42 10.10.10.1   Gi0/0/1     STATIC
                16      16       0       0       0       0
                 U       U       0       0      55       2
```

ステップ 4 境界ルータに移動して、次のステップを開始します。

次のコマンドは、マスター コントローラではなく、境界ルータで入力します。

例：

ステップ 5 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 6 **show pfr border routes {bgp | cce | eigrp [parent] | rwatch | static}**

このコマンドは、境界ルータで入力します。 このコマンドは、境界ルータ上の PfR 制御ルートに関する情報を表示するために使用します。 この例の出力では、PfR によって制御される 10.1.1.0 プレフィックスが示されます。

例：

```
Router# show pfr border routes bgp

OER BR 10.10.10.1 ACTIVE, MC 10.10.10.3 UP/DOWN: UP 00:10:08,
   Auth Failures: 0
   Conn Status: SUCCESS, PORT: 3949
BGP table version is 12, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
OER Flags: C - Controlled, X - Excluded, E - Exact, N - Non-exact, I - Injected
    Network          Next Hop        OER    LocPrf Weight Path
*> 10.1.1.0/24     10.40.40.2         CE         0 400 600 i
```

アドバンスド パフォーマンス ルーティングの設定例

プロファイル フェーズのタスクの例

自動的に学習されたプレフィックスベースのトラフィック クラスの学習リストの定義例

マスターコントローラ上で設定された次の例では、プレフィックス リストだけに基づいて自動的に学習されたトラフィック クラスを含む学習リストが定義されます。 この例では、3 つの支社があり、支社 A および B へのすべてのトラフィックを 1 つのポリシー（Policy1）を使用して最適化し、支社 C へのトラフィックを別のポリシー（Policy2）を使用して最適化することが目的です。

支社 A は、10.1.0.0./16 に一致するすべてのプレフィックスとして定義され、支社 B は、10.2.0.0./16 に一致するすべてのプレフィックスとして定義されます。支社 C は、10.3.0.0./16 に一致するすべてのプレフィックスとして定義されます。

次のタスクでは、最高アウトバウンド スループットに基づいたプレフィックスの学習が設定されます。

```
ip prefix-list BRANCH_A_B permit seq 10 10.1.0.0/16
ip prefix-list BRANCH_A_B permit seq 20 10.2.0.0/16
```

```
ip prefix-list BRANCH_C permit seq 30 10.3.0.0/16
pfr master
 learn
 list seq 10 refname LEARN_BRANCH_A_B
 traffic-class prefix-list BRANCH_A_B
 throughput
 exit
 exit
 learn
 list seq 20 refname LEARN_BRANCH_C
 traffic-class prefix-list BRANCH_C
 throughput
 exit
 exit
pfr-map POLICY1 10
 match learn list LEARN_BRANCH_A_B
 exit
pfr-map POLICY2 10
 match learn list LEARN_BRANCH_C
 end
```

アクセス リストを使用して自動的に学習されたアプリケーション トラフィック クラスの学習リストの定義例

次の例では、カスタム アプリケーション トラフィック クラスを定義するアクセス リストが作成されます。 この例のカスタム アプリケーションは、次の 4 つの基準で構成されます。

- 宛先ポート 500 上のすべての TCP トラフィック
- 700 ～ 750 の範囲のポート上のすべての TCP トラフィック
- 送信元ポート 400 上のすべての UDP トラフィック
- ef の DSCP ビットでマーキングされた、すべての IP パケット

ここでの目的は、POLICY_CUSTOM_APP という名前の PfR ポリシー内で参照されている学習リストを使用して、カスタム アプリケーション トラフィックを最適化することです。 次のタスクでは、最高アウトバウンドスループットに基づいたトラフィック クラスの学習が設定されます。

```
ip access-list extended USER_DEFINED_TC
 permit tcp any any 500
 permit tcp any any range 700 750
 permit udp any eq 400 any
 permit ip any any dscp ef
 exit
pfr master
 learn
  list seq 10 refname CUSTOM_APPLICATION_TC
  traffic-class access-list USER_DEFINED_TC
  aggregation-type prefix-length 24
  throughput
  exit
 exit
pfr-map POLICY_CUSTOM_APP 10
 match learn list CUSTOM_APPLICATION_TC
 end
```

プレフィックスリストを使用した、プレフィックスベースのトラフィック クラスの手動選択例

次の例は、マスターコントローラ上で設定されます。トラフィック クラスが、送信先プレフィックスだけに基づいて手動で選択されます。次のタスクは、トラフィック クラスに選択する送信先プレフィックスが判明している場合に実行します。送信先プレフィックスを定義するためにIPプレフィックス リストが作成され、PfR マップを使用してこのトラフィック クラスのプロファイリングが行われます。

```
ip prefix-list PREFIX_TC permit 10.1.1.0/24
ip prefix-list PREFIX_TC permit 10.1.2.0/24
ip prefix-list PREFIX_TC permit 172.16.1.0/24
pfr-map PREFIX_MAP 10
 match traffic-class prefix-list PREFIX_TC
```

アクセス リストを使用したアプリケーション トラフィック クラスの手動選択例

次の例は、マスター コントローラ上で設定されます。トラフィック クラスが、アクセス リストを使用して手動で選択されます。アクセスリストの各エントリは、トラフィック クラスであり、送信先プレフィックスが必ず含まれています。他の省略可能なパラメータが含まれていることもあります。

```
ip access-list extended ACCESS_TC
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800any any dscp ef
 exit
pfr-map ACCESS_MAP 10
 match traffic-class access-list ACCESS_TC
```

測定フェーズのタスクの例

発信トラフィックの PfR リンク使用率の変更例

次に、PfR 出口リンクの使用率のしきい値を変更する例を示します。 この例では、出口使用率は 80% に設定されています。 この出口リンクの使用率が 80 % を超えると、PfR は、この出口リンクを使用していたトラフィック クラスのために別の出口リンクを選択します。

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.1.4.1
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br-if)# max-xmit-utilization percentage 80
Router(config-pfr-mc-br-if)# end
```

PfR 出口リンクの使用率範囲の変更例

次に、PfR 出口リンクの使用率範囲を変更する例を示します。 この例では、すべての出口リンクの出口使用率範囲が 10% に設定されています。 PfR は、最大使用率の範囲を使用して、出口リン

クがポリシーに準拠しているかどうかを判断します。 PfR は、過剰使用されている、またはポリシー違反の出口から、ポリシー準拠の出口にプレフィックスを移動することによって、すべての出口リンクでアウトバウンド トラフィックを均等化します。

```
Router(config)# pfr master
Router(config-pfr-mc)# max-range-utilization percentage 10
Router(config-pfr-mc)# end
```

最長一致ターゲット割り当ての TCP プローブの例

次に、最長一致ターゲット割り当てを使用したTCPプローブを使用してアクティブ プローブを設定する例を示します。 まず、ターゲット デバイスで IP SLA Responder をイネーブルにする必要があります。このデバイスをPfR用に設定する必要はありません。 境界ルータは、ターゲット デバイスとして使用できます。 2 番目の設定は、マスター コントローラ上で実行します。

ターゲット デバイス

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor responder type tcpConnect port 49152
Router(config)# exit
```

マスター コントローラ

```
Router(config)# pfr master
Router(config-pfr-mc)# mode monitor active
Router(config-pfr-mc)# active-probe tcp-conn 10.4.4.44 target-port 49152
```

強制ターゲット割り当ての UDP プローブの例

次に、プローブ頻度が 20 秒に設定されている、強制ターゲット割り当てを使用したアクティブ プローブを設定する例を示します。 この例では、ターゲット デバイスで IP SLA Responder をイネーブルにする必要があります。

ターゲット デバイス

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor responder type udpEcho port 1001
Router(config)# exit
```

マスター コントローラ

```
Router(config)# pfr master

Router(config-pfr-mc)# mode monitor active
Router(config-pfr-mc)# exit

Router(config)# pfr-map FORCED_MAP 10

Router(config-pfr-map)# match ip address access-list FORCED_LIST
Router(config-pfr-map)# set active-probe udp-echo 10.5.5.57 target-port 1001
Router(config-pfr-map)# set probe frequency 20
```

```
Router(config-pfr-map)# end
```

高速フェールオーバー用 PfR 音声プローブの設定例

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、高速フェールオーバーが設定されている場合に迅速に新しい出口を作成する例を示します。

（注） 高速モニタリングは、継続的なプローブによって多くのオーバーヘッドが発生する、非常にアグレッシブなモードです。高速モニタリングは、パフォーマンスに影響されやすいトラフィックだけに使用することを推奨します。

最初の出力は、3 台の境界ルータのマスター ルータでの設定を示します。 ルート制御モードは、イネーブルです。

```
Router# show run | sec pfr master
pfr master
 policy-rules MAP
 port 7777
 logging
 !
 border 10.3.3.3 key-chain key1
  interface GigabitEthernet0/0/0 external
  interface GigabitEthernet0/4/2 internal
 !
 border 10.3.3.4 key-chain key2
  interface GigabitEthernet0/0/2 external
  interface GigabitEthernet0/0/1 internal
 !
 border 10.4.4.2 key-chain key3
  interface GigabitEthernet0/2/0 external
  interface GigabitEthernet0/2/1 internal
 backoff 90 90
 mode route control
 resolve jitter priority 1 variance 10
 no resolve delay
!
```

基本設定を確認し、境界ルータのステータスを表示するには、**show pfr master** コマンドを実行します。

```
Router# show pfr master
OER state: ENABLED and ACTIVE
  Conn Status: SUCCESS, PORT: 7777
  Version: 2.1
  Number of Border routers: 3
  Number of Exits: 3
  Number of monitored prefixes: 1 (max 5000)
  Max prefixes: total 5000 learn 2500
  Prefix count: total 1, learn 0, cfg 1

Border          Status   UP/DOWN             AuthFail  Version
10.4.4.2        ACTIVE   UP       17:00:32          0  2.1
10.3.3.4        ACTIVE   UP       17:00:35          0  2.1
10.3.3.3        ACTIVE   UP       17:00:38          0  2.1

Global Settings:
  max-range-utilization percent 20 recv 20
  mode route metric bgp local-pref 5000
  mode route metric static tag 5000
  trace probe delay 1000
  logging
```

```
Default Policy Settings:
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

Learn Settings:
  current state : DISABLED
  time remaining in current state : 0 seconds
  no throughput
  no delay
  no inside bgp
  no protocol
  monitor-period 5
  periodic-interval 120
  aggregation-type prefix-length 24
  prefixes 100
  expire after time 720
```

PfR マップを使用してアクティブ音声プローブ用に高速フェールオーバーが設定され、プローブ頻度が2秒に設定されました。高速フェールオーバーモニタリング モードはイネーブルであり、監視対象音声トラフィックは、IP プレフィックス リストを使用して 10.1.1.0/24 プレフィックスを指定することによって識別されます。高速フェールオーバーモードで発生するオーバーヘッドを削減するために、アクティブ音声プローブが PfR の強制ターゲットに割り当てられます。

```
Router# show run | sec pfr-map
pfr-map MAP 10
 match traffic-class prefix-list VOICE_FAIL_LIST
 set mode select-exit best
 set mode monitor fast
 set jitter threshold 12
 set active-probe jitter 120.120.120.1 target-port 20 codec g729a
 set probe frequency 2
```

次に示すのは、policy キーワードを使用してプレフィックスを指定したときの **show pfr master prefix** コマンドからの出力です。このコマンドでは、10.1.1.0/24 プレフィックスに設定されたポリシーが表示されます。 mode monitor は fast に設定されています。したがって、select-exit は自動的に best に設定され、probe frequency を 2 に設定できます。

```
Router# show pfr master prefix 10.1.1.0/24 policy
* Overrides Default Policy Setting
pfr-map MAP 10
  sequence no. 8444249301975040, provider id 1, provider priority 30
    host priority 0, policy priority 10, Session id 0
  match ip prefix-lists: VOICE_FAIL_LIST
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
 *probe frequency 2
  mode route control
 *mode monitor fast
 *mode select-exit best
  loss relative 10
 *jitter threshold 12
  mos threshold 3.60 percent 30
  unreachable relative 50
```

```
  next-hop not set
  forwarding interface not set
  resolve jitter priority 1 variance 10
  resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 10.120.120.1 target-port 20 codec g729a
```

このタスクに示されるようにマスター コントローラが高速フェールオーバー用に設定された後で、トラフィック クラスがポリシー違反となった場合、次のロギング出力には、10.1.1.0/24 プレフィックスで表されるトラフィック クラスが、PfR によって 3 秒以内に 10.3.3.4 インターフェイスの新しい境界ルータ出口を経由してルーティングされたことが示されます。 ロギング出力から、トラフィック クラスは、ジッターしきい値を超えたためにポリシー違反状態になったと考えられます。

```
May  2 10:55:27.355: %OER_MC-5-NOTICE: Active ABS Jitter OOP Prefix 10.1.1.0/24,
jitter 15, BR 10.4.4.2, i/f Gi0/0/2
May  2 10:55:27.367: %OER_MC-5-NOTICE: Route changed Prefix 10.1.1.0/24, BR 10.3.3.4,
i/f Gi0/0/3, Reason Jitter, OOP Reason Jitter
```

アクティブ プローブのソース アドレスの設定例

次に、グローバル コンフィギュレーション モードを開始して、FastEthernet 0/0 をアクティブ プローブのソース インターフェイスとして設定する例を示します。

```
Router(config)# pfr border
Router(config-pfr-br)# active-probe address source interface GigabitEthernet 0/0/0
```

ポリシー適用フェーズのタスクの例

PfR ポリシーの設定および学習済みトラフィック クラスへの適用例

次に、学習済みトラフィック クラスを使用して多数のデフォルト ポリシー設定を上書きし、設定されたポリシー設定またはデフォルトのポリシー設定のいずれかがそれぞれのしきい値を超えた場合に利用可能な最良の出口にトラフィック クラスを移動するようにマスター コントローラを設定する例を示します。

```
enable
configure terminal
pfr master
 backoff 200 2000 200
 delay threshold 2000
 holddown 400
 loss threshold 1500
 periodic 180
 unreachable threshold 1000
 mode select-exit best
 end
```

PfR ポリシーの設定および設定されたトラフィック クラスへの適用例

次に、プレフィックス リストおよびアクセス リストによってフィルタリングされたトラフィック クラスを使用し、デフォルトのポリシー設定の一部を上書きする例を示します。 ポリシーは、音

声トラフィックを表す異なるトラフィック クラスに適用する 2 つの PfR マップを使用して設定します。マスターコントローラは、設定されたポリシー設定またはデフォルトのポリシー設定のいずれかがそれぞれのしきい値を超えた場合に最初のポリシー準拠リンクにトラフィック クラスを移動するように設定します。

```
enable
configure terminal
ip prefix-list CONFIG_TRAFFIC_CLASS seq 10 permit 10.1.5.0/24
ip access-list extended VOICE_TRAFFIC_CLASS
 permit udp any range 16384 32767 10.1.5.0 0.0.0.15 range 16384 32767 dscp ef
 exit
pfr-map CONFIG_MAP 10
 match ip address prefix-list CONFIG_TRAFFIC_CLASS
 set backoff 100 1000 100
 set delay threshold 1000
 set loss relative 25
 set periodic 360
 set unreachable relative 20
 exit
pfr-map VOICE_MAP 10
 match ip address access-list VOICE_TRAFFIC_CLASS
 set active-probe jitter 10.1.5.1 target-port 2000 codec g729a
 set probe-frequency 20
 set jitter threshold 30
 set mos threshold 4.0 percent 25
 set mode select-exit good
 end
```

学習済みプレフィックスの PfR 最適化の防止例

次に、指定したプレフィックスが最適化されないように PfR を設定する例を示します。 次の例では、IP プレフィックス リストは、最適化されない異なるプレフィックスに対する 2 つのエントリで作成されます。 PfR マップは、1 つのシーケンスの 2 つのエントリで設定されます。これによって、プレフィックスは学習されますが、PfR は、プレフィックス リストで指定したプレフィックスを最適化しなくなります。 PfR マップ エントリのシーケンス番号が逆方向になった場合、PfR はプレフィックスを学習し、プレフィックスの最適化を試みます。

```
enable
configure terminal
ip prefix-list DENY_PREFIX deny 172.17.10.0/24
ip prefix-list DENY_PREFIX deny 172.19.10.0/24
pfr-map DENY_PREFIX_MAP 10
 match ip address prefix-list DENY_PREFIX
 exit
pfr-map DENY_PREFIX_MAP 20
 match pfr learn throughput
 end
```

PfR マップ用ポリシー ルールの設定例

次に、**policy-rules**（PfR）コマンドを設定して、PfR マスター コントローラ モードで BLUE という名前の PfR マップの設定を適用する例を示します。

```
enable
configure terminal
pfr-map BLUE 10
 match pfr learn delay
 set loss relative 90
 exit
```

```
pfr master
 policy-rules BLUE
 exit
```

複数 PfR ポリシーの競合解決の設定例

次に、遅延を最高プライオリティに設定し、損失、使用率の順にプライオリティを設定する PfR 解決ポリシーを設定する例を示します。 遅延ポリシーは、20 % の分散を許可するように設定され、損失ポリシーは、30 % の分散を許可するように設定されます。使用率ポリシーは、10 % の分散を許可するように設定されます。

```
enable
configure terminal
pfr master
 resolve delay priority 1 variance 20
 resolve loss priority 2 variance 30
 resolve utilization priority 3 variance 10
 end
```

出口リンクの PfR ロード バランシング ポリシーの設定例

次に、境界ルータの出口リンク上のトラフィック クラス フローに PfR ロード バランシング ポリシーを設定する例を示します。 この例のタスクは、マスターコントローラ上で実行され、出口リンクの使用率範囲、出口リンクの使用率しきい値、使用率および範囲ポリシーに設定されるポリシー プライオリティが設定されます。 パフォーマンス ポリシー、遅延および損失は、ディセーブルです。 PfR は、使用率および範囲のしきい値の両方を使用して、出口リンク上のトラフィック フローのロード バランシングを行います。

```
enable
configure terminal
pfr master
 max-range-utilization percentage 25
 mode select-exit best
 resolve range priority 1
 resolve utilization priority 2 variance 15
 no resolve delay
 no resolve loss
 border 10.1.4.1
 interface GigabitEthernet 0/0/0 external
 max-xmit-utilization absolute 10000
 exit
 exit
 border 10.1.2.1
 interface GigabitEthernet 0/0/2 external
 max-xmit-utilization absolute 10000
 end
```

PfR マップを使用したブラック ホール ルーティングの設定例

次に、PREFIX_BLACK_HOLE という名前の IP プレフィックス リストで定義されたトラフィックに一致する、BLACK_HOLE_MAP という名前の PfR マップを作成する例を示します。 PfR マップは、ヌルインターフェイスに転送されるパケット、つまり、「ブラック ホール」に廃棄されるパ

ケットをフィルタリングします。IP プレフィックスが、ネットワーク上の攻撃のソースとして識別されると、プレフィックス リストが設定されます。

```
enable
configure terminal
ip prefix-list PREFIX_BLACK_HOLE seq 10 permit 10.1.5.0/24
pfr-map BLACK_HOLE_MAP 10
 match ip address prefix-list PREFIX_BLACK_HOLE
 set interface null0
 end
```

PfR マップを使用したシンクホール ルーティングの設定例

次に、PREFIX_SINK_HOLE という名前の IP プレフィックス リストで定義されたトラフィックに一致する、SINK_HOLE_MAP という名前の PfR マップを作成する例を示します。 PfR マップは、ネクスト ホップに転送されるパケットをフィルタリングします。 ネクスト ホップは、パケットの保存、分析、または廃棄を実行できるルータです（シンクホールアナロジー）。IPプレフィックスがネットワーク上の攻撃のソースとして識別されると、プレフィックス リストが設定されます。

```
enable
configure terminal
ip prefix-list PREFIX_SINK_HOLE seq 10 permit 10.1.5.0/24
pfr-map SINK_HOLE_MAP 10
 match ip address prefix-list PREFIX_SINK_HOLE
 set next-hop 10.1.1.3
 end
```

施行フェーズのタスクの例

挿入された PfR スタティック ルートのタグ値の設定例

次に、挿入されたスタティック ルートにタグ値を設定し、ルートが一意に識別されるようにする例を示します。 スタティック ルートは、トラフィック クラスによって定義されるトラフィックがポリシー違反になったときに、そのトラフィックを制御するために PfR によって挿入されることがあります。 デフォルトでは、PfR は挿入されたスタティック ルートに 5000 のタグ値を使用します。 次のタスクでは、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 **mode**（PfR）コマンドにより PfR ルート制御モードがグローバルに設定され、挿入されるスタティック ルートは 15000 の値でタグ付けされます。

```
Router(config)# pfr master
Router(config-pfr-mc)# mode route control

Router(config-pfr-mc)# mode route metric static tag 15000
Router(config-pfr-mc)# end
```

PfR 制御 BGP ルートの BGP ローカル プリファレンス値の設定例

次に、BGP ローカル プリファレンス属性値を設定する例を示します。 PfR は、BGP Local_Pref 値を使用して、強制出口リンクの選択方法として内部 BGP（iBGP）ネイバー上での BGP 最良パス

選択に影響を及ぼします。 デフォルトでは、PfR は 5000 の Local_Pref 値を使用します。 次のタスクでは、プレフィックス リストに一致するトラフィックのルート制御はイネーブルであり、60000 の BGP ローカル プリファレンス値が設定されています。

```
Router(config)# pfr-map BLUE 10
Router(config-pfr-map)# match ip address prefix-list BLUE
Router(config-pfr-map)# set mode route control
Router(config-pfr-map)# set mode route metric bgp local-pref 60000
Router(config-pfr-map)# end
```

アプリケーション トラフィックの制御例

次に、ポリシーベース ルーティング（PBR）を使用して、指定したアプリケーション トラフィック クラスを PfR で制御できるようにする例を示します。 Telnet トラフィックなどのアプリケーション トラフィックは、遅延に影響されやすいトラフィックです。 TCP 遅延が長いと、Telnet セッションの使用が困難になることがあります。 この例は、マスターコントローラ上で設定されます。192.168.1.0/24 ネットワークをソースとする Telnet トラフィックに一致させ、ポリシーを適用して、この Telnet トラフィックが 30 ミリ秒以下の応答時間で出口リンクを経由して送信されるようにします。

```
Router(config)# ip access-list extended TELNET
Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq telnet
Router(config-ext-nacl)# exit

Router(config)# pfr-map SENSITIVE
Router(config-route-map)# match ip address access-list TELNET
Router(config-route-map)# set mode route control
Router(config-route-map)# set delay threshold 30
Router(config-route-map)# set resolve delay priority 1 variance 20
Router(config-route-map)# end
```

次に、ポート 23（Telnet）に基づいてフィルタリングされた TCP アプリケーション トラフィックの例を示します。

```
Router# show pfr master appl tcp 23 23 dst policy

Prefix              Appl Prot       Port                 Port Type       Policy
-------------------------------------------------------------------------------
10.1.1.0/24         tcp             [23, 23]             src             10
```

確認フェーズのタスクの例

PfR ルート制御変更の手動確認の例

次に、PfR 施行フェーズで実行されたトラフィック制御が実際にトラフィック フローを変更し、OOP イベントをポリシー準拠に変更したことを手動で確認する例を示します。 マスター コントローラで **show logging** コマンドを使用すると、システム ロギング（syslog）の状態および標準的なシステム ロギング バッファの内容が表示されます。 省略可能な区切り文字を使用すると、特定のプレフィックスの PfR メッセージ付きでロギング バッファを表示できます。 **show pfr master prefix** コマンドでは、監視対象プレフィックスのステータスが表示されます。 境界ルータで **show pfr border routes** コマンドを使用すると、境界ルータ上の PfR 制御による BGP またはスタティッ

ク ルートに関する情報が表示されます。 これらのコマンドの出力例は、「PfR ルート強制変更の手動確認」の項を参照してください。

マスター コントローラ

```
Router# show logging | i 10.1.1.0
Router# show pfr master
prefix 10.1.1.0
Router# end
```

境界ルータ

```
Router# show pfr border routes static
Router# show pfr border routes bgp
Router# end
```

関連情報

他のパフォーマンス ルーティング機能の詳細または一般的な概念に関する資料については、「関連資料」の項に記載の資料を参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール

関連項目	マニュアル タイトル
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

アドバンスドパフォーマンスルーティングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *5*：アドバンスド パフォーマンス ルーティングに関する機能情報

機能名	リリース	機能情報
Optimized Edge Routing（OER）	Cisco IOS XE Release 2.6.1、Cisco IOS XE Release 3.1S	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。 PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 次のコマンドが導入または変更されました。**pfr**、**show pfr master**。 （注） 境界ルータ専用機能は Cisco IOS XE Release 2.6.1 および Cisco IOS XE Release 3.1S リリースに含まれています。マスター コントローラ設定は使用できません。 境界ルータとして使用される Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M を実行するルータでなければなりません。
ASR 1000 用 PfR マスター コントローラのサポート	Cisco IOS XE Release 3.3S	Cisco IOS XE Release 3.3S 以降のリリースでは、PfR マスター コントローラ機能がサポートされます。

機能名	リリース	機能情報
ポリシー ルール設定に対する OER のサポート	Cisco IOS XE Release 3.3S	ポリシー ルール設定に対する OER サポート機能に、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 PfR マップを選択し設定を適用できる機能が導入されました。定義済みの PfR マップ間での切り替えを容易に実行できます。 この機能により、次のコマンドが導入または変更されました。**policy-rules**（PfR）。
expire after コマンド[1]	Cisco IOS XE Release 3.3S	**expire after**（PfR）コマンドは、学習済みプレフィックスの有効期間の設定に使用します。デフォルトでは、マスター コントローラは、中央ポリシー データベースから非アクティブなプレフィックスを削除します。これは、メモリが必要とされるためです。 このコマンドを使用すると、制限に基づいて時間またはセッションを設定することによって、この動作を改良できます。 時間ベースの制限は、分単位で設定します。セッション ベースの制限は、監視期間数（またはセッション数）に対して設定します。
OER アクティブ プローブ ソース アドレス	Cisco IOS XE Release 3.3S	OER アクティブ プローブ ソースアドレス機能では、境界ルータ上の特定の出口インターフェイスをアクティブ プローブのソースとして設定できます。 **active-probe address source**（PfR）コマンドが、この機能によって導入されました。

機能名	リリース	機能情報
OER アプリケーション アウェア ルーティング：PBR	Cisco IOS XE Release 3.3S	OER アプリケーション アウェア ルーティング：PBR 機能によって、監視対象プレフィックスによって伝送されるアプリケーションのタイプに基づいて IP トラフィックを最適化できるようになっています。 トラフィックのサブセット（アプリケーション）には、個別のポリシー設定が適用されます。 この機能により、次のコマンドが導入または変更されました。**debug pfr border pbr**、**debug pfr master prefix**、**match ip address（PfR）**、**show pfr master active-probes**、および **show pfr master appl**。

機能名	リリース	機能情報
OER DSCP モニタリング	Cisco IOS XE Release 3.3S	OER DSCP モニタリングに、プロトコル、ポート番号、および DSCP 値に基づいたトラフィック クラスの自動学習が導入されました。 トラフィック クラスは、プロトコル、ポート番号、および DSCP 値で構成され、不要なトラフィックをフィルタリングでき、関心のあるトラフィックを集約できる、キーの組み合わせによって定義できます。 これで、プロトコル、ポート番号、およびDSCP情報などのレイヤ4情報は、レイヤ3プレフィックス情報に加えてマスター コントローラ データベースに送信されるようになります。 この新しい機能により、PfRによるアプリケーショントラフィックのアクティブ モニタリングおよびパッシブ モニタリングの両方が可能になりました。 この機能により、次のコマンドが導入または変更されました。 **show pfr border passive applications**、**show pfr border passive cache**、**show pfr border passive learn**、**show pfr master appl**、**traffic-class aggr egation（PfR）**、**traffic-class filter（PfR）**、および **traffic-class key s（PfR）**。

機能名	リリース	機能情報
パフォーマンス ルーティング - リンク グループ	Cisco IOS XE Release 3.3S	パフォーマンス ルーティング - リンク グループ機能によって、出口リンクのグループを優先リンク セットとして、またはPfR用フォールバック リンク セットとして定義し、PfRポリシーで指定されたトラフィック クラスを最適化する際に使用できるようになっています。 この機能により、次のコマンドが導入または変更されました。**link-group（PfR）**、**set link-group（PfR）**、および**show pfr master link-group**。
高速フェールオーバー モニタリングのサポート[2]	Cisco IOS XE Release 3.3S	高速フェールオーバー モニタリングに、高速モニタリング モードを設定できる機能が導入されました。高速フェールオーバー モニタリング モードでは、アクティブ モニタリングとパッシブ モニタリングを使用して、すべての出口が継続的にプローブされます。 高速フェールオーバー モニタリング モードのプローブ頻度は、他のモニタリング モードよりも低く設定できます。これにより、より迅速なフェールオーバー機能が可能になります。高速フェールオーバー モニタリングは、すべてのタイプのアクティブ プローブ（ICMP エコー、ジッター、TCP接続、およびUDP エコー）で使用できます。 この機能により、次のコマンドが導入または変更されました。**mode（PfR）**、**set mode（PfR）**。

[1] これはマイナーな拡張です。 マイナーな拡張は、通常 Feature Navigator に記載されません。

[2] これはマイナーな拡張です。 マイナーな拡張は、通常 Feature Navigator に記載されません。

第 5 章

パフォーマンス ルーティングを使用した BGP インバウンド最適化

PfR BGPインバウンド最適化機能は、自律システム内部プレフィックス宛ての自律システム外部のプレフィックスから送信されたトラフィックに対する最適な入口選択をサポートするようになりました。自律システムからインターネットサービスプロバイダー（ISP）への外部EGP（eBGP）アドバタイズメントにより、ネットワークに入るトラフィックの入口パスが影響を受けることがあります。 PfR では、eBGP アドバタイズメントを使用して最適な入口選択を行います。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンスルーティングを使用したBGPインバウンド最適化の概要

BGP インバウンド最適化

PfR BGP インバウンド最適化機能により、内部プレフィックスがサポートされるようになりました。 BGP を使用すると、PfR は内部プレフィックスを選択し、自律システム外のプレフィックスから自律システム内のプレフィックス宛てに送信されるトラフィックに対する最良入口選択をサポートできます。 企業ネットワークは、インターネット サービス プロバイダー（ISP）を使用してインターネットで内部プレフィックスをアドバタイズし、ISPから外部プレフィックスのアドバタイズメントを受け取ります。

BGPインバウンド最適化を使用すると、内部プレフィックスを手動で設定したり、内部プレフィックスを自動的に学習したりできます。 その結果得られたプレフィックスは、リンク使用率しきい値やリンク使用率範囲テクニックを使用して監視できます。 トラフィックの負荷や範囲パフォーマンスの特性を定義するリンク ポリシーは PfR 管理の入口リンクに対して適用できます。 BGP インバウンド最適化は、eBGPアドバタイズメントを操作して内部プレフィックス宛てのトラフィックに対する最適な入口選択に影響を与えることによってインバウンド トラフィックに影響を与えることができます。

（注） PfR は内部プレフィックスを学習できますが、BGP ルーティング情報ベース（RIB）に完全に一致するものがない限り PfR は内部プレフィックスを制御しません。これは、PfR は新しいプレフィックスをインターネットにアドバタイズしないためです。

PfR を使用したプレフィックス トラフィック クラスの学習

NetFlow Top Talker 機能を使用して、最大のアウトバウンド スループットまたは最大の遅延時間に基づいてプレフィックスを自動的に学習するように PfR マスター コントローラを設定できます。 スループットの学習では、最大のアウトバウンド トラフィック ボリュームを生成するプレフィックスを判定します。 スループット プレフィックスは高い順にソートされます。 遅延学習では、ラウンドトリップ応答時間（RTT）が最大のプレフィックスを判定し、これらのプレフィックスの RTT を低減するために、最大遅延プレフィックスを最適化します。 遅延プレフィックスは、遅延時間の長い順にソートされます。

PfR は、次の 2 種類のプレフィックスを自動的に学習できます。

- 外部プレフィックス：外部プレフィックスは、社外で割り当てられたパブリックIPプレフィックスとして定義されています。 外部プレフィックスは他のネットワークから受信します。

- 内部プレフィックス：内部プレフィックスは、社内で割り当てられたパブリック IP プレフィックスとして定義されています。 内部プレフィックスは、企業ネットワーク内部で設定されたプレフィックスです。 モニタリング期間中に学習可能な内部プレフィックスの最大数は 30 です。

PfR BGP インバウンド最適化機能により、内部プレフィックスを学習できるようになりました。BGP を使用すると、PfR は内部プレフィックスを選択し、自律システム外のプレフィックスから自律システム内のプレフィックス宛てに送信されるトラフィックに対する最良入口選択をサポートできます。 企業ネットワークは、インターネット サービス プロバイダー（ISP）を使用してインターネットで内部プレフィックスをアドバタイズし、ISP から外部プレフィックスのアドバタイズメントを受け取ります。

PfR リンク使用率の測定

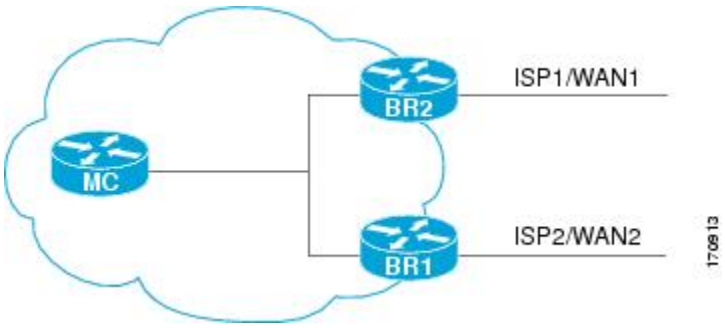
リンク使用率のしきい値

境界ルータに外部インターフェイスが設定されると、PfR は自動的に外部リンクの使用率を監視します（外部リンクは境界ルータ上のインターフェイスで、通常は WAN にリンクしています）。デフォルトでは、境界ルータは 20 秒ごとにリンクの使用率をマスター コントローラにレポートします。出力（送信済み）と入力（受信済み）の両方のトラフィック使用率の値がマスターコントローラにレポートされます。出口または入口リンクの使用率がデフォルトしきい値である 75% を超えている場合、その出口または入口リンクは OOP 状態であり、PfR はトラフィック クラス用の代替リンクを検出するためにモニタリング プロセスを開始します。 リンク使用率のしきい値は、毎秒あたりのキロバイト数（kbps）で表す絶対値またはパーセンテージとして手動で設定できます。

リンク使用率範囲

また、PfR では、すべてのリンクに対する使用率の範囲を計算するよう設定することもできます。出力（送信済み）と入力（受信済み）の両方のトラフィック使用率の値がマスター コントローラにレポートされます。 次の図に、個別の ISP 経由でインターネットに接続する出口リンクを持つ 2 つの境界ルータを示します。 マスター コントローラは、どちらのボーダー ルータ（次の図の BR1 または BR2）のリンクがトラフィック クラスによって使用されるのかを決定します。

図 *10*：*PfR* ネットワーク図



PfR 範囲機能は、確実にトラフィックの負荷を分散するために、出口または入口リンクが相互に相対的な使用率の範囲内に収まるよう動作します。 範囲は割合で指定されます。この値はマスターコントローラ上で設定され、そのマスターコントローラで管理されている境界ルータ上のすべての出口リンクまたは入口リンクに適用されます。 たとえば、範囲が 25 % として指定され、（上の図の）BR1 の出口リンクの使用率が 70 % で、（上の図の）BR2 の出口リンクの使用率が 40 % に下がった場合、2 つの出口リンクの間の割合の範囲が 25 % を上回るので、PfR は、BR1 の出口リンクを使用する一部のトラフィック クラスを移動して、トラフィック負荷を均等にしようとします。（上の図の）BR1 が入口リンクとして設定されている場合は、使用率の値が送信済みトラフィックではなく受信済みトラフィックに関するものでない限り、出口リンクの場合と同じ方法でリンク使用率範囲が計算されます。

PfR リンク ポリシー

PfR リンク ポリシーは PfR 管理の外部リンクに対して適用される一連のルールです（外部リンクはネットワーク エッジの境界ルータのインターフェイスです）。 リンク ポリシーでは、目的とするリンクのパフォーマンス特性を定義します。 トラフィック クラス パフォーマンス ポリシーのように、リンクを使用する個々のトラフィック クラスエントリのパフォーマンスを定義するのではなく、リンク ポリシーではリンク全体のパフォーマンスを定義します。

BGP インバウンド最適化機能は、選択された入口（入力）リンク ポリシーをサポートします。

リンク ポリシーで管理されるパフォーマンス特性は次のとおりです。

- トラフィック負荷（使用率）
- 範囲
- コスト：コスト ポリシーは BGP インバウンド最適化機能でサポートされません。 コスト ポリシーの詳細については、「パフォーマンス ルーティング コスト ポリシーの設定」モジュールを参照してください。

トラフィックの負荷

トラフィック負荷（使用率とも呼ばれます）ポリシーは、特定のリンクで伝送できるトラフィック量に関する上限しきい値で構成されます。 Cisco IOS PfR は、トラフィック クラスごとの負荷分散をサポートします。 境界ルータに外部インターフェイスが設定されると、境界ルータはデフォルトにより、20 秒ごとにリンク使用率をマスター コントローラに報告します。 出口リンクおよび入口リンクのトラフィック負荷しきい値は PfR ポリシーとして設定できます。 出口または入口リンク使用率が、設定されたしきい値またはデフォルトしきい値である 75 % を超えている場合、その出口または入口リンクは OOP 状態であり、PfR はトラフィック クラス用の代替リンクを検出するためにモニタリング プロセスを開始します。 リンク使用率のしきい値は、毎秒あたりのキロバイト数（kbps）で表す絶対値またはパーセンテージとして手動で設定できます。 各インターフェイスの負荷使用率ポリシーは、マスター コントローラで境界ルータを設定する際に設定します。

ヒント　負荷分散を設定する場合は、**load-interval** インターフェイス コンフィギュレーション コマンドを使用して、外部インターフェイスでのインターフェイス負荷計算の間隔を 30 秒に設定することを推奨します。 デフォルトの計算間隔は 300 秒です。 負荷計算は、インターフェイス コンフィギュレーション モードの境界ルータで設定します。 この設定は必須ではありませんが、Cisco IOS PfR ができる限り迅速に負荷分散に対応できるよう、これを設定しておくことを推奨します。

範囲

範囲ポリシーは、確実にトラフィックの負荷が分散されるよう、すべてのリンクを相互に相対的な一定の使用率の範囲内で維持するために定義します。 たとえば、ネットワークに複数の出口リンクがあり、いずれかのリンクを優先する財務上の理由がない場合、最善の選択はすべてのリンクに負荷を均一に分散することです。 従来のルーティング プロトコルによる負荷共有では、必ずしも均一に負荷が分散されるわけではありません。なぜなら、負荷共有はフローベースであり、パフォーマンスまたはポリシー ベースではないからです。 Cisco IOS PfR の範囲機能を使用すると、リンク セットのトラフィック使用率がお互いの特定の割合範囲内に収まるよう PfR を設定できます。 リンク間の差異が大きくなりすぎると、PfR は使用可能なリンク間にトラフィック クラスを分散し、リンクをポリシー準拠状態に戻そうとします。 デフォルトでは、マスター コントローラは PfR が管理するすべてのリンクに対して最大範囲使用率を 20 % に設定しますが、使用率の範囲は最大割合値を使用して設定できます。 出口リンクおよび入口リンクの使用率範囲は PfR ポリシーとして設定できます。

（注）　リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

PfR 入口リンク選択の制御テクニック

PfR BGP インバウンド最適化機能に、インバウンド トラフィックを操作する機能が追加されました。 ネットワークは ISP への eBGP アドバタイズメントを使用して、内部プレフィックスの到達可能性をインターネットにアドバタイズします。 同じプレフィックスが複数の ISP にアドバタイズされると、そのネットワークはマルチホーム状態になります。 PfR BGP インバウンド最適化は、マルチホームのネットワークで最も効果的に機能します。ただしこの最適化は、同じ ISP に対して複数の接続を持つネットワークでも使用できます。 BGP インバウンド最適化を実装するために、PfR は eBGP アドバタイズメントを操作して、内部プレフィックス宛てのトラフィックに対して最良入口選択を反映させます。 最良入口選択は、複数の ISP に接続しているネットワークだけに効果があります。

入口リンクの選択を強制的に行うために、PfR は次の方法を提供します。

BGP 自律システム番号のプリペンド

遅延が原因で、または、Cisco IOS Release 15.2(1)T1 および 15.1(2)S よりも前のイメージで、入口リンクがポリシー違反（OOP）になり、PfR が内部プレフィックスに対して最適な入口を選択すると、追加の自律システム ホップが、他の入口に対する内部プレフィックス BGP アドバタイズメントの先頭に 1 つずつ（最大 6 個）追加されます。 Cisco IOS Release 15.2(1)T1、15.1(2)S、およびそれ以降のリリースでは、到達不能または損失が原因で入口リンクがポリシー違反（OOP）になり、PfR が内部プレフィックスに対して最適な入口を選択すると、6 つの追加の自律システム ホップが、他の入口に対する内部プレフィックス BGP アドバタイズメントの先頭にすぐに追加されます。 他の入口の追加の自律システム ホップにより、内部プレフィックスに対して最適な入口が使用される可能性が高まります。 到達不能または損失が原因で入口リンクが OOP になると、6 つの追加の自律システム ホップがすぐに追加されるので、ソフトウェアは、古い入口リンクからトラフィックをすぐに移動できます。 これは内部プレフィックスを制御するために PfR が使用するデフォルトの方法であり、ユーザ設定は必要ありません。

BGP 自律システム番号コミュニティのプリペンド

遅延が原因で、または、Cisco IOS Release 15.2(1)T1 および 15.1(2)S よりも前のイメージで、入口リンクがポリシー違反（OOP）になり、PfR が内部プレフィックスに対して最適な入口を選択すると、BGP プリペンド コミュニティが、ネットワークから ISP などの別の自律システムへの内部プレフィックス BGP アドバタイズメントに 1 つずつ（最大 6 個）アタッチされます。 Cisco IOS Release 15.2(1)T1、15.1(2)S、およびそれ以降のリリースでは、到達不能または損失が原因で入口リンクがポリシー違反（OOP）になり、PfR が内部プレフィックスに対して最適な入口を選択すると、6 つの BGP プリペンド コミュニティが、内部プレフィックス BGP アドバタイズメントにアタッチされます。 BGP プリペンド コミュニティは、ISP からピアへの内部プレフィックスのアドバタイズメントで自律システム ホップの数を増加させます。 自律システム プリペンド BGP コミュニティは、ローカル ISP が追加の自律システム ホップをフィルタリングする可能性がないため、PfR BGP インバウンド最適化で推奨される方法です。 この場合、すべての ISP が BGP プリペンド コミュニティをサポートするわけではないこと、ISP ポリシーが自律システム ホップを無視または変更する場合があること、中継 ISP が自律システム パスをフィルタリングする可能性があることなどいくつかの問題点があります。 インバウンドを最適化するこの方法を使用している場合、自律システムを変更するには、**clear ip bgp** コマンドを使用してアウトバウンドの再設定を行う必要があります。

内部プレフィックスに対する PfR マップ操作

PfR マップの操作はルート マップの操作に似ています。 PfR マップは、match 句を使用して IP プレフィックス リストまたは PfR 学習ポリシーを選択し、set 句を使用して PfR ポリシー設定を適用するよう設定されます。 PfR マップはルートマップと同様にシーケンス番号で設定され、シーケンス番号が最小の PfR マップが最初に評価されます。

BGP インバウンド最適化機能では、内部プレフィックスを識別するために **inside** キーワードが **match ip address**（PfR）コマンドに導入されました。 インバウンド BGP は、PfR マップを使用するときに設定に関する制約事項が発生するパッシブ モードだけをサポートします。インバウンド BGP 用の PfR マップでは、**set active-probe**、**set interface**、**set mode monitor**、**set mode verify**

bidirectional、**set mos threshold**、**set nexthop**、**set periodic**、**set probe frequency**、**set traceroute reporting** コマンドはサポートされません。

（注） match precedence のプライオリティは PfR マップではサポートされません。

パフォーマンスルーティングを使用してBGPインバウンド最適化の設定方法

内部プレフィックスを使用したトラフィッククラスの自動学習のための PfR の設定

PfR マスター コントローラでこのタスクを実行してトラフィック クラスとして使用する内部プレフィックスを自動的に学習するよう PfR を設定します。 トラフィック クラスは MTC リストに入力されます。 このタスクでは、PfR Top Talker/Top Delay コンフィギュレーション モードで使用される **inside bgp**（PfR）コマンドを使用します。 このタスクでは、内部プレフィックス（ネットワーク内のプレフィックス）の自動プレフィックス学習が設定されます。 また、学習期間タイマー、プレフィックスの最大数、MTC リストエントリの有効期間などの省略可能な設定パラメータも示されます。

はじめる前に

このタスクを設定する前に、内部および外部 BGP ネイバーの BGP ピアリングを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **learn**
5. **inside bgp**
6. **monitor-period** *minutes*
7. **periodic-interval** *minutes*
8. **prefixes** *number*
9. **expire after session** *number* | **time** *minutes*
10. **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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**learn** 例： `Router(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、プレフィックス学習ポリシーとタイマーを設定します。
ステップ 5	**inside bgp** 例： `Router(config-pfr-mc-learn)# inside bgp`	ネットワーク内部のプレフィックスを学習します。
ステップ 6	**monitor-period** *minutes* 例： `Router(config-pfr-mc-learn)# monitor-period 10`	（任意）PfR マスター コントローラがトラフィック フローを学習する期間を設定します。 • デフォルトの学習期間は 5 分です。 • モニタリング期間の長さは **periodic-interval** コマンドで設定されます。 • 学習するプレフィックスの数は **prefixes** コマンドで設定されます。 • この例では、各モニタリング期間の長さを 10 分に設定します。

	コマンドまたはアクション	目的
ステップ 7	**periodic-interval** *minutes* 例： `Router(config-pfr-mc-learn)# periodic-interval 20`	（任意）プレフィックス学習期間の間隔を設定します。 • デフォルトでは、プレフィックス学習期間の間隔は 120 分です。 • この例では、モニタリング期間の間隔を 20 分に設定します。
ステップ 8	**prefixes** *number* 例： `Router(config-pfr-mc-learn)# prefixes 30`	（任意）モニタリング期間中にマスター コントローラが学習するプレフィックスの数を設定します。 • デフォルトでは、上位 100 のトラフィック フローが学習されます。 • この例では、マスター コントローラがモニタリング期間中に 30 個のプレフィックスを学習するよう設定します。 （注） モニタリング期間中に学習可能な内部プレフィックスの最大数は 30 です。
ステップ 9	**expire after session** *number* | **time** *minutes* 例： `Router(config-pfr-mc-learn)# expire after session 100`	（任意）学習されたプレフィックスが中央ポリシー データベース内に保持される期間を設定します。 • **session** キーワードは、指定された数のモニタリング期間が経過した後に、学習されたプレフィックスが削除されるように設定します。 • **time** キーワードは、指定された期間の経過後に、学習されたプレフィックスが削除されるように設定します。 時間の値は分単位で入力されます。 • この例では、100 回のモニタリング期間経過後に、学習されたプレフィックスを削除するよう設定します。
ステップ 10	**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 モードを開始します。

PfR モニタリングに対して内部プレフィックスを手動で選択

PfR BGP インバウンド最適化機能は、自律システム内部プレフィックス宛ての自律システム外部のプレフィックスから送信されたトラフィックに対する最適な入口の選択をサポートするように

なりました。 このタスクを実行して内部プレフィックスまたはプレフィックス範囲を定義する IP プレフィックス リストを作成することにより、PfR モニタリングに対して内部プレフィックスを手動で選択します。 次に、プレフィックス リストは、PfR マップで match 句を設定することにより Monitored Traffic Class（MTC）リストにインポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network/length* | **permit** *network/length*}
4. **pfr-map map-name** *sequence-number*
5. **match ip address prefix-list** *name* [**inside**]
6. **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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*]{**deny** *network/length* | **permit** *network/length*} 例： `Router(config)# ip prefix-list INSIDE_PREFIXES seq 20 permit 192.168.1.0/24`	プレフィックスリストを作成し、モニタリングのためにプレフィックスを手動で選択します。 • マスターコントローラは、デフォルトルートを含む任意の長さの、完全に一致するプレフィックスを監視し、制御できます。マスターコントローラは設定されたプレフィックスでだけ動作します。 • 例では、PfR が 192.168.1.0/24 の特定のプレフィックスを監視および制御するために IP プレフィックス リストを作成します。
ステップ 4	**pfr-map map-name** *sequence-number* 例： `Router(config)# pfr-map INSIDE_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを作成または設定します。 • PfR マップの操作はルート マップの操作に似ています。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。

	コマンドまたはアクション	目的
		• パフォーマンスを最大化するために、共通シーケンスおよび拒否シーケンスは最小の PfR マップ シーケンスに適用する必要があります。 • 例では、INSIDE_MAP という名前の PfR マップを作成します。
ステップ 5	**match ip address prefix-list** *name* [**inside**] 例： `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	PfR ポリシーを適用するプレフィックス リスト match 句エントリを PfR マップで作成します。 • このコマンドは IP プレフィックス リストだけをサポートします。 • **inside** キーワードを使用して内部プレフィックスを識別します。 • 例では、match 句を作成し、プレフィックス リスト INSIDE_PREFIXES を使用して内部プレフィックスが一致するよう指定します。
ステップ 6	**end** 例： `Router(config-pfr-map)# end`	PfR マップ 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。

インバウンド トラフィックに対する PfR リンク使用率の変更

BGP インバウンド最適化機能では、インバウンド トラフィック使用率をマスター コントローラに報告できるようになりました。 マスター コントローラでこのタスクを実行し、PfR 入口（インバウンド）リンク使用率しきい値を変更します。 境界ルータの外部インターフェイスが設定されると、PfR は境界ルータの出口リンクの使用率を 20 秒ごとに自動的に監視します。 使用率は再びマスター コントローラに報告され、使用率が 75% を超えると、PfR はリンクのトラフィック クラスに対して別の入口リンクを選択します。 キロバイト/秒（kbps）単位の絶対値または割合を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*}
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Router(config-pfr-mc)# border 10.1.1.2`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界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 つの境界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境界ルータは、最大 10 台です。 （注） 境界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、既存の境界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。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* **external** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	PfR 管理の外部インターフェイスとして境界ルータを設定し、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 モードを開始します。 • 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 つの外部境界ルータ インターフェイスが必要です。 各境界ルータでは、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。 （注） **external** キーワードまたは **internal** キーワードを指定せずに **interface** 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 6	**maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*} 例： `Router(config-pfr-mc-br-if)# maximum utilization receive percent 90`	設定された PfR 管理リンク インターフェイスに対して最大受信使用率のしきい値を設定します。 • **absolute** キーワードと *kbps* 引数を使用してすべての入口リンクのスループットの絶対しきい値を 1 秒あたりのキロバイト数（kbps）で指定します。 • **percent** キーワードと *percentage* 引数を使用してすべての入口リンクで受信される帯域幅の割合として最大使用率しきい値を指定します。 • この例では、境界ルータのこの入口リンクに対する着信トラフィックの最大使用率しきい値を 90 % 以下に指定する必要があります。
ステップ 7	**end** 例： `Router(config-pfr-mc-br-if)# end`	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 モードを終了し、特権 EXEC モードに戻ります。

PfR 入口リンク使用率範囲の変更

マスター コントローラでこのタスクを実行し、すべての境界ルータに対する最大入口リンク使用率範囲を変更します。 デフォルトでは、PfR は境界ルータ上の外部リンクの使用率を 20 秒ごとに

自動監視し、境界ルータがマスターコントローラに使用率を報告します。BGPインバウンド最適化機能では、インバウンドトラフィック使用率をマスターコントローラに報告し、入口リンクのリンク使用率範囲を指定できるようになりました。

このタスクでは、すべての入口リンク間の使用率範囲が20%を超えると、マスターコントローラは、一部のトラフィック クラスを別の入口リンクに移動することによって、トラフィック負荷の均等化を試みます。 最大使用率の範囲は、割合として設定されます。

PfR は、最大使用率範囲を使用して、リンクがポリシーに準拠しているかどうかを判断します。このタスクでは、PfR は、過剰使用されている出口またはポリシー違反の出口から、ポリシー準拠の出口にトラフィック クラスを移動することによって、すべての入口リンクでインバウンドトラフィックを均等化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max range receive percent** *percentage*
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**max range receive percent** *percentage* 例： `Router(config-pfr-mc)# max range receive percent 20`	境界ルータにあるすべての入口リンク間の受信使用率範囲の上限を指定します。 • **percent** キーワードと *percentage* 引数は範囲の割合を指定するために使用されます。

	コマンドまたはアクション	目的
		• この例では、境界ルータにあるすべての入口リンク間の受信使用率範囲は 20% 以内である必要があります。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

学習された内部プレフィックスに対する PfR ポリシーの設定および適用

このタスクを実行して、ポリシーをマスター コントローラにある MTC リストの学習された内部プレフィックス トラフィック クラス エントリに適用します。 BGP インバウンド最適化機能では、内部プレフィックスの最適化がサポートされるようになりました。 ポリシーは PfR マップを使用して設定し、いくつかの set 句を含みます。

インバウンド BGP は、PfR マップを使用するときに設定に関する制約事項が発生するパッシブ モードだけをサポートします。 インバウンド BGP 用の PfR マップでは、**set active-probe**、**set interface**、**set mode monitor**、**set mode verify bidirectional**、**set mos threshold**、**set nexthop**、**set periodic**、**set probe frequency**、**set traceroute reporting** コマンドはサポートされません。

（注） PfR マップに適用されたポリシーは、グローバル ポリシー設定よりも優先されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn inside**
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
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。 • パスワードを入力します（要求された場合）。
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	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map INSIDE_LEARN 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは、最初に IP プレフィックス リストに定義してから、**match** コマンドを使用して適用します。 • 例では、INSIDE_LEARN という名前の PfR マップを作成します。
ステップ 4	**match pfr learn inside** 例： `Router(config-pfr-map)# match pfr learn inside`	PfR 学習プレフィックスに一致する match 句エントリを PfR マップで作成します。 • プレフィックスは内部プレフィックスであるプレフィックスを学習したり、最小の遅延または最大のアウトバウンド スループットに基づいてプレフィックスを学習したりするよう設定できます。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、内部プレフィックスを使用して学習されたトラフィックに一致する match 句エントリを作成します。
ステップ 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay threshold 2000`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。 相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 2000 ミリ秒に設定する set 句が設定されます。

	コマンドまたはアクション	目的
ステップ 6	**set loss** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set loss relative 20`	マスターコントローラが出口リンクに対して許容する相対または最大パケット損失制限を設定する set 句エントリを作成します。 • PfR マップを設定して、出口リンクでの送信中に PfR が許可するパケット損失の相対割合または最大数を指定するには、このコマンドを使用します。パケット損失がユーザ定義またはデフォルトの値を超えると、マスター コントローラはその出口リンクをポリシー違反であると判断します。 • **relative** キーワードは、相対パケット損失割合を設定するために使用されます。 相対パケット損失割合は、短期的なパケット損失と長期的なパケット損失の比較に基づきます。 • **threshold** キーワードは、絶対最大パケット損失を設定するために使用されます。 最大値は、百万パケットに対して実際に損失したパケットの数に基づきます。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックに対して許容できるパケット損失の相対割合を 20% に設定する set 句を作成します。
ステップ 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set unreachable relative 10`	到達不能ホストの最大数を設定する set 句エントリを作成します。 • このコマンドは、PfR がトラフィック エントリに許可する到達不能ホストの相対割合または最大数（100 万フローあたりのフロー数（fpm））を指定するために使用します。 到達不能ホストの絶対数または相対割合がユーザ定義の値またはデフォルト値を超える場合、PfR はトラフィック クラス エントリが OOP であると判断し、代替出口リンクを検索します。 • 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。 到達不能ホストの相対割合は、短期測定値および長期測定値の比較に基づいています。 • 到達不能ホストの絶対最大数を fpm に基づいて設定するには **threshold** キーワードを使用します。 • 例では、最大の遅延に基づいて学習されたトラフィックに対して到達不能ホストの相対割合が 10% 以上である場合に、トラフィック クラス エントリの新しい出口リンクを検索するようマスター コントローラを設定する set 句エントリを作成します。
ステップ 8	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

設定された内部プレフィックスに対する PfR ポリシーの設定および適用

このタスクを実行して、ポリシーをマスター コントローラにある MTC リストの設定された内部プレフィックス トラフィック クラス エントリに適用します。 BGP インバウンド最適化機能では、内部プレフィックスの最適化がサポートされるようになりました。 ポリシーは PfR マップを使用して設定します。 このタスクには、set 句の異なる基準によるプレフィックス リスト設定が含まれます。

（注） PfR マップで適用されたポリシーによって、グローバル ポリシーの設定が上書きされることはありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr-map map-name** *sequence-number*
4. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name* [**inside**]
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
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。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**pfr-map map-name** *sequence-number* 例： `Router(config)# pfr-map INSIDE_CONFIGURE 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを作成または設定します。 • PfR マップの操作はルート マップの操作に似ています。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • パフォーマンスを最大化するために、permit シーケンスおよび deny シーケンスは最小の pfr マップ シーケンスに適用する必要があります。 • 例では、INSIDE_CONFIGURE という名前の PfR マップを作成します。
ステップ 4	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name* [**inside**] 例： `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックス リストを参照します。 • **inside** キーワードを使用して、自律システム内部プレフィックス宛ての自律システム外部のプレフィックスから送信されたトラフィックに対する最適な入口の選択をサポートする PfR BGP インバウンド最適化をサポートする内部プレフィックスを指定します。 • 例では、内部プレフィックスを指定するプレフィックス リスト INSIDE_PREFIXES を使用して match 句エントリを作成しています。
ステップ 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay threshold 2000`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。 相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 2000 ミリ秒に設定する set 句が設定されます。
ステップ 6	**set loss** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set loss relative 20`	マスター コントローラが出口リンクに対して許容する相対または最大パケット損失制限を設定する set 句エントリを作成します。 • PfR マップを設定して、出口リンクでの送信中に PfR が許可するパケット損失の相対割合または最大数を指定するには、このコマンドを使用します。 パケット損失がユーザ定義またはデフォルトの値を超えると、マスター コントローラはその出口リンクをポリシー違反であると判断します。

	コマンドまたはアクション	目的
		• **relative** キーワードは、相対パケット損失割合を設定するために使用されます。 相対パケット損失割合は、短期的なパケット損失と長期的なパケット損失の比較に基づきます。 • **threshold** キーワードは、絶対最大パケット損失を設定するために使用されます。 最大値は、百万パケットに対して実際に損失したパケットの数に基づきます。 • 例では、同じPfRマップ シーケンスで一致するトラフィックに対して許容できるパケット損失の相対割合を 20% に設定する set 句を作成します。
ステップ 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set unreachable relative 10`	到達不能ホストの最大数を設定する set 句エントリを作成します。 • このコマンドは、PfR がトラフィック エントリに許可する到達不能ホストの相対割合または最大数（100 万フローあたりのフロー数（fpm））を指定するために使用します。 到達不能ホストの絶対数または相対割合がユーザ定義の値またはデフォルト値を超える場合、PfR はトラフィック クラス エントリが OOP であると判断し、代替出口リンクを検索します。 • 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。 到達不能ホストの相対割合は、短期測定値および長期測定値の比較に基づいています。 • 到達不能ホストの絶対最大数を fpm に基づいて設定するには **threshold** キーワードを使用します。 • 例では、最大の遅延に基づいて学習されたトラフィックに対して到達不能ホストの相対割合が 10% 以上である場合に、トラフィック クラス エントリの新しい出口リンクを検索するようマスター コントローラを設定する set 句エントリを作成します。
ステップ 8	**end** 例： `Router(config-pfr-map)# end`	PfR マップ 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。

パフォーマンスルーティングを使用したBGPインバウンド最適化の設定例

内部プレフィックスを使用したトラフィッククラスの自動学習のための PfR の設定例

次に、ネットワーク内部のプレフィックスを自動的に学習するよう PfR を設定する例を示します。

```
Router> enable
Router#
configure terminal
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# inside bgp
Router(config-pfr-mc-learn)# monitor-period 10
Router(config-pfr-mc-learn)# periodic-interval 20

Router(config-pfr-mc-learn)# prefixes 30
Router(config-pfr-mc-learn)# end
```

PfR モニタリングに対して内部プレフィックスを手動で選択する例

次に、PfR マップを使用してネットワーク内部のプレフィックスを学習するよう PfR を手動で設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip prefix-list INSIDE_PREFIXES seq 20 permit 192.168.1.0/24
Router(config)# pfr-map INSIDE_MAP 10
Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside
Router(config-pfr-map)# end
```

着信トラフィックに対する PfR リンク使用率の変更例

次に、PfR 入口リンク使用率しきい値を変更する例を示します。 この例では、入口使用率が 65% に設定されます。 この出口リンクの使用率が 65 % を超えると、PfR はこの入口リンクを使用していたトラフィック クラスの別の入口リンクを選択します。

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.1.2.1
Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-pfr-mc-br-if)# maximum receive utilization percentage 65
Router(config-pfr-mc-br-if)# end
```

PfR 入口リンク使用率範囲の変更例

次に、PfR 入口使用率範囲を変更する例を示します。 この例では、すべての入口リンクの入口使用率範囲が 15% に設定されます。PfR は最大使用率範囲を使用して入口リンクがポリシーに準拠しているかどうかを判断します。 PfR は、使用率が高すぎる出口またはポリシーに準拠しない出口からのプレフィックスをポリシーに準拠する出口に移動することによって、すべての入口リンクでインバウンド トラフィックを均等化します。

```
Router(config)# pfr master
Router(config-pfr-mc)# max range receive percent 15
Router(config-pfr-mc)# end
```

学習された内部プレフィックスに対する PfR ポリシーの設定および適用例

次に、学習された内部プレフィックスに PfR ポリシーを適用する例を示します。

```
enable
configure terminal
pfr-map INSIDE_LEARN 10
 match pfr learn inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 90
 end
```

設定された内部プレフィックスに対する PfR ポリシーの設定および適用例

次に、INSIDE_CONFIGURE という名前の PfR マップを作成し、手動で設定された内部プレフィックスに PfR ポリシーを適用する例を示します。

```
enable
configure terminal
 pfr-map INSIDE_CONFIGURE 10
 match ip address prefix-list INSIDE_PREFIXES inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 80
 end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンス ルーティングを使用した BGP インバウンド最適化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *6*：パフォーマンス ルーティングを使用した *BGP* インバウンド最適化に関する機能情報

機能名	リリース	機能情報
OER BGP インバウンド最適化	Cisco IOS XE Release 3.3.S	PfR BGP インバウンド最適化は、自律システム内部プレフィックス宛ての自律システム外部のプレフィックスから送信されたトラフィックに対する最適な入口選択をサポートします。自律システムからインターネット サービス プロバイダー（ISP）への外部 EGP（eBGP）アドバタイズメントにより、ネットワークに入るトラフィックの入口パスが影響を受けることがあります。 PfR では、eBGP アドバタイズメントを使用して最適な入口選択を行います。 この機能により、次のコマンドが導入または変更されました。**clear pfr master prefix**、**downgrade bgp**（**PfR**）、**inside bgp**（**PfR**）、**match ip address**（**PfR**）、**match pfr learn**、**max range receive**（**PfR**）、**maximum utilization receive**（**PfR**）、**show pfr master prefix**。

機能名	リリース	機能情報
expire after コマンド[3]	Cisco IOS XE Release 3.3.S	**expire after**（**PfR**）コマンドは、学習済みプレフィックスの有効期間の設定に使用します。デフォルトでは、マスター コントローラは、中央ポリシー データベースから非アクティブなプレフィックスを削除します。これは、メモリが必要とされるためです。 このコマンドを使用すると、制限に基づいて時間またはセッションを設定することによって、この動作を改良できます。 時間ベースの制限は、分単位で設定します。セッション ベースの制限は、監視期間数（またはセッション数）に対して設定します。

[3] これはマイナーな拡張です。 マイナーな拡張は、通常 Feature Navigator に記載されません。

第 6 章

パフォーマンス ルーティング コスト ポリシーの設定

このモジュールでは、Cisco IOS パフォーマンス ルーティング（PfR）コスト ポリシーの設定方法について説明します。 PfR ポリシーは、出口リンクの金銭的なコストに基づいてトラフィックを最適化するよう設定できます。 PfR コストベース最適化機能を使用すると、遅延、損失、使用率などの、設定された他のポリシーに準拠しつつトラフィックを下位のコスト リンクに割り当てることによって金銭的な恩恵がもたらされます。 コストベース最適化は、固定課金方法または階層課金方法を使用して課金されるリンクに適用できます。 また、コストに基づいたロードバランシングも実現できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンス ルーティング コスト ポリシーの前提条件

PfR コスト ポリシーを実装する前に、PfR のしくみの概要と PfR ネットワーク コンポーネントの設定方法を理解する必要があります。詳細については、「パフォーマンス ルーティングの理解」、「ベーシック パフォーマンス ルーティングの設定」、および「アドバンスド パフォーマンス ルーティングの設定」モジュールを参照してください。

パフォーマンス ルーティング コスト ポリシーの概要

PfR ポリシーを設定および適用するには、次の概念を理解する必要があります。

PfR リンク ポリシーの概要

PfR リンク ポリシーは PfR 管理の外部リンクに対して適用される一連のルールです（外部リンクはネットワーク エッジの境界ルータのインターフェイスです）。 リンク ポリシーでは、目的とするリンクのパフォーマンス特性を定義します。 トラフィック クラス パフォーマンス ポリシーのように、リンクを使用する個々のトラフィック クラス エントリのパフォーマンスを定義するのではなく、リンク ポリシーではリンク全体のパフォーマンスを定義します。 リンク ポリシーは、出口（出力）リンクと入口（入力）リンクの両方に適用されます。 次のリンク ポリシー タイプは、リンク ポリシーを使用して管理できるさまざまなパフォーマンス特性を定義します。

トラフィック負荷（使用率）ポリシー

トラフィック負荷（使用率とも呼ばれます）ポリシーは、特定のリンクで伝送できるトラフィック量に関する上限しきい値で構成されます。 Cisco IOS XE PfR は、トラフィック クラスごとの負荷分散をサポートします。 境界ルータに外部インターフェイスが設定されると、境界ルータはデフォルトにより、20 秒ごとにリンク使用率をマスター コントローラに報告します。 出口リンク トラフィックおよび入口リンク トラフィック負荷しきい値は PfR ポリシーとして設定できます。出口または入口リンクの使用率が、設定されたしきい値またはデフォルトしきい値である 75% を超えると、出口または入口リンクがポリシーに準拠していない（OOP）状態になり、PfR はトラフィック クラスの代替リンクを見つけるためにモニタリング プロセスを起動します。 リンク使用率のしきい値は、毎秒あたりのキロバイト数（kbps）で表す絶対値またはパーセンテージとして手動で設定できます。 各インターフェイスの負荷使用率ポリシーは、マスター コントローラで境界ルータを設定する際に設定します。

ヒント　負荷分散を設定する場合は、**load-interval** インターフェイス コンフィギュレーション コマンドを使用して、外部インターフェイスでのインターフェイス負荷計算の間隔を 30 秒に設定することを推奨します。 デフォルトの計算間隔は 300 秒です。 負荷計算は、インターフェイス コンフィギュレーション モードの境界ルータで設定します。 この設定は必須ではありませんが、Cisco IOS XE PfR ができる限り迅速に負荷分散に対応できるよう、これを設定しておくことを推奨します。

トラフィック負荷ポリシーは、単一のリンクで伝達されるトラフィックの上限を定義します。 トラフィック負荷ポリシーの設定の詳細については、「アドバンスドパフォーマンス ルーティングの設定」モジュールの出口リンクのロード バランシング PfR ポリシーの設定例を参照してください。

範囲ポリシー

範囲ポリシーは、確実にトラフィックの負荷が分散されるよう、すべてのリンクを相互に相対的な一定の使用率の範囲内で維持するために定義します。 たとえば、ネットワークに複数の出口リンクがあり、いずれかのリンクを優先する財務上の理由がない場合、最善の選択はすべてのリンクに負荷を均一に分散することです。 従来のルーティング プロトコルによる負荷共有では、必ずしも均一に負荷が分散されるわけではありません。なぜなら、負荷共有はフローベースであり、パフォーマンスまたはポリシー ベースではないからです。 Cisco PfR 範囲機能を使用すると、一連のリンクにおけるトラフィック使用率が所定の割合の範囲内で相互に維持されるように PfR を設定できます。 リンク間の差異が大きくなりすぎると、PfR は使用可能なリンク間にトラフィック クラスを分散し、リンクをポリシー準拠状態に戻そうとします。 デフォルトでは、マスター コントローラは PfR が管理するすべてのリンクに対して最大範囲使用率を 20 % に設定しますが、使用率の範囲は最大割合値を使用して設定できます。

出口リンクおよび入口リンクの使用率範囲は PfR ポリシーとして設定できます。

（注）　範囲ポリシーを設定する場合、シリアル リンクの 80% の使用率は GigabitEthernet リンクの 80% の使用率と大きく異なることに注意してください。

範囲ポリシーは、複数のリンクのトラフィックを負荷分散する方法を定義します。 範囲ポリシーの設定の詳細については、「アドバンスドパフォーマンス ルーティングの設定」モジュールの出口リンクのロード バランシング PfR ポリシーの設定例を参照してください。

コスト ポリシー

コストベース最適化の PfR サポートは、Cisco IOS XE Release 3.3S で導入されました。 コストベース最適化により、ネットワークの各出口リンクの金銭的なコスト（ISP サービス レベル契約（SLA））に基づいてポリシーを設定できます。 PfR コストベース最適化を実装するには、帯域幅使用率の費用効果が最も高い出口リンクからトラフィックを送信し、なおかつ目的とするパ

フォーマンス特性は維持するようにマスター コントローラを設定します。 コスト ポリシーは、複数のリンクのトラフィックを負荷分散する方法を定義します。

コスト ポリシー課金モデル

PfR コストベース最適化は、固定レート課金と階層ベース課金の 2 つの課金方法をサポートします。

固定レート課金は、ISPが帯域幅の使用量に関係なくリンクに対して特定の定額レートを課金する場合に使用します。 外部リンクに対して固定レート課金だけが設定された場合は、コスト最適化に関してすべての出口が平等であると見なされ、プレフィックスまたは出口リンクがポリシーに準拠しているかどうかを判断するために他のパラメータ（遅延、損失、使用率など）が使用されます。

階層ベース課金は、ISPが出口リンク使用率に基づいて階層レートで課金する場合に使用します。各コスト階層は関連する金銭的なコストとともに個別に設定され、階層をアクティブにする帯域幅使用率が定義されます。 階層ベース課金を使用している出口の最小コスト階層は、実際に使用された帯域幅に関係なく毎月課金されます。 階層ベース課金の決定に使用されるアルゴリズムでバーストが発生したときのために、一定の許容差が設定されています。 この場合、「バースト」とは、固定レート課金で高額になる帯域幅使用量が短期間で増加することと定義されます。

固定レート課金では、使用率に関係なく毎月一定額を支払います。 また、階層ベース課金では毎月少なくとも最低階層のコストが発生しますが、最終的な月の階層ベース課金の額は、月の平均使用率に一致する階層に割り当てられたコストによって決まります。

リンク使用率ロールアップ計算

各出口に対する毎月の課金金額を決定する最初の手順は、リンク使用率ロールアップ値を計算することです。 リンク使用率ロールアップ値は、あるロールアップ期間の間、境界ルータの入力インターフェイスと出力インターフェイスから定期的（サンプリング期間）に測定されたリンク使用率の平均値です。 たとえば、サンプリング期間が 60 分に設定され、ロールアップが 1440 分（24 時間）で設定された場合は、リンク使用率ロールアップを計算するために 24 個の入力リンク使用率サンプルと 24 個の出力リンク使用率サンプルが使用されます。 入力リンクと出力リンクに対してリンク使用率ロールアップ値を取得するために、このロールアップ期間から入力サンプルと出力サンプルの各セットの平均値が取得されます。

月間平均使用率計算

リンク使用率ロールアップ計算が実行されたら、月間平均使用率が計算されます。階層ベース課金モデルの固有な詳細は ISP ごとに異なります。 ただし、ほとんどの ISP は階層課金プランで企業が支払うべき金額を計算するために次のアルゴリズムに似たものを使用します。

- ISP ネットワークへのエンタープライズ接続で伝達された出力および入力トラフィックを定期的に測定し、その測定値を収集してロールアップ期間に対するロールアップ値を生成します。
- 課金期間ごとに 1 つまたは複数のロールアップ値を計算します。

- 課金期間のロールアップ値を最大値から最小値の順にランク付けし、スタックに格納します。
- バーストに対応するためにロールアップ値のデフォルトの上位 5%（絶対値または割合値を設定できますが、デフォルト値は 5% です）を廃棄します。 この場合、「バースト」とは、月間平均使用率を超える任意の帯域幅と定義されます。 デフォルトの 5% が破棄された場合、残りのロールアップ値は 95 パーセンタイル順位となります。
- 最大使用率値（この場合は上位 5%）を持つロールアップが削除されたら、ロールアップ値に関連する階層を決定するために、スタック内の残りの最大ロールアップ値（平均 Monthly Target Link Utilization（MTLU）と呼ばれます）を階層構造に適用します。
- 識別された階層に関連する一定のコストに基づいて顧客に課金します。

（注） マスター コントローラがコストベース最適化を実行するには、課金ポリシーを設定し、リンクに適用する必要があります。

月間平均使用率ロールアップ計算で次の 3 種類のテクニックのいずれかを使用するように設定できます。

- 複合
- 分離
- 合算

平均使用率計算テクニックに関する次の説明では、破棄値が絶対値 10 として設定されます。 デフォルトの破棄値は 5% です。

組み合わせテクニックを使用する場合、月間平均使用率計算はソートされた単一のスタックの出力および入力ロールアップ サンプルの組み合わせに基づき、最も大きい 10 個のロールアップ値が破棄されます。次に大きいロールアップ値は MTLU です。

分離テクニックを使用する場合は、リンクの出力および入力ロールアップ サンプルがソートされて異なるスタックに格納され、各スタックの最も大きい10個のロールアップ値が破棄されます。2 つのスタックの残りの最も大きいロールアップ値は MTLU として選択されます。

合算テクニックを使用する場合、出力ロールアップサンプルと入力ロールアップサンプルがひとまとめに合算されます。 各ロールアップ サンプルの合算値は 1 つのスタックに格納され、上位 10 個のロールアップ値が破棄され、次に大きいロールアップ値が MTLU となります。

次の表に、分離テクニックを使用した月間平均使用率の計算例を示します。 次の表では、30 日間のロールアップ値が、出力ロールアップ値と入力ロールアップ値の両方に対して最大の帯域幅から最小の帯域幅の順に示されています。 上位 10 個の値（斜体表示）は、マスター コントローラがロールアップのこの絶対数を破棄するよう設定されたため、破棄されます。 2 つのスタックに残っている次に大きいロールアップ値である 62（太字表示）は月間平均使用率です。 月間平均使用率は、該当する課金期間の該当するリンクの帯域幅使用に対して顧客が課金される階層を決定するために使用されます。

表 *7*：月間平均使用率の計算例

出力ロールアップ	入力ロールアップ	ロールアップは課金期間に最大の帯域幅から最小の帯域幅の順にソートされる
89	*92*	絶対値（斜体の数字を参照）として設定された上位 10 個の出力および入力を破棄します。
80	*84*	
71	*82*	
70	*80*	
65	*78*	
65	*75*	
51	*73*	
50	*84*	
49	*82*	
49	*80*	
45	**62**	廃棄された値の後。 次に大きい値は 62 であり、この値が**月間平均使用率**になります
42	60	
39	55	
35	53	
34	52	
30	45	
30	43	
30	35	
29	33	
25	31	

出力ロールアップ	入力ロールアップ	ロールアップは課金期間に最大の帯域幅から最小の帯域幅の順にソートされる
20	25	
19	23	
12	21	
10	15	
10	11	
9	10	
8	10	
4	5	
1	1	
0	**0**	

パフォーマンス ルーティング コスト ポリシーの設定方法

PfR コストベース ポリシーの設定

このタスクを実行して基本的な PfR コストベース最適化を設定します。 コストベース最適化は、マスター コントローラで 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（外部インターフェイス設定に基づく）を開始し、**cost-minimization** コマンドを使用して設定します。コストベース最適化は階層課金方法と固定課金方法をサポートします。

このタスクでは、マスターコントローラ ルータで設定が行われます。この場合、境界ルータは設定されていると見なされます。 階層ベース課金は、3 つのコスト階層で設定され、サービス プロバイダーのニックネームは ISP1 に設定されます。 月間平均使用率計算テクニックは、合算テクニックを使用するよう設定され、課金サイクルの最終日は月の 30 日になり、タイムゾーンの差異を考慮するために 3 時間のオフセットが提供されます。

cost-minimization コマンドには、さまざまなキーワードと引数があります。 1 つの CLI 行には 1 つの必須キーワードとそれに関連する構文だけしか設定できませんが、このコマンドの複数のインスタンスを入力できます。各境界ルータ リンクの設定内では、**fixed** キーワードと **tier** キーワー

ドだけが同時に使用できます。 完全な構文の詳細については、『*Cisco IOS Performance Routing Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **cost-minimization nickname** *name*
7. **cost-minimization calc** {**combined** | **separate** | **sum**}
8. **cost-minimization sampling period** *minutes* [**rollup** *minutes*]
9. **cost-minimization end day-of-month** *day* [**offset** [**-**] *hh:mm*]
10. **cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*}
11. ステップ 9 を繰り返して階層ベース課金サイクルの追加階層を設定します。
12. **exit**
13. **interface** *type number* **internal**
14. **exit**
15. ステップ 14 を繰り返して 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。
16. ステップ 4 ～ 15 を繰り返し、他のリンクに対して追加のコストベース最適化ポリシーを設定します（必要な場合）。
17. **mode route control**
18. **resolve cost priority** *value*
19. **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。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**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、グローバル プレフィックスおよび出口リンク ポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Router(config-pfr-mc)# border 10.100.1.1 key-chain PFR_cost`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界ルータを識別するために、IP アドレスを設定します。 • *key-chain-name* 引数の値は、*ip-address* 引数により識別された境界ルータで設定されたキー チェーン名に一致する必要があります。 （注） 境界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、この境界ルータを再設定したり、ルータの設定を追加したりする場合、このキーワードは省略可能です。
ステップ 5	**interface** *type number* **external** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	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 モードを開始して、境界ルータ インターフェイスを外部インターフェイスとして設定します。 • 各境界ルータでは、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。
ステップ 6	**cost-minimization nickname** *name* 例： `Router(config-pfr-mc-br-if)# cost-minimization nickname ISP1`	マスターコントローラのコストベース最適化ポリシー内で境界ルータ インターフェイスのニックネームを設定します。 • **nickname** キーワードを使用してサービス プロバイダーを識別するラベルを適用します。 • この例では、サービス プロバイダーに対して ISP1 のラベルが設定されます。
ステップ 7	**cost-minimization calc** {**combined** | **separate** | **sum**} 例： `Router(config-pfr-mc-br-if)# cost-minimization calc sum`	コスト最小料金をどのように計算するかを設定します。 • **combined** キーワードを使用して入力サンプルと出力サンプルを組み合わせるようマスター コントローラを設定します。 • **separate** キーワードを使用して入力サンプルと出力サンプルを別々に分析するようマスター コントローラを設定します。 • **sum** キーワードを使用して最初に入力サンプルと出力サンプルを追加し、次にサンプルを組み合わせるようマスター コントローラを設定します。

	コマンドまたはアクション	目的
		• この例では、合算テクニックを使用してコスト最小料金が計算されます。
ステップ 8	**cost-minimization sampling period** *minutes* [**rollup** *minutes*] 例： `Router(config-pfr-mc-br-if)# cost-minimization sampling period 10 rollup 60`	サンプリング期間を分単位で指定します。 • サンプリング期間 *minutes* 引数に入力できる値は 1 ～ 1440 の数字です。 • 省略可能な **rollup** キーワードを使用してサンプルが *minutes* 引数に指定された間隔でロールアップされるよう指定します。ロールアップ *minutes* 引数に入力できる値は 1 ～ 1440 の数字です。 入力できる最も小さい数字は、サンプリング期間に入力された数字以上である必要があります。 • この例では、サンプリング間の間隔が 10 分に設定されます。これらのサンプルは 60 分ごとにロールアップされるよう設定されます。
ステップ 9	**cost-minimization end day-of-month** *day* [**offset** [**-**] *hh:mm*] 例： `Router(config-pfr-mc-br-if)# cost-minimization end day-of-month 30 offset 5:00`	課金サイクルの最終日を設定するために使用するパラメータを設定します。 • 省略可能な **offset** キーワードを使用して UTC とは異なるゾーンのサービス プロバイダーを考慮するためにサイクルの最後を調整します。 省略可能な「-」キーワードは、タイム ゾーンが UTC よりも進んでいる場合にマイナスの時間と分を指定するために使用します。 • この例では、課金サイクルの最終日は月の 30 日であり、UTC に 5 時間のオフセットが追加されます。
ステップ 10	**cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*} 例： `Router(config-pfr-mc-br-if)# cost-minimization tier 100 fee 1000`	使用量に基づかない固定コスト課金サイクルまたは階層ベース課金サイクルの階層を設定します。 • **fixed fee** キーワードと *cost* 引数は、出口リンクに関連する固定（使用量に基づかない）コストを指定するために使用します。 • *percentage* 引数は、コスト階層の使用率を指定するために使用します。 • **tier fee** キーワードと *fee* 引数は、この階層に関連するコストを指定するために使用します。 • この例では、100% の使用率に対する階層ベースの料金が 1000 に設定されます。

	コマンドまたはアクション	目的
		（注） 指定された最初の階層は 100% の使用率である必要があります。 それ以降の階層設定は、低い割合と低い料金で行う必要があります。
ステップ 11	ステップ 9 を繰り返して階層ベース課金サイクルの追加階層を設定します。	--
ステップ 12	**exit** **例**： `Router(config-pfr-mc-br-if)# exit`	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 モードを終了し、PfR 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* **internal** **例**： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal`	境界ルータ 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。 • 各境界ルータでは、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 14	**exit** **例**： `Router(config-pfr-mc-br-if)# exit`	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 モードを終了し、PfR 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 15	ステップ 14 を繰り返して 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 4 ～ 15 を繰り返し、他のリンクに対して追加のコストベース最適化ポリシーを設定します（必要な場合）。	--
ステップ 17	**mode route control** **例**： `Router(config-pfr-mc)# mode route control`	一致するトラフィックにルート制御を設定します。 • 制御モードでは、マスターコントローラが監視対象プレフィックスを分析し、ポリシー パラメータに基づいて変更を実行します。

	コマンドまたはアクション	目的
ステップ 18	**resolve cost priority** *value* 例： `Router(config-pfr-mc)# resolve cost priority 1`	コスト ポリシーに対してポリシー優先度を設定します。 • 解決ポリシーは、コスト ポリシーが最も高い優先度を持つように設定します。 • このタスクでは、PfR ポリシーの 1 つの種類だけに優先度が割り当てられます。 通常は、他の PfR ポリシーが設定され、優先度を慎重に確認する必要があることに注意してください。
ステップ 19	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

次の例はタスクで示された単なる設定例ですが、階層ベースでの料金設定を行うために階層が追加されています。 固定レート課金と階層ベース課金の両方を含む基本的な PfR コスト ポリシーのより詳細な設定例については、基本 PfR コストベース ポリシーの設定例に関する項を参照してください。

```
pfr master
 border 10.100.1.1 key-chain PFR_cost
  interface GigabitEthernet 0/0/0 external
   cost-minimization nickname ISP1
   cost-minimization calc sum
   cost-minimization sampling period 10 rollup 60
   cost-minimization end day-of-month 30 offset 5:00
   cost-minimization tier 100 fee 1000
   cost-minimization tier 70 fee 700
   cost-minimization tier 50 fee 500
   exit
  interface GigabitEthernet 0/0/1 internal
  exit
 mode route control
 resolve cost priority 1
 end
```

PfR コスト ポリシーを使用した課金の最小化とトラフィックのロード バランス

基本的な PfR コストベース最適化が有用である一方で、多くの企業は複数の境界ルータ出口リンクを持ち、複数のさまざまなサービス プロバイダーは使用された帯域幅に応じて増加するさまざまな課金レートを課金します。 この状況では、コスト最小化ポリシーに加えて、リンクに対して何らかの形のトラフィックのロード バランシングが必要になることがあります。

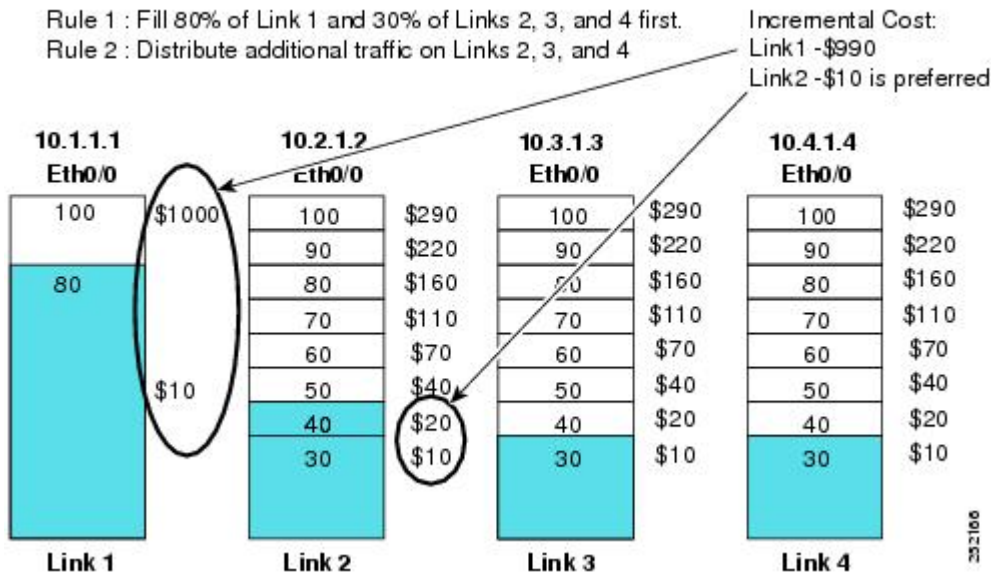
マスターコントローラでこのタスクを実行し、リンクでトラフィックをロードバランシングしつつ複数の境界ルータ出口リンクに対して毎月の課金を最小化するパフォーマンスルーティングコストポリシーを設定します。このシナリオでは、ネットワークは固定レート課金と階層ベース課金の両方を持ち、顧客が固定レート課金と階層ベース課金のプリペイド（最小コスト）階層に対して毎月の料金を支払うことを前提とし、PfR はコストを最適化しつつトラフィックのロード バランシングを実行できます。

次の図に、この図でルールとして指定されたサービス レベル契約（SLA）で定義された帯域幅とコスト パラメータを使用して各リンクに対してさまざまな課金レートを定義する例を示します。このタスクの主な目的は、外部リンクごとの課金を最小化し、外部リンクに対してトラフィックをロード バランスすることです。 リンク 1 は固定レートで課金され、リンク 2 ～ 4 は階層ベース課金に基づきますが、すべてのリンクは PfR 階層として設定されます。 コスト最小化を実現するために、最初のルールはリンク 1 の 80 %、リンク 2、3、および 4 の 30 % を使用します（次の図を参照）。 2 つ目のルールはリンク 2、3 および 4 で追加のトラフィックを分散し、トラフィック負荷を分散します。 コストを最小化しつつトラフィックのロード バランシングを実現するために、すべての出口で分散されたコストと負荷に対して PfR トラフィックが最適化されるよう人為的なコストが割り当てられた帯域幅割合を表す複数の階層を使用して PfR コスト ポリシーを設定します。 設定された階層については、次の図を参照してください。

このタスクの手順に従うと、PfR がトラフィックを最小コストの出口のいずれかから最初に送信するよう設定されるコスト ポリシーが作成されます。リンク 1 には 10.1.1.1 が割り当てられ、プリペイド階層は他の 3 つの出口から構成されます。 各リンクのプリペイド階層帯域幅が完全に使用されると、ソフトウェアはすべてのリンクの階層間で次に最も小さい増分コストを決定します。リンク 1 の次の階層を使用する増分コストは $990 です。 リンク 2 の次の階層を使用する増分コストはたった $10 です。 PfR は、リンク 2 の帯域幅の 40 % を表す青色のバーである次に最も小さいコスト階層にトラフィックを転送します（次の図を参照）。プロセスは引き続きリンク 2、3、および 4 で負荷を分散するコストを使用します。 このタスクは、リンク 1 ～ 4 のプリペイド帯域幅を最初に使用して出口リンクごとの月間課金レートがどのように最小化されるかを示します。

この場合、階層間で最小の増分コストを決定することによりトラフィックはリンク 2、3、および 4 で効果的に負荷分散されます。

図 *11*：課金の最小化とトラフィックをロード バランスする *PfR* コスト最小化ソリューションを示す図



次のタスクの手順では、出口リンク 10.1.1.1 は階層ベース リンクとして設定されます（ただし、実際には固定レートで課金されます）。 固定レート リンクがロード バランシングの階層として設定された場合、月間コスト計算はそのリンクの実際のコストを反映しません。 このソリューションを使用した場合は、複数の階層に割り当てられた人為的なコストがすべての月間コスト計算の精度に影響を及ぼすことがあります。

概要と詳細な手順にはこのタスク シナリオの一部の設定手順だけが示されており、マスター コントローラの完全な設定は詳細な手順の表の後に示された「例」の項に記載されています。

（注） コスト最小化機能と競合する可能性があるため、範囲および使用率ポリシー優先度をディセーブルにします。

（注） システム チャーンを回避するために、**periodic**（PfR）または **set periodic**（PfR）コマンドを時間間隔とともに設定しないでください。システムは、指定された間隔で最良の出口リンクを選択しようと試みます。 このコマンドは、デフォルトでディセーブルになっています。

cost-minimization（PfR）コマンドには、さまざまなキーワードと引数があります。 1 つの CLI 行には 1 つの必須キーワードとそれに関連する構文だけしか設定できませんが、このコマンドの複数のインスタンスを入力できます。 各境界ルータ リンクの設定内では、**fixed** キーワードと **tier**

キーワードだけが同時に使用できます。 完全な構文の詳細については、『*Cisco IOS Performance Routing Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **cost-minimization nickname** *name*
7. **cost-minimization summer-time** *start end* [*offset*]
8. **cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*}
9. ステップ 8 を繰り返して階層ベース課金サイクルの追加階層を設定します。
10. **cost-minimization discard** [**daily**] {**absolute** *number*| **percent** *percentage*}
11. **exit**
12. **interface** *type number* **internal**
13. **exit**
14. ステップ 13 を繰り返して 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。
15. ステップ 4 ～ 14 を繰り返し、他のリンクに対して追加のコストベース最適化ポリシーを設定します（必要な場合）。
16. **mode route control**
17. **policy-rules** *map-name*
18. **exit**
19. **pfr-map** *map-name sequence-number*
20. **match pfr learn** {**delay**| **inside**| **throughput**}
21. **set resolve cost priority** *value*
22. **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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**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、グローバル プレフィックスおよび出口リンク ポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Router(config-pfr-mc)# border 10.1.1.1 key-chain pfr`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界ルータを識別するために、IP アドレスを設定します。 • *key-chain-name* 引数の値は、*ip-address* 引数により識別された境界ルータで設定されたキー チェーン名に一致する必要があります。 （注） 境界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、この境界ルータを再設定したり、ルータの設定を追加したりする場合、このキーワードは省略可能です。
ステップ 5	**interface** *type number* **external** 例： `Router(config-pfr-mc-br)# interface ethernet 0/0 external`	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 モードを開始して、境界ルータ 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します。 • 各境界ルータでは、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。 • 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。
ステップ 6	**cost-minimization nickname** *name* 例： `Router(config-pfr-mc-br-if)# cost-minimization nickname 80-percent`	マスター コントローラのコストベース最適化ポリシー内で境界ルータ インターフェイスのニックネームを設定します。 • この例では、10.1.1.1 境界ルータ リンクのニックネーム ラベルは 80-percent です。

	コマンドまたはアクション	目的
ステップ 7	**cost-minimization summer-time** *start end* [*offset*] 例： `Router(config-pfr-mc-br-if)# cost-minimization summer-time 2 Sunday March 02:00 1 Sunday November 02:00 60`	サマー タイム（デイライト セービング）の開始および終了日時を指定します。 • *start* 引数と *end* 引数は、サマータイムが始まる、または終わる週、日、月、時間、分（24 時間時計）を指定するために使用します。 • *offset* 引数を使用すると、1 ～ 120 分のオフセットが許可され、最大 2 時間を春に加算し、秋に減算できます。 • この例では、サマー タイムは 3 月の第 2 週日曜日の午前 2 時に 1 時間加算されて始まり、11 月の第 1 週日曜日の午前 2 時に 1 時間減算されて終わります。 （注） **summer-time** キーワード設定は各マスター コントローラに対して 1 回だけ必要です。
ステップ 8	**cost-minimization** {**fixed fee** *cost*| **tier** *percentage* **fee** *fee*} 例： `Router(config-pfr-mc-br-if)# cost-minimization tier 100 fee 1000`	使用量に基づかない固定コスト課金サイクルまたは階層ベース課金サイクルの階層を設定します。 • **fixed fee** キーワードと *cost* 引数は、出口リンクに関連する固定（使用量に基づかない）コストを指定するために使用します。 • *percentage* 引数は、コスト階層の使用率を指定するために使用します。 • **tier fee** キーワードと *fee* 引数は、この階層に関連するコストを指定するために使用します。 • この例では、100% の使用率に対する階層ベースの料金が 1000 に設定されます。 （注） 指定された最初の階層は 100% の使用率である必要があります。 それ以降の階層設定は、低い割合と低い料金で行う必要があります。 ロード バランシングのために階層を設定する場合は、ロードバランシングが機能するために、同じリンクのある階層から次の階層に段階的に階層を大きくする必要があります。
ステップ 9	ステップ 8 を繰り返して階層ベース課金サイクルの追加階層を設定します。	--
ステップ 10	**cost-minimization discard** [**daily**] {**absolute** *number*| **percent** *percentage*}	月間平均使用率値を計算する場合は、爆発的なリンク使用率に対して削除するサンプルの数を設定します。

	コマンドまたはアクション	目的
	例： `Router(config-pfr-mc-br-if)# cost-minimization discard percent 5`	• 使用率サンプルは、最も大きい値から最も小さい値の順にソートされ、このコマンドを使用して設定された数または割合により、リストから最も大きい数または割合が削除されます。 • 省略可能な **daily** キーワードが入力された場合は、サンプルが毎日分析され、破棄されます。 **daily** キーワードが入力されない場合は、デフォルトでサンプルが毎月分析され、破棄されます。 課金サイクルの最後に、1 日の平均使用率の平均値を求めることによって月間平均使用率が計算されます。 • **absolute** キーワードを使用して削除する一定の数のサンプルを設定します。 • **percentage** キーワードを使用して削除する一定の割合のサンプルを設定します。 • サンプリング ロールアップが設定されている場合は、破棄値がロールアップに適用されます。 • この例では、月間平均使用率値を計算するときに上位 5% のサンプルが削除されます。
ステップ 11	**exit** 例： `Router(config-pfr-mc-br-if)# exit`	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 モードを終了し、PfR 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 12	**interface** *type number* **internal** 例： `Router(config-pfr-mc-br)# interface Ethernet 1/0 internal`	境界ルータ 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。 • 各境界ルータでは、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 13	**exit** 例： `Router(config-pfr-mc-br-if)# exit`	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 モードを終了し、PfR 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 14	ステップ 13 を繰り返して 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。	--

	コマンドまたはアクション	目的
ステップ 15	ステップ 4 ～ 14 を繰り返し、他のリンクに対して追加のコストベース最適化ポリシーを設定します（必要な場合）。	--
ステップ 16	**mode route control** 例： `Router(config-pfr-mc)# mode route control`	一致するトラフィックにルート制御を設定します。 • 制御モードでは、マスター コントローラが監視対象プレフィックスを分析し、ポリシー パラメータに基づいて変更を実行します。
ステップ 17	**policy-rules** *map-name* 例： `Router(config-pfr-mc)# policy-rules cost_balance`	PfR マップからの設定をマスター コントローラ設定に適用します。 • この例では、cost_balance という名前の PfR マップからの設定が適用されます。
ステップ 18	**exit** 例： `Router(config-pfr-mc)# exit`	PfR マスター コントローラ コンフィギュレーション モードを終了し、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 19	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map cost_balance 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。
ステップ 20	**match pfr learn** {**delay**| **inside**| **throughput**} 例： `Router(config-pfr-map)# match pfr learn throughput`	学習済みの PfR プレフィックスに一致させるために、PfR マップ内で match 句エントリを作成します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • この例では、最大アウトバウンド スループットを使用して学習されたトラフィック クラスに一致する match 句エントリが作成されます。
ステップ 21	**set resolve cost priority** *value* 例： `Router(config-pfr-map)# set resolve cost priority 1`	重複するポリシーに対してポリシー優先度を設定する set 句エントリを PfR マップで作成します。 • この例では、解決ポリシーは、コスト ポリシーが最も高い優先度を持つように設定します。

	コマンドまたはアクション	目的
		• このタスクでは、PfR ポリシーの 1 つの種類だけに優先度が割り当てられます。 通常は、他の PfR ポリシーが設定され、優先度を慎重に確認する必要があることに注意してください。
ステップ 22	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

次の設定例は、このタスク手順の上の図でマスター コントローラで制御されたすべてのリンクに対する完全な設定です。 コストをこのタスクの最大優先度にするために使用された cost_balance という名前の PfR マップの set resolve cost priority 1 コマンドに注意してください。 それとは逆に、最適化の競合を回避するために、resolve range コマンドと resolve utilization コマンドがディセーブルになります。 関連する **show** コマンドからの出力については、「PfR コスト最小化ポリシーの検証とデバッグ」の項を参照してください。

```
pfr master
 logging
 border 10.1.1.1 key-chain pfr
  interface Ethernet1/0 internal
  interface Ethernet0/0 external
   cost-minimization nickname 80-percent
   cost-minimization summer-time 2 Sunday March 02:00 1 Sunday November 02:00 60
   cost-minimization tier 100 fee 1000
   cost-minimization tier 80 fee 10
   cost-minimization discard percent 5
   exit
  exit
 border 10.2.1.2 key-chain pfr
  interface Ethernet1/0 internal
  interface Ethernet0/0 external
   cost-minimization nickname 30-meg
   cost-minimization tier 100 fee 290
   cost-minimization tier 90 fee 220
   cost-minimization tier 80 fee 160
   cost-minimization tier 70 fee 110
   cost-minimization tier 60 fee 70
   cost-minimization tier 50 fee 40
   cost-minimization tier 40 fee 20
   cost-minimization tier 30 fee 10
   cost-minimization discard percent 5
   exit
  exit
 border 10.3.1.3 key-chain pfr
  interface Ethernet1/0 internal
  interface Ethernet0/0 external
   cost-minimization nickname 30-meg-2
   cost-minimization tier 100 fee 290
   cost-minimization tier 90 fee 220
   cost-minimization tier 80 fee 160
   cost-minimization tier 70 fee 110
   cost-minimization tier 60 fee 70
```

```
   cost-minimization tier 50 fee 40
   cost-minimization tier 40 fee 20
   cost-minimization tier 30 fee 10
   cost-minimization discard percent 5
   exit
  exit
 border 10.4.1.4 key-chain pfr
  interface Ethernet1/0 internal
  interface Ethernet0/0 external
   cost-minimization nickname 30-meg-3
   cost-minimization tier 100 fee 290
   cost-minimization tier 90 fee 220
   cost-minimization tier 80 fee 160
   cost-minimization tier 70 fee 110
   cost-minimization tier 60 fee 70
   cost-minimization tier 50 fee 40
   cost-minimization tier 40 fee 20
   cost-minimization tier 30 fee 10
   cost-minimization discard percent 5
   exit
  exit
  learn
   throughput
   periodic-interval 0
   monitor-period 1
   prefixes 2500
   aggregation-type prefix-length 32
   exit
  mode route control
  policy-rules cost_balance
  max-range-utilization percent 100
  exit
 pfr-map cost_balance 10
  match pfr learn throughput
  set resolve cost priority 1
  no set resolve range
  no set resolve utilization
  set probe frequency 10
  end
```

PfR コスト最小化ポリシーの検証とデバッグ

マスター コントローラでこのタスクを実行して、コスト最小化ポリシーを検証し、問題をデバッグするのに役に立つ情報を表示します。 コスト最小化ポリシーが設定され、トラフィックに適用されると、**show** コマンドの手順に従って、ポリシー設定が期待したように動作していることを検証できます。 ポリシー設定が期待したように動作していない場合は、**debug** コマンドの手順に従って問題のトラブルシューティングを行うことができます。 **show** コマンドと **debug** コマンドはどちらも省略可能で、任意の順で入力できます。

はじめる前に

これらの手順を実行する前に、コスト ポリシーを設定し、PfR トラフィックに適用する必要があります。

手順の概要

1. **enable**
2. **show pfr master cost-minimization** {**border** *ip-address* [*interface*] | **nickname** *name*}
3. **show pfr master cost-minimization billing-history**
4. **debug pfr master cost-minimization** [**detail**]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr master cost-minimization** {**border** *ip-address* [*interface*] | **nickname** *name*}

border キーワードと **nickname** キーワードの両方を **show pfr master cost-minimization** コマンドで使用すると、同じコスト最小化情報が表示されます。 これらのキーワードと引数は、指定された境界ルータをニックネームや IP アドレスで識別したり、任意でルータの特定のインターフェイスに対して識別したりするために使用できます。 この手順に適用できる構文だけが示されています。 完全な構文については、『*Cisco IOS Performance Routing Command Reference*』を参照してください。

この例では、上の図の 10.2.1.2 リンクに関する情報が表示されます。 このリンクに設定されるコスト階層の数に注意してください。 10.3.1.3 と 10.4.1.4 のリンクは、より正確なロード バランシングを可能にするために同じコスト階層セットを持ちます。絶対値5として示された破棄値に対して設定されたロールアップ値とパラメータに関する情報が存在します。 この出力で示されたフィールドの詳細については、『*Cisco IOS Performance Routing Command Reference*』を参照してください。

例：

```
Router# show pfr master cost-minimization border 10.2.1.2 GigabitEthernet 3/2/0
pM - per Month, pD - per Day
 --------------------------------------------------------------------------------
  Nickname  : 30-meg           Border: 10.2.1.2         Interface: Gi3/2/0
  Calc type : Separate
  End Date  : 1
  Summer time: Enabled,  2 Sun Mar 02:00 1 Sun Nov 02:00 60
  Fee       : Tier Based
              Tier 1: 100, fee:   290
              Tier 2:  90, fee:   220
              Tier 3:  80, fee:   160
              Tier 4:  70, fee:   110
              Tier 5:  60, fee:    70
              Tier 6:  50, fee:    40
              Tier 7:  40, fee:    20
              Tier 8:  30, fee:    10
  Period    : Sampling 5, Rollup 5
  Discard   : Type Absolute, Value 5

  Rollup Information:
  Total(pM)       Discard(pM)     Remaining(pM)   Collected(pM)
  8928            5               1460            264

  Current Rollup Information:
    MomentaryTgtUtil:          382 Kbps    CumRxBytes:           747167
   StartingRollupTgt:          400 Kbps    CumTxBytes:          4808628
    CurrentRollupTgt:          400 Kbps    TimeRemain:         00:03:23

  Rollup Utilization (Kbps):
  Egress Utilization Rollups (Descending order)

  1   : 0           2   : 440          3   : 439          4   : 398
  5   : 383         6   : 378          7   : 375          8   : 372
  9   : 371         10  : 371          11  : 370          12  : 370
  13  : 368         14  : 365          15  : 255          16  : 231
```

```
 17  : 216          18  : 197          19  : 196          20  : 196
 21  : 195          22  : 194          23  : 191          24  : 190
 25  : 190          26  : 184          27  : 183          28  : 182
 29  : 178          30  : 177          31  : 176          32  : 175
```

ステップ 3 **show pfr master cost-minimization billing-history**

このコマンドは、以前の課金期間の課金情報を表示するために使用されます。この例では、月間平均使用率は 62 であり、境界ルータ 10.1.1.1 のギガビットイーサネット インターフェイス 3/0/0 リンクのコストは $10,000 です。

例：

```
Router# show pfr master cost-minimization billing-history

Billing History for the past three months

         ISP2 on 10.4.1.4          Gi4/0/0
  No cost min on 10.2.1.2          Gi3/2/0
         ISP1 on 10.1.1.1          Gi3/0/0
                  Mon1                 Mon2                 Mon3
 Nickname     SustUtil       Cost   SustUtil       Cost   SustUtil       Cost
 ----------    ------------------    ------------------   ------------------
    ISP2             0       3000        ---NA---            ---NA---
    ISP1            62      10000        ---NA---            ---NA---

 ----------    ------------------    ------------------   ------------------
 Total Cost                13000                     0                     0
```

ステップ 4 **debug pfr master cost-minimization** [**detail**]

このコマンドは、コスト最小化ポリシーのデバッグ情報を表示するために使用されます。次に、コスト最小化ポリシーの詳細なデバッグ情報の例を示します。

例：

```
Router# debug pfr master cost-minimization detail

OER Master cost-minimization Detail debugging is on
*May 14 00:38:48.839: OER MC COST: Momentary target utilization for exit 10.2.1.2 i/f
GigabitEthernet3/2/0 nickname ISP1 is 7500 kbps, time_left 52889 secs, cumulative 16 kb,
rollup period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:38:48.839: OER MC COST: Cost OOP check for border 10.2.1.2, current util: 0
target util: 7500 kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 ingress Kbps
*May 14 00:39:00.199: OER MC COST: ISP1 calc separate rollup ended at 55 egress bytes
*May 14 00:39:00.199: OER MC COST: Target utilization for nickname ISP1 set to 6000,
rollups elapsed 4, rollups left 24
*May 14 00:39:00.271: OER MC COST: Momentary target utilization for exit 10.2.1.2 i/f
GigabitEthernet3/2/0 nickname ISP1 is 7500 kbps, time_left 52878 secs, cumulative 0 kb,
rollup period 84000 secs, rollup target 6000 kbps, bw_capacity 10000 kbps
*May 14 00:39:00.271: OER MC COST: Cost OOP check for border 10.2.1.2, current util: 0
target util: 7500 kbps
```

パフォーマンス ルーティング コスト ポリシーの設定例

PfR コストベース ポリシーの設定例

次に、マスターコントローラでコストベース最適化を設定する例を示します。 コストベース最適化設定は、外部インターフェイス設定に基づいて適用されます。 この例では、境界ルータ 10.2.1.2 のいずれかの出口インターフェイスに対する階層課金サイクルと、境界ルータ 10.2.1.2 の他の出口インターフェイスおよび境界ルータ 10.3.1.3 の両方の出口インターフェイスに対する固定課金サイクルを持つ複数の出口に対してポリシーが設定されます。

このシナリオでは、PfR は最初に固定レート出口（境界ルータ 10.2.1.2 のギガビットイーサネット インターフェイス 0/0/2 および境界ルータ 10.3.1.3 のギガビットイーサネット インターフェイス 0/0/3 と 0/0/4）を使用してトラフィックを送信します。この理由は、帯域幅コストが、階層ベースの出口よりもこれらの固定料金出口のほうが低いためです。 固定レート出口が完全に使用されると、トラフィックは境界ルータ 10.2.1.2 のギガビットイーサネット インターフェイス 0/0/0 から送信されます。 月間平均使用率が 40% 以下の場合は、その月の課金額は $4000 になります。 月間平均使用率がそれよりも大きい場合は、月間平均使用率に一致する階層が課金されます。 この例では、計算設定が入力されず、デフォルトの動作がトリガーされます。計算は出力サンプルと入力サンプルに対して別々に実行されます。

この設定例では、境界ルータがすでに設定されていることを前提としています。

```
pfr master
 no periodic
 resolve cost priority 1
 no resolve delay
 no resolve utilization
 border 10.2.1.2 key-chain key_cost1
  interface GigabitEthernet0/0/0 external
   cost-minimization tier 100 fee 10000
   cost-minimization tier 75 fee 8000
   cost-minimization tier 40 fee 4000
   cost-minimization end day-of-month 31
  interface GigabitEthernet0/0/2 external
   cost-minimization fixed fee 3000
 border 10.3.1.3 key-chain key_cost2
  interface GigabitEthernet0/0/3 external
   cost-minimization fixed fee 3000
  interface GigabitEthernet0/0/4 external
   cost-minimization fixed fee 3000
   end
```

PfR コスト ポリシーを使用した課金の最小化とトラフィックのロードバランスの例

次に、コスト最小化ポリシーを設定し、複数のリンクで PfR トラフィック負荷を分散する例を示します。 このタスクは各リンクのコストを最小化し、複数の境界ルータ リンクでロード バランシングを正確に制御するよう設計されています。 このタスクは、PfR で最初に最も小さいコスト

階層の帯域幅を強制的に使用し、次にすべてのリンクで次に最も小さいコスト階層を強制的に使用することにより、複数のリンク間でロード バランシングを制御します。

show pfr master cost-minimization コマンドのキーワードは、特定のリンクの使用率を月の出力および入力ロールアップ値とともに表示するために使用されます。 月の課金期間が終わると、課金履歴の別のキーワード オプションにより月間平均使用率とリンク コストが表示されます。

境界ルータ 10.1.1.1

```
key chain key1
  key 1
    key-string border1
!
pfr border
  logging
  local GigabitEthernet3/0/0
  master 10.1.1.1 key-chain key1
```

すべての境界ルータを設定する場合は、類似の設定を使用し、適切な変更を行ってください。 次に、マスター コントローラを設定します。

マスター コントローラ

```
key chain key1
  key 1
    key-string border1
 key chain key2
  key 1
    key-string border2
 key chain key3
  key 1
    key-string border3
 pfr master
  logging
  border 10.1.1.1 key-chain key1
   interface GigabitEthernet3/0/0 external
    cost-minimization nickname ISP1
    cost-minimization tier 100 fee 50000
    cost-minimization tier 65 fee 10000
    cost-minimization tier 30 fee 500
    cost-minimization end day-of-month 24
    cost-minimization sampling period 5 rollup 1440
    cost-minimization discard absolute 10
    exit
   interface GigabitEthernet3/0/1 internal
   exit
  border 10.2.1.2 key-chain key2
   interface GigabitEthernet3/2/0 external
   interface GigabitEthernet3/0/0 internal
   exit
  border 10.4.1.4 key-chain key3
   interface GigabitEthernet4/0/0 external
    cost-minimization nickname ISP2
    cost-minimization fixed fee 3000
    cost-minimization end day-of-month 24
    exit
   interface GigabitEthernet4/0/2 internal
   exit
  no max range receive
  delay threshold 10000
  loss threshold 1000000
  mode route control
  mode monitor passive
  mode select-exit best
  resolve cost priority 1
```

```
  active-probe echo 10.1.9.1
  end
```

マスター コントローラで **show pfr master cost-minimization border** コマンドを入力して設定と使用率を表示します。 境界ルータ 10.1.1.1 のギガビットイーサネット インターフェイス 3/0/0 に対する 3 月から 4 月 24 日までの 30 日間の課金期間のロールアップ値が出力に表示されます。

```
Router# show pfr master cost-minimization border 10.1.1.1
pM - per Month, pD - per Day
 --------------------------------------------------------------------------------
  Nickname  : ISP1             Border: 10.1.1.1          Interface: Gi3/0/0
  Calc type : Separate
  End Date  : 24
  Summer time: Disabled
  Fee       : Tier Based
              Tier 1: 100, fee:      50000
              Tier 2:  65, fee:      10000
              Tier 3:  30, fee:        500
  Period    : Sampling 5, Rollup 1440
  Discard   : Type Absolute, Value 10

  Rollup Information:
  Total(pM)       Discard(pM)     Remaining(pM)   Collected(pM)
  31              10              1               29

  Current Rollup Information:
    MomentaryTgtUtil:           75 Kbps    CumRxBytes:                0
   StartingRollupTgt:           75 Kbps    CumTxBytes:                0
    CurrentRollupTgt:           75 Kbps    TimeRemain:         00:00:51

  Rollup Utilization (Kbps):
  Egress Utilization Rollups (Descending order)

  1   : 0           2   : 89          3   : 80          4   : 71
  5   : 70          6   : 65          7   : 65          8   : 51
  9   : 50          10  : 49          11  : 49          12  : 45
  13  : 42          14  : 39          15  : 35          16  : 34
  17  : 30          18  : 30          19  : 30          20  : 29
  21  : 25          22  : 20          23  : 19          24  : 12
  25  : 10          26  : 10          27  : 9           28  : 8
  29  : 4           30  : 1
  Ingress Utilization Rollups (Descending order)

  1   : 0           2   : 92          3   : 84          4   : 82
  5   : 80          6   : 78          7   : 75          8   : 73
  9   : 72          10  : 70          11  : 63          12  : 62
  13  : 60          14  : 55          15  : 53          16  : 52
  17  : 45          18  : 43          19  : 35          20  : 33
  21  : 31          22  : 25          23  : 23          24  : 21
  25  : 15          26  : 11          27  : 10          28  : 10
  29  : 5           30  : 1
```

3 月から 4 月 24 日までの課金期間が終了したと仮定すると、**show pfr master cost-minimization billing-history** コマンドを使用して以前の課金期間の課金を参照できます。 月間平均使用率は 62 であり、境界ルータ 10.1.1.1 のギガビットイーサネット インターフェイス 3/0/0 リンクのコストは $10,000 です。

```
Router# show pfr master cost-minimization billing-history
Billing History for the past three months

         ISP2 on 10.4.1.4          Gi4/0/0
  No cost min on 10.2.1.2          Gi3/2/0
         ISP1 on 10.1.1.1          Gi3/0/0
                  Mon1                 Mon2                 Mon3
 Nickname     SustUtil       Cost   SustUtil       Cost   SustUtil       Cost
 ----------    ------------------    ------------------   ------------------
    ISP2             0       3000        ---NA---             ---NA---
    ISP1            62      10000        ---NA---             ---NA---
```

```
----------    ------------------    ------------------    ------------------
Total Cost                 13000                     0                     0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンス ルーティング コスト ポリシーの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *8*：パフォーマンス ルーティング コスト ポリシーの設定に関する機能情報

機能名	リリース	機能の設定情報
コストベース最適化向け OER サポート	Cisco IOS XE Release 3.3S	コストベース最適化向け OER サポート機能で、出口リンク ポリシー ベースの金銭的なコストを設定し、ホップバイホップ ベースでプレフィックス特性を調べるために traceroute プローブを設定できるようになりました。 この機能により、次のコマンドが導入または変更されました。**cost-minimization**（**PfR**）、**debug pfr master cost-minimization**、**show pfr master cost-minimization**。

第 7 章

PfR Data Export v1.0 NetFlow v9 フォーマット

パフォーマンス ルーティング（PfR）Data Export v1.0 NetFlow v9 フォーマット機能により、RFC 3954『*Cisco Systems NetFlow Services Export Version 9*』でサポートされている NetFlow v9 標準プロトコルとフォーマットを使用してリアルタイム PfR パフォーマンス データのエクスポートを簡素化できます。 通常の時間ベースのパフォーマンス データと、PfR ルート ポリシー制御イベント データの両方をエクスポートできます。

この機能では、マスター コントローラ（MC）からネットワークのデータ コレクタにデータをエクスポートするので、パフォーマンス ルーティングがネットワークでどのように機能しているかをより簡単に確認できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR Data Export v1.0 NetFlow v9 フォーマットの詳細

NetFlow バージョン 9 データ エクスポート フォーマット

NetFlow バージョン 9 は、ネットワーク ノードからコレクタに NetFlow レコードを送信するための柔軟で拡張性のある手段です。 NetFlow バージョン 9 には定義可能なレコード タイプが用意されています。また、自己記述型で、NetFlow Collection Engine の設定を容易にします。

NetFlow バージョン 9 エクスポートでは、新しいフィールドを設定された間隔で NetFlow Collection Engine（以前の NetFlow コレクタ）に送信できます。 必要な機能をイネーブルにすると、それらの機能に対応するフィールド値が NetFlow Collection Engine に送信されます。

PfR Data Export v1.0 NetFlow v9 フォーマット機能の利点

PfR Data Export v1.0 NetFlow v9 フォーマット機能では、マスター コントローラ（MC）からネットワークのデータ コレクタにデータをエクスポートするので、パフォーマンス ルーティングがネットワークでどのように機能しているかをより簡単に確認できます。

NetFlow Collection Engine を提供したり、NetFlow のサービスを表示したりするアプリケーションを製造するシスコのお客様は、新規の NetFlow テクノロジーが追加されるたびにアプリケーションを再コンパイルする必要はありません。 代わりに、シスコのお客様は、PfR Data Export v1.0 NetFlow v9 フォーマット機能を利用することで、既知のフィールド タイプを文書化する外部のデータ ファイルを使用できます。

PfR Data Export v1.0 NetFlow v9 フォーマット機能をイネーブルにする方法

PfR Data Export v1.0 NetFlow v9 フォーマット機能のイネーブル化

PfR Data Export v1.0 NetFlow v9 フォーマット機能をイネーブルにするには、PfR マスター コントローラで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** *ip-address*
5. **export-protocol netflow-v9**
6. **transport udp** *udp-port*
7. **exit**
8. **pfr master**
9. **exporter** *exporter-name*
10. **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。 • パスワードを入力します（要求された場合）。
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	**flow exporter** *exporter-name* 例： `Router(config)# flow exporter pfr_exp`	Flexible NetFlow フロー エクスポータを作成し、Flexible NetFlow フロー エクスポータ 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	**destination** *ip-address* 例： `Router(config-flow-exporter)# destination 192.168.2.0`	エクスポート先を設定します。
ステップ 5	**export-protocol netflow-v9** 例： `Router(config-flow-exporter)# export-protocol netflow-v9`	エクスポート プロトコルとして NetFlow バージョン 9 を設定します。

	コマンドまたはアクション	目的
ステップ 6	**transport udp** *udp-port* 例： `Router(config-flow-exporter)# transport udp 2000`	トランスポート プロトコルを設定します。
ステップ 7	**exit** 例： `Router(config-flow-exporter)# 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 8	**pfr master** 例： `Router(config)# pfr master`	Cisco IOS パフォーマンス ルーティング（PfR）プロセスをイネーブルにして、ルータを PfR マスター コントローラとして設定し、PfR マスター コントローラ コンフィギュレーション モードを開始します。
ステップ 9	**exporter** *exporter-name* 例： `Router(config-pfr-mc)# exporter pfr_exp`	フロー エクスポータを設定します。
ステップ 10	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR Data Export v1.0 NetFlow v9 フォーマット設定の確認

PfR Data Export v1.0 NetFlow v9 フォーマット設定を確認し、データが想定どおりにマスター コントローラにエクスポートされていることを確認するには、PfR マスター コントローラで次の手順を実行します。

手順の概要

1. **enable**
2. **show pfr master export statistics**
3. **show pfr master traffic-class**
4. **exit**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show pfr master export statistics** 例： `Router# show pfr master export statistics`	PfR NetFlow バージョン 9 エクスポート統計情報を表示します。 • 表示をクリアするには、**clear pfr master export statistics** コマンドを使用します。
ステップ 3	**show pfr master traffic-class** 例： `Router# show pfr master traffic-class`	PfR マスター コントローラで監視および制御されるすべてのトラフィック クラスに関する情報を表示します。
ステップ 4	**exit** 例： `Router# exit`	特権 EXEC コンフィギュレーション モードを終了します。

PfR Data Export v1.0 NetFlow v9 フォーマット機能の設定例

PfR Data Export v1.0 NetFlow v9 フォーマット機能のイネーブル化の例

次に、PfR Data Export v1.0 NetFlow v9 フォーマット機能をイネーブルにする例を示します。

```
Router> enable
Router> configure terminal
Router(config)# flow exporter pfr_exp
Router(config-flow-exporter)# destination 192.168.2.0
Router(config-flow-exporter)# export-protocol netflow-v9
Router(config-flow-exporter)# transport udp 2000
Router(config-flow-exporter)# exit
Router(config)# pfr master
Router(config-pfr-mc)# exporter pfr_exp
Router(config-pfr-mc)#
```

次に、PfR Data Export v1.0 NetFlow v9 フォーマット機能がイネーブルの場合の **show pfr master export statistics** コマンドの出力例を示します。

```
Router# show pfr master export statistics

PfR NetFlow Version 9 Export: Enabled

   Destination IP:     10.0.0.1
   Destination port:   2000
   Packet #:           0

  Type of Export:      Total
  -------------------- ------
  TC Config            0
  External Config      0
  Internal Config      0
  Policy Config        7
  Reason Config        100
  Passive Update       0
  Passive Performance  0
  Active Update        0
  Active Performance   0
  External Update      0
  Internal Update      0
  TC Event             0
  Cost                 0
  BR Alert             0
  MC Alert             0
  -------------------- ------
  Total:               107
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command 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』
ベーシック PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
NetFlow および NetFlow データ エクスポート	「*Configuring NetFlow and NetFlow Data Export*」
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

RFC

RFC	タイトル
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR Data Export v1.0 NetFlow v9 フォーマットの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *9*：***PfR Data Export v1.0 NetFlow v9*** フォーマットの機能情報

機能名	リリース	機能情報
PfR Data Export v1.0 NetFlow v9 フォーマット	Cisco IOS XE Release 3.4S	PfR Data Export v1.0 NetFlow v9 フォーマット機能により、RFC 3954 でサポートされている NetFlow v9 標準プロトコルとフォーマットを使用してリアルタイム PfR パフォーマンスデータのエクスポートを簡素化できます。 PfR Data Export v1.0 NetFlow v9 フォーマット機能では、通常の時間ベースのデータと、PfR ルート ポリシー制御イベント データの両方をエクスポートできます。 PfR Data Export v1.0 NetFlow v9 フォーマット機能では、マスター コントローラ（MC）からデータ コレクタにパフォーマンス データをエクスポートするので、PfR がどのように機能しているかをより簡単に確認できます。 この機能により、次のコマンドが導入されました。**clear pfr master export statistics**、 **debug pfr master export passive**、 **debug pfr master export active**、 **debug pfr master export link**、 **debug pfr master export traffic-class**、 **debug pfr master export cost-minimization**、 **debug pfr master export border**、 **debug pfr master export option**、 **debug pfr master export process**、 **debug pfr master export config**、 **debug pfr master export**、 **exporter**（**PfR**）、 および **show pfr master export statistics**。

第 8 章

パフォーマンス ルーティングの mGRE DMVPNハブアンドスポークサポートを使用した EIGRP ルートの制御

PfR EIGRP mGRE DMVPN ハブアンドスポーク サポート機能によって、ルートを拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）ルーティング テーブルに追加し、パフォーマンス ルーティング（PfR）でEIGRPルートを介してプレフィックスおよびアプリケーションを制御できるようになっています。 この機能では、マルチポイント総称ルーティング カプセル化（mGRE）Dynamic Multipoint Virtual Private Network（DMVPN）のハブアンドスポーク ネットワーク設計に従った展開もサポートされます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR を使用した EIGRP ルートの制御の前提条件

この機能は、EIGRP がすでにネットワークで設定されていること、および PfR の基本機能も設定されていることを前提とします。

PfR を使用した EIGRP ルートの制御の制約事項

- 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。 EIGRP をネットワークの mGRE DMVPN トポロジに導入する場合は、ハブ アンド スポーク ネットワーク設計に準拠している必要があります。
- PfR は、DMVPN マルチポイント GRE（mGRE）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 を使用した EIGRP ルートの制御の概要

PfR EIGRP ルート制御

PfR EIGRP mGRE DMVPN ハブアンドスポーク サポート機能により、PfR で EIGRP ルートを制御できるようになっています。 この機能がイネーブルの場合、既存の BGP およびスタティック ルート データベースのほか、EIGRP データベースで、PfR プレフィックスおよびルートを制御する親ルート チェックが実行されます。

PfR では、プレフィックスのパスの最適化だけが行われます。ルーティング プロトコルには完全一致ルートと、それよりも一致度が低いルート（親ルートとも呼ばれます）があります。 PfR によって制御されるのは、親ルートと完全一致するルートまたは一致度が高いルートです。 たとえば、PfR で 10.1.1.0/24 を制御するとき、EIGRP ルーティング テーブルに存在するルートが 10.1.0.0/16 だけの場合、親ルートは 10.1.0.0/16 となり、PfR は 10.1.1.0/24 を EIGRP ルーティング テーブルに追加します。

完全一致の親ルートが EIGRP ルーティング テーブルで見つかった場合、PfR はメトリックに影響を与え、マスター コントローラが選択した出口にルートを設定しようとします。 完全一致の親ルートが見つからなかった場合、PfR は親の属性に一致する新しいルートを EIGRP テーブルに追加します。 そのルートが EIGRP テーブルに正常に設定されると、PfR はその EIGRP の親を保存

し、親ルートへの更新をすべて登録します。 親ルートが削除されると、PfR はこの親ルートに基づいて EIGRP テーブルに追加したすべてのルートを制御しなくなります。

PfR は、制御しているプレフィックスのトラフィック パフォーマンスを、NetFlow を使用してパッシブに、または IP SLA プローブを使用してアクティブに監視します。 遅延、損失、到達可能性などのパフォーマンス統計情報が収集され、プレフィックスに設定された一連のポリシーと比較されます。 トラフィックのパフォーマンスがポリシーに従っていない場合、そのプレフィックスはポリシー違反（OOP）と呼ばれます。 プレフィックスが OOP の状態になった場合、PfR は代替パスを検索します。

BGP とスタティック ルートの両方の制御がデフォルトでイネーブルになっている場合は、EIGRP ルート制御を設定する必要があります。 PfR は常に、最初に BGP を使用してプレフィックスを制御しようとします。 BGP ルート制御が失敗すると、スタティック ルート制御が試行されます。 EIGRP ルート制御がイネーブルな場合、PfR は最初に BGP を使用してプレフィックスを制御しようとします。 親ルートが見つからない場合、EIGRP ルート制御が試行されます。 EIGRP ルート制御が失敗すると、スタティック ルート制御が試行されます。

プレフィックスの代替パスを検索するため、PfR は境界ルータにあるすべての外部インターフェイスから送信先プレフィックス ネットワークの一連のホストに、アクティブ プローブを送信します。 外部インターフェイスでアクティブ プローブが送信される前に、ルーティング プロトコル テーブルで親ルートが検索されます。 PfR EIGRP mGRE DMVPN ハブアンドスポーク サポート機能がイネーブルの場合、PfR は BGP およびスタティック ルーティング テーブルのほか、EIGRP ルーティング テーブルでも、親ルートをチェックしてから外部インターフェイスでアクティブ プローブを送信します。 EIGRP ルーティング テーブルに親ルートを持つすべての外部インターフェイスで、アクティブ プローブが開始されます。 プローブのアクティビティが完了してタイマーの期限が切れると、境界ルータからマスター コントローラへ統計情報が送信され、ポリシーの決定と最適な出口の選択が行われます。

出口が選択されると、その出口を持った境界ルータにプレフィックス制御コマンドが送信され、ルートのインストールまたは変更用プロトコルとして EIGRP が指定されます。 境界ルータはコマンドを受信すると、EIGRP テーブルをチェックして親ルートを検索します。 親ルートが見つかった場合は、PfR が EIGRP テーブルでルートをインストールまたは変更し、ルート制御の状態をマスター コントローラに通知します。

EIGRP ルートが正常にインストールされてドメインにアドバタイズされた場合、PfR はこのプレフィックスのトラフィック パフォーマンスを引き続き監視し、プレフィックスが OOP になった場合は前述したアクションを実行します。

PfR 制御モードの詳細と、BGP、スタティック ルート、ポリシーベース ルーティング、Protocol Independent Route Optimization（PIRO）などのその他の PfR 出口リンクの選択制御の詳細については、「パフォーマンス ルーティングの理解」モジュールおよび「パフォーマンス ルーティング：Protocol Independent Route Optimization（PIRO）」モジュールを参照してください。

PfR および mGRE Dynamic Multipoint VPN

パフォーマンス ルーティングは、Dynamic Multipoint VPN（DMVPN）トポロジの mGRE インターフェイスでサポートされています。 DMVPN により、IPsec 暗号化 VPN ネットワークのゼロタッチ導入が可能になります。 通常の DMVPN 導入では、EIGRP ネットワークが使用されます。PfR

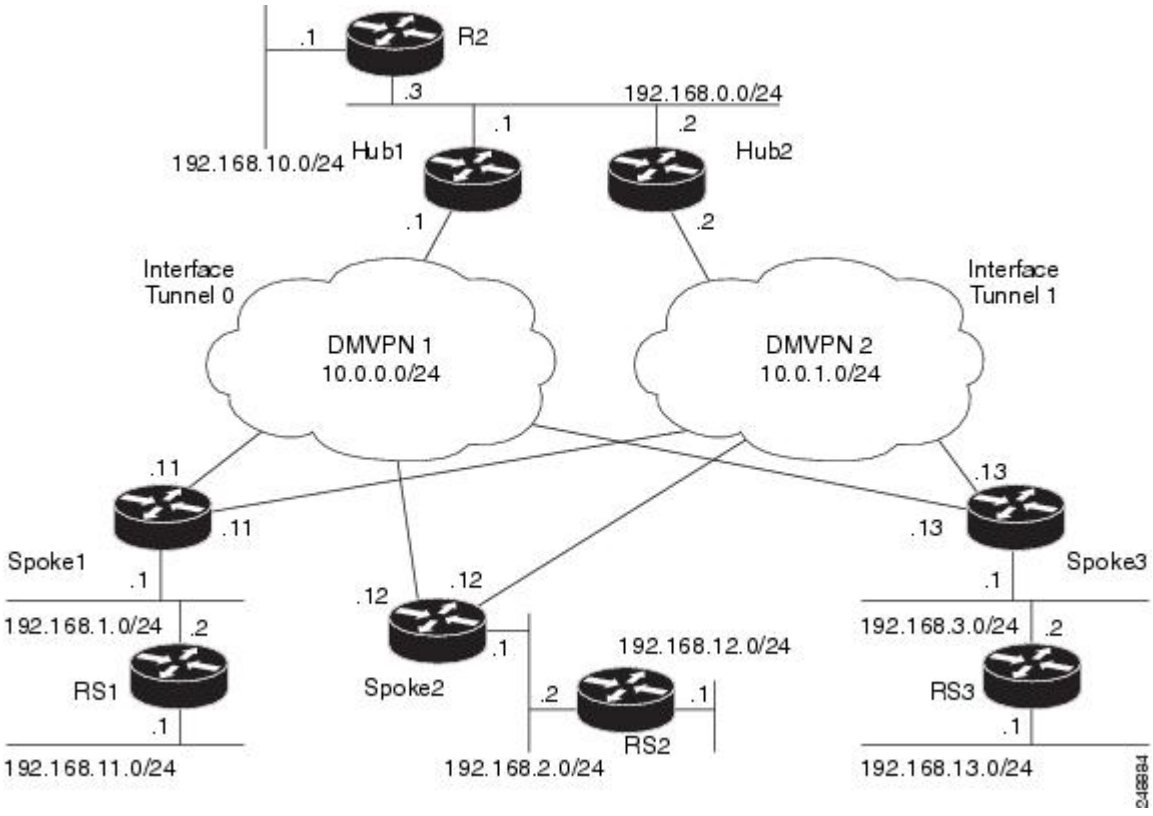
により、DMVPN ネットワーク導入において、DMVPN ネットワーク内で EIGRP ルートを制御できるようになりました。 PfR EIGRP ルート制御の実装では、ハブツースポークのネットワーク設計だけがサポートされます。

DMVPN トポロジにおいて、mGRE インターフェイスは、1 対多のインターフェイスとして機能し、接続された各ブランチのダイナミック作成を可能にします。

下の図は、一般的なデュアル DMVPN トポロジを示しています。 この図では、本社（R2）に、DMVPN ネットワーク（DMVPN 1 または DMVPN 2）あるいは MPLS-GETVPN ネットワークのいずれかを使用してリモート サイト スポークに接続されるハブ（hub1）が 1 つあります。

リモート サイト 1（RS1）には、DMVPN1 および DMVPN2 ネットワークを使用してハブに接続されるスポーク 1 および 2 があります。 リモート サイト 2（RS2）には、スポーク 3 があり、DMVPN1 ネットワークだけを使用してハブに接続されます。 つまり、RS2 には冗長性がなく、パフォーマンス最適化は、ハブと RS2 間だけで実行されます。 リモート サイト 3（RS3）には、DMVPN2 ネットワークおよび MPLS-GETVPN ネットワークを使用してハブに接続されるスポーク 3 があります。

図 *12*：*PfR* デュアル *DMVPN* トポロジ



PfR がネットワークで設定されている場合、システムは次の機能を実行できます。

- mGRE インターフェイスで PfR トラフィック クラスのパフォーマンスを制御および測定する。

- PfR外部インターフェイスとして設定されるマルチポイントインターフェイス上のトラフィックでロードバランシングを実行する。 たとえば、2つのDMVPNクラウドを使用するトポロジでは、PfRは、ネットワーク パフォーマンスが維持されるように、2つのトンネル インターフェイス間のトラフィックでロード バランスを実行するように設定できます。
- マルチポイント インターフェイス間におけるトラフィックで再ルーティングを行って、パフォーマンスを改善する。 たとえば、スポークへの最適なパス、およびスポークからハブへの最適なパスを選択するように、PfR ポリシーを設定できます。
- プライマリ接続が失敗した場合にバックアップ接続を提供する。 たとえば、1つのMPLS-GETVPNおよび1つのDMVPN接続を使用するトポロジでは、MPLS-GETVPNクラウドはプライマリ接続として機能し、プライマリ接続が失敗した場合にDMVPN接続を使用するようにPfRクラウドを設定できます。

DMVPN トポロジは、ハブツースポーク機能には、マルチポイント GRE（mGRE）のようなプロトコルを使用し、スポークツースポーク機能には、Next Hop Resolution Protocol（NHRP）を使用します。 mGRE DMVPN ネットワークの設定の詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Dynamic Multipoint VPN」モジュールを参照してください。 DMVPN の一般的な情報については、http://www.cisco.com/go/dmvpn を参照してください。

PfR で EIGRP ルート制御を設定する方法

PfR EIGRP ルート制御のイネーブル化とコミュニティ値の設定

EIGRP ルート制御をイネーブルにするには、マスター コントローラで次のタスクを実行します。 BGP とスタティック ルートの制御はいずれもデフォルトでイネーブルになっていますが、EIGRP ルート制御はコマンドライン インターフェイス（CLI）コマンド、**mode route metric eigrp** を使用してイネーブルにする必要があります。 PfR は常に、最初に BGP を使用してプレフィックスを制御しようとします。 BGP ルート制御が失敗すると、スタティック ルート制御が試行されます。 EIGRP ルート制御がイネーブルな場合、PfR は最初に BGP を使用してプレフィックスを制御しようとします。 親ルートが見つからない場合、EIGRP ルート制御が試行されます。 EIGRP ルート制御が失敗すると、スタティック ルート制御が試行されます。

このタスクでは、追加された EIGRP ルートに対して、そのルートを一意に識別できる拡張コミュニティ値も設定できます。 EIGRPルートは、トラフィック クラスによって定義されるトラフィックがポリシー違反（OOP）になったときに、そのトラフィックを制御するために PfR によって挿入されることがあります。 次のタスクでは、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 **mode route control** コマンドにより PfR ルート制御モードがグローバルに設定され、挿入される EIGRP ルートは 700 の値でタグ付けされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode route control**
5. **mode route metric eigrp tag** *community*
6. **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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**mode route control** 例： `Router(config-pfr-mc)# mode route control`	マスター コントローラで PfR ルート制御モードを設定します。 • **route** および **control** キーワードにより、ルート制御モードがイネーブルになります。制御モードでは、マスター コントローラが監視対象トラフィック クラスを分析し、ポリシー パラメータに基づいて変更を実行します。
ステップ 5	**mode route metric eigrp tag** *community* 例： `Router(config-pfr-mc)# mode route metric eigrp tag 7000`	EIGRP ルート制御をイネーブルにして、追加された EIGRP ルートの EIGRP タグとコミュニティ番号値を設定します。 • **tag** キーワードを使用して、PfR が制御する EIGRP ルートにタグを適用します。 *community* 引数は 1 ～ 65535 の数字です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR EIGRP ルート制御のディセーブル化

（注） このタスクが完了すると、EIGRP プロトコルを使用して制御されるすべてのルートが PfR で削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **no mode route metric eigrp**
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。 • パスワードを入力します（要求された場合）。
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	**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、マスターコントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 4	**no mode route metric eigrp** 例： `Router(config-pfr-mc)# no mode route metric eigrp`	EIGRP ルート制御をディセーブルにして、EIGRP プロトコルを使用して制御されるすべてのルートを削除します。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR による EIGRP 制御ルートの手動確認

PfR は、NetFlow 出力を使用して、ネットワーク内のルート制御を自動的に確認します。 PfR は NetFlow メッセージを監視し、メッセージでルート制御変更を確認できない場合は、トラフィック クラスを制御しません。 PfR 制御フェーズで実行されたトラフィック制御が実際にトラフィック フローを変更し、OOPイベントをポリシー準拠に変更したことを手動で確認する場合は、この任意のタスクのステップを実行します。

このタスクのすべてのステップは任意ですが、順番は任意ではありません。 これらのステップから得られる情報では、トラフィック クラスに関連付けられた特定のプレフィックスが、別の出口リンク インターフェイスまたは入口リンク インターフェイスに移動されたか、または PfR によって制御されているかを確認できます。 最初の 2 つのコマンドは、マスター コントローラで入力します。最後の 2 つのコマンドは、境界ルータで入力します。

このタスクで使用されている **show** コマンドの一部については、部分的なコマンド構文だけを示しています。 PfR **show** コマンドの詳細については、『*Cisco IOS Performance Routing Command Reference*』を参照してください。

はじめる前に

このタスクは、PfR を使用した EIGRP ルート制御をイネーブルにしていることを前提条件とします。

手順の概要

1. **enable**
2. **show pfr master prefix** *prefix* [**detail**]
3. 境界ルータに移動して、次のステップを開始します。
4. **enable**
5. **show pfr border routes eigrp** [**parent**]

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr master prefix** *prefix* [**detail**]
このコマンドは、監視対象プレフィックスの状態を表示するために使用します。 このコマンドからの出力には、送信元境界ルータ、現在の出口インターフェイス、プロトコル、プレフィックス遅延、出口インターフェイスの帯域幅、および入口インターフェイスの帯域幅に関する情報が含まれています。 この例では、プレフィックス 10.1.0.0/16 のプロトコルは EIGRP です。つまり、トラフィック クラスの親ルートが EIGRP ルーティング テーブルに存在し、EIGRP のコミュニティ値がプレフィックスの制御に使用されています。 このステップでは、次のタスクに関連する構文だけを示します。

例：

```
Router# show pfr master prefix 10.1.0.0

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
Prefix                  State     Time Curr BR         CurrI/F         Protocol
                     PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                     ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                     ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.0.0/16          DEFAULT*      @69 10.1.1.1        Gi1/22          EIGRP
                           U        U        0        0        0        0
                           U        U        0        0       22        8
                           N        N
```

ステップ 3 境界ルータに移動して、次のステップを開始します。
次のコマンドは、マスター コントローラではなく、境界ルータで入力します。

例：

ステップ 4 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 5 **show pfr border routes eigrp** [**parent**]

このコマンドは、境界ルータで入力します。 境界ルータ上の PfR 制御 EIGRP ルートに関する情報を表示するには、このコマンドを使用します。 この例の出力では、PfR によって制御される 10.1.2.0/24 プレフィックスが示されます。 このコマンドは、EIGRP ルーティング テーブルで親ルートが特定された場合に、親ルートの検索と既存の親ルートへのルート変更を表示するときに使用されます。

例：

```
Router# show pfr border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact
Flags Network            Parent             Tag
CE    10.1.2.0/24        10.0.0.0/8         5000
```

この例では、**parent** キーワードが使用されていて、親ルートの検索に関する詳細情報が表示されます。

例：

```
Router# show pfr border routes eigrp parent

Network            Gateway            Intf       Flags
10.0.0.0/8         10.40.40.2         Gi0/0/2    1
Child Networks
Network            Flag
10.1.2.0/24        6
```

トラブルシューティングのヒント

show コマンドの出力に、EIGRP ルート制御を確認する内容が示されなかった場合は、**debug pfr border routes eigrp** コマンドをオプションの **detail** キーワードとともに使用すると詳細を確認できます。 必要なコマンドを入力する前にデバッグをイネーブルにする必要があります。また、デバッグ出力は、続いて入力するコマンドによって異なります。

PfR を使用した EIGRP ルートの制御の設定例

PfR EIGRP ルート制御のイネーブル化とコミュニティ値の設定例

次の設定例では、最初に PfR ルート制御をイネーブルにし、次に EIGRP ルート制御をイネーブルにして、追加された EIGRP ルートに拡張コミュニティ値 700 を設定しています。

```
pfr master
 mode route control
 mode route metric eigrp tag 700
 end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR を使用した EIGRP ルートの制御の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *10*：*PfR* を使用した *EIGRP* ルートの制御の機能情報

機能名	リリース	機能情報
PfR EIGRP mGRE DMVPN ハブアンドスポーク サポート	Cisco IOS XE Release 3.3S	PfR EIGRP 機能では、EIGRP データベースで親ルートチェックを行うことにより、EIGRP に基づいて PfR ルートを制御できます。 また、ハブツースポーク ネットワーク設計に準拠する mGRE Dynamic Multipoint VPN（DMVPN）導入のサポートも追加します。 この機能により、次のコマンドが導入または変更されました。**debug pfr border routes**、**mode（PfR）**、**show pfr border routes**、および **show pfr master prefix**。

第 9 章

パフォーマンスルーティングリンクグループ

パフォーマンスルーティング-リンクグループ機能は、出口リンクのグループを優先リンクセットとして、またはパフォーマンス ルーティング（PfR）用フォールバック リンク セットとして定義し、PfRポリシーで指定されたトラフィック クラスを最適化する際に使用できる機能を導入しました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンス ルーティング リンク グループの概要

パフォーマンス ルーティング リンク グループ

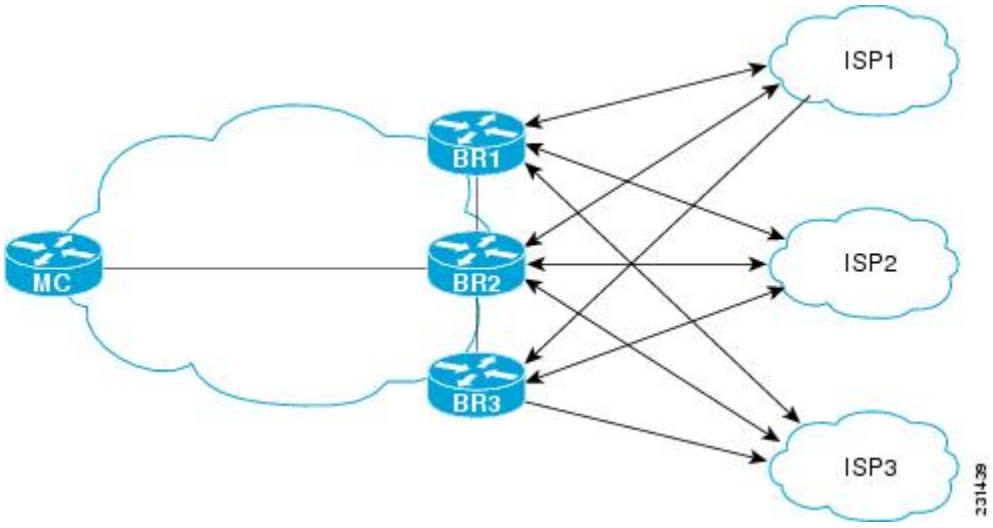
パフォーマンス ルーティング リンク グループ機能は、出口リンクのグループを優先リンク セットとして、またはPfR用フォールバック リンク セットとして定義し、PfRポリシーで指定されたトラフィック クラスを最適化する際に使用できる機能を導入しました。 現在PfRは、ポリシーで指定されたプリファレンスと、指定リンク外のパスでのトラフィック クラスのパフォーマンス（到達可能性、遅延、損失、ジッター、MOSなどのパラメータを使用）に基づいて、トラフィック クラスに最良のリンクを選択しています。最良リンクの選択では、帯域幅の使用率、コスト、リンクの範囲を考慮することもできます。 リンクのグループ化に使用される手法では、1つ以上のトラフィック クラスに対する優先リンクをPfRポリシーで指定し、プライマリ リンク グループと呼ばれる優先リンクのリストにある最良リンクを介してトラフィック クラスがルーティングされるようにします。プライマリ グループに所定のポリシーとパフォーマンス要件を満たすリンクがない場合は、フォールバック リンク グループを指定することもできます。プライマリ グループ リンクを使用できない場合、トラフィック クラスはフォールバック グループ内の最良リンクを介してルーティングされます。 最良のリンクを特定するために、PfRはプライマリ グループとフォールバック グループの両方をプローブします。

プライマリおよびフォールバック リンク グループは、マスター コントローラで設定でき、一意な名前で識別されます。 リンク グループでは、PfRポリシーで最良のリンクが高帯域幅リンクだけで構成されるリンク グループから選択されるように設定することで、たとえば、ビデオ トラフィックで使用される高帯域幅リンクなど、リンクをグループ化できます。 ポリシーで指定されるトラフィック クラスは、プライマリ リンク グループ1つ、フォールバック リンク グループ1つだけで設定できます。リンク グループの優先順位は、ポリシーにより異なるので、同じリンク グループが、ポリシーによっては、プライマリ リンク グループになったり、フォールバック リンク グループになったりすることがあります。

リンクのグループ化を実装する方法の例については、次の図を参照してください。 3つのリンク グループ、ISP1、ISP2およびISP3は、異なるインターネット サービス プロバイダー（ISP）を表しています。これら3つのISPにはすべて、次の図に示されている3つの境界ルータのインターフェイスのリンクがあります。ISP1リンクは、最もコストがかかるリンクですが、サービス レベル契約（SLA）保証は最高です。ISP3リンクは、ベストエフォート型リンクで、最もコストが低いリンクです。 ISP2リンクは、ISP1リンクほどは優れていませんが、ISP3リンクよりは信頼できます。 ISP2リンクのコストは、ISP3リンクよりは高く、ISP1リンクより低いです。 この状況

で、各 ISP は、リンク グループとして作成され、次の図に示されている各境界ルータのインターフェイスに関連付けられています。

図 *13*：リンク グループの図



ビデオ、ボイス、FTP、データの 4 種類のトラフィック クラスがあるとします。各トラフィック クラスは、適切なリンク グループに属する境界ルータ インターフェイスを介してルーティングできます。 ビデオとボイスのトラフィック クラスでは、最良のリンクが必要であるため、ISP1 リンク グループがプライマリ リンク グループとして、ISP2 がフォールバック グループとして設定されます。 FTP トラフィックでは、信頼できるリンクが必要であり、コスト効率も考慮が必要となる可能性があるので、ISP2 をプライマリ グループとして、ISP3 をフォールバック リンク グループとして割り当てます。 ISP1 は、最も信頼できるリンクを提供しますが、ファイル転送トラフィックとしてコストが高すぎることがあります。 データ トラフィックにおいて、ISP3 はプライマリ リンク グループに、ISP2 はフォールバック グループに適しています。

（注） リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

スピルオーバー

パフォーマンス ルーティング リンク グループを使用して、スピルオーバーをサポートできます。スピルオーバーは次のように機能します。ネットワークを介して同じプロバイダーエッジ（PE）ルータに 2 つのパス（たとえば、トラフィック エンジニアリング（TE）トンネル）があり、これらのトンネルのパスがネットワーク上で異なる場合、トラフィックは、一方のトンネルを介して送信され、トラフィック負荷しきい値に達すると、もう一方のトンネルにスピルオーバーされます。 PfR リンク グループを使用すると、一方のトンネルをプライマリ リンク グループとして作成して、もう一方のトンネルをフォールバック リンク グループにできます。 最初のトンネルが

ポリシー違反になると、PfR はフォールバック トンネル リンク グループに切り替えます。これにより、最初のトンネルのトラフィック負荷がしきい値を下回るまで、スピルオーバー容量が提供されます。 トンネルは、PfR リンク グループが設定される前に確立される必要があります。

パフォーマンス ルーティング リンク グループの設定方法

パフォーマンス ルーティング リンク グループの実装

境界ルータの出口リンクをリンク グループのメンバーとして識別しいくつかのパフォーマンス ルーティング リンク グループを設定して、PfR マップを作成して PfR ポリシーで定義されるトラフィック クラスのリンク グループを指定するには、マスター コントローラでこのタスクを実行します。 このタスクでは、リンク グループは、ビデオ トラフィックに設定されます。高帯域幅の出口リンクのセットは、プライマリ リンク グループとして識別されるビデオ リンク グループのメンバーとして識別されます。 フォールバック リンク グループも指定されます。

PfR ポリシーは、PfR マップを使用して作成されます。ここで、プライマリおよびフォール リンク グループが、PfR マップ条件と一致するトラフィック クラスに指定されます。 PfR は、プライマリとフォールバックの両方のグループ リンクをプローブし、プライマリ リンク グループから、このタスクで指定されるトラフィック クラスに最良のリンクを選択します。 ポリシー内でプライマリ リンクがない場合、PfR は、フォールバック グループから最良のリンクを選択します。 リンクのグループ化の詳細については、「パフォーマンス ルーティング リンク グループ」の項を参照してください。

（注） リンクのグループ化を設定している場合、リンク使用率範囲は、リンクのグループ化に対して設定された出口リンクの優先セットまたはフォールバック セットと両立できないので、**no max-range-utilization** コマンドを設定します。 CSCtr33991 では、この要件は削除され、PfR は PfR リンク グループ内でロード バランシングを実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **link-group** *link-group-name* [*link-group-name* [*link-group-name*]]
7. **exit**
8. 適切な変更を加えてステップ 5 ～ 7 を繰り返し、すべての外部インターフェイスにリンク グループを設定します。
9. **interface** *type number* **internal**
10. **exit**
11. **ip access-list** {**standard** | **extended**} *access-list-name*
12. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
13. 必要に応じて、追加のアクセス リスト エントリについてステップ 12 を繰り返します。
14. **exit**
15. **pfr-map** *map-name sequence-number*
16. **match traffic-class access-list** *access-list-name*
17. **set link-group** *link-group-name* [**fallback** *link-group-name*]
18. **end**
19. **show pfr master link-group** [*link-group-name*]

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。 • パスワードを入力します（要求された場合）。
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	**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境界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

	コマンドまたはアクション	目的
		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 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Router(config-pfr-mc)# border 192.168.1.2 key-chain border1_PFR`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界ルータを識別するために、IP アドレスを設定します。 • PfR の管理対象ネットワークを作成するには、少なくとも 1 台の境界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境界ルータは、最大 10 台です。 • *key-chain-name* 引数の値は、境界ルータの設定時に指定されたキーチェーン名と一致する必要があります。 （注） 境界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、既存の境界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 5	**interface** *type number* **external** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	PfR 管理の外部インターフェイスとして境界ルータ インターフェイスを設定します。 • 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 つの外部境界ルータ インターフェイスが必要です。 各境界ルータでは、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。

	コマンドまたはアクション	目的
ステップ 6	**link-group** *link-group-name* [*link-group-name* [*link-group-name*]] 例： `Router(config-pfr-mc-br-if)# link-group VIDEO`	PfR 境界ルータ出口インターフェイスをリンク グループのメンバーとして設定します。 • インターフェイスのリンク グループ名を指定するには、*link-group-name* を使用します。 • 各インターフェイスには最高 3 つのリンク グループを指定できます。 • この例では、ギガビットイーサネット 0/0/0 外部インターフェイスが、VIDEO という名前のリンク グループのメンバーとして設定されます。 （注） **link-group**（PfR）コマンドは、リンク グループとインターフェイスを関連付けます。 ステップ 17 では、**set link-group**（PfR）コマンドを使用して、PfR マップで定義されているトラフィック クラスのプライマリまたはフォールバック グループとしてリンク グループを識別します。
ステップ 7	**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 管理境界ルータ コンフィギュレーション モードに戻ります。
ステップ 8	適切な変更を加えてステップ 5 ～ 7 を繰り返し、すべての外部インターフェイスにリンク グループを設定します。	--
ステップ 9	**interface** *type number* **internal** 例： `Router(config-pfr-mc-br)# interface GigabitEthernet 0/0/1 internal`	境界ルータ 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。 • 各境界ルータでは、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 10	**exit** 例： `Router(config-pfr-mc-br)# exit`	PfR 管理ボーダー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**ip access-list** {**standard** | **extended**} *access-list-name* 例： `Router(config)# ip access-list extended ACCESS_VIDEO`	IP アクセス リストを名前で定義し、拡張名前付きアクセス リスト コンフィギュレーション モードを開始します。 • PfR は、名前付きアクセス リストだけをサポートします。 • 例では、ACCESS_VIDEO という名前の拡張 IP アクセス リストが作成されます。
ステップ 12	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] 例： `Router(config-ext-nacl)# permit tcp any any 500`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • 例では、任意の宛先または送信元から、および宛先ポート番号 500 からのすべての伝送制御プロトコル（TCP）トラフィックを識別するように設定されます。 この特定の TCP トラフィックが最適化されます。
ステップ 13	必要に応じて、追加のアクセス リスト エントリについてステップ 12 を繰り返します。	--
ステップ 14	**exit** 例： `Router(config-ext-nacl)# exit`	（任意）拡張名前付きアクセス リスト 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 15	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map VIDEO_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • permit シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 16 で **match ip address**（PfR）コマンドを使用して適用します。 • 例では、VIDEO_MAP という名前の PfR マップが作成されます。
ステップ 16	**match traffic-class access-list** *access-list-name* 例： `Router(config-pfr-map)# traffic-class access-list ACCESS_VIDEO`	PfR マップを使用して、トラフィック クラスの作成に使用される一致基準として、アクセス リストを手動で設定します。 • 各アクセス リスト エントリには、送信先プレフィックスが含まれている必要があります。また、他の省略可能なパラメータを含むこともできます。

	コマンドまたはアクション	目的
		• 例では、ACCESS_VIDEO という名前のアクセス リストで定義された条件を使用してトラフィック クラスが定義されます。
ステップ 17	**set link-group** *link-group-name* [**fallback** *link-group-name*] 例： `Router(config-pfr-map)# set link-group video fallback voice`	PfR マップで指定されているトラフィック クラスのリンク グループを指定して、PfR ポリシーを作成します。 • ポリシーのプライマリ リンク グループ名を指定するには、*link-group-name* を使用します。 • ポリシーのフォールバック リンク グループ名を指定するには、**fallback** キーワードを使用します。 • この例では、アクセス リスト ACCESS_VIDEO と一致するトラフィック クラスのプライマリ リンク グループとして VIDEO リンク グループを指定します。リンク グループ VOICE は、フォールバック リンク グループとして指定されます。
ステップ 18	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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 pfr master link-group** [*link-group-name*] 例： `Router# show pfr master link-group`	設定されている PfR リンク グループに関する情報を表示します。 • 指定された PfR リンク グループの情報を表示するには、オプションの *link-group-name* 引数を使用します。 • *link-group-name* 引数を指定しない場合、すべての PfR リンク グループに関する情報が表示されます。 • この例では、設定されているすべてのリンク グループに関する情報を表示します。

例

次に、PfR を使用して設定されるパフォーマンス ルーティング リンク グループに関する情報を表示する **show pfr master link-group** コマンドの出力例を示します。 この例では、VIDEO リンク グループと、設定されている他のリンク グループが示されています。

```
Router# show pfr master link-group

link group video
  Border           Interface       Exit id
  192.168.1.2      Gi0/0/0         1
 link group voice
  Border           Interface       Exit id
```

```
 192.168.1.2      Gi0/0/0         1
 192.168.1.2      Gi0/0/1         2
 192.168.3.2      Gi0/0/3         4
link group data
 Border           Interface       Exit id
 192.168.3.2      Gi0/0/2         3
```

パフォーマンス ルーティング リンク グループの設定例

パフォーマンス ルーティング リンク グループの実装例

次の例に、リンク グループを実装する方法を示します。 この例では、ACCESS_VIDEO という名前のアクセスリストと一致するトラフィック クラスを定義するようにPfRを設定する、VIDEO_MAP という名前の PfR マップが作成されます。 トラフィック クラスは、VIDEO という名前のリンク グループをプライマリ リンク グループとして使用し、VOICE という名前のフォールバック グループを使用するように設定されています。 VIDEO リンク グループには、ビデオ トラフィックに適した高帯域幅リンクのセットが選択されることがあります。

```
enable
configure terminal
border 10.1.4.1
 interface GigabitEthernet 0/0/0 external
  link-group VIDEO
  exit
 interface GigabitEthernet 0/0/2 external
  link-group VOICE
  exit
 interface GigabitEthernet 0/0/1 internal
 exit
ip access-list extended ACCESS_VIDEO
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800 any any dscp ef
 exit
pfr-map VIDEO_MAP 10
 match traffic-class access-list ACCESS_VIDEO
 set link-group VIDEO fallback VOICE
 end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』

関連項目	マニュアル タイトル
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンス ルーティング リンク グループの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *11* : パフォーマンス ルーティング リンク グループの機能情報

機能名	リリース	機能情報
パフォーマンス ルーティング - リンク グループ	Cisco IOS XE Release 3.3S	パフォーマンス ルーティング - リンク グループ機能によって、出口リンクのグループを優先リンク セットとして、またはPfR用フォールバック リンク セットとして定義し、PfRポリシーで指定されたトラフィック クラスを最適化する際に使用できるようになっています。 この機能により、次のコマンドが導入または変更されました。**link-group**（**PfR**）、**set link-group**（**PfR**）、および**show pfr master link-group**。

第 10 章

NAT を使用したパフォーマンス ルーティング

パフォーマンスルーティング（PfR）は、ネットワークアドレス変換（NAT）を使用するネットワークでスタティック ルーティングによりトラフィック クラス ルーティングを制御できるようになりました。また、既存の NAT コマンドに新しいキーワードが追加されました。 PfR および NAT 機能が同じルータで設定されていて、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。 このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネットサービスプロバイダー（ISP）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送（Unicast RPF）フィルタリングを使用する場合に発生します。 NAT に対する PfR サポートの Cisco IOS XE での実装が説明されます。

新しいキーワードが設定されている場合、新しい NAT 変換に、PfR がパケットに選択したインターフェイスのソース IP アドレスが提供され、PfR は、この NAT 変換が作成されたときのインターフェイスを介して、既存のフローを強制的にルーティングします。

（注） Cisco IOS XE Release 3.1S および 3.2S では、境界ルータ専用機能がサポートされます。 また、PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 Optimized Edge Routing（OER）構文を使用して Cisco IOS XE Release 2.6.1 を実行している場合、『Cisco IOS XE Performance Routing Configuration Guide, Release 2』を参照してください。 Cisco IOS XE Release 3.3S 以降のリリースでは、マスター コントローラのサポートが追加されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

NAT を使用するパフォーマンス ルーティングの前提条件

PfR 境界ルータとして使用する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、Cisco IOS XE Release 3.1S 以降のリリースを実行している必要があります。

NAT を使用したパフォーマンス ルーティングの制約事項

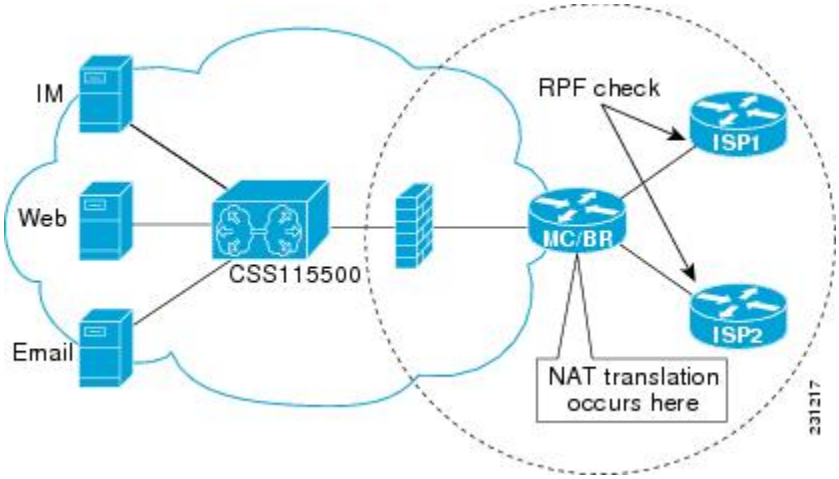
- Cisco IOS XE Release 3.1S 以降のリリースを実行する Cisco ASR 1000 シリーズのアグリゲーション サービス ルータ上では、NAT を使用するネットワーク内で PfR がスタティック ルーティングによってトラフィック クラス ルーティングを制御する機能において、トンネル インターフェイスまたは DMVPN 実装はサポートされません。
- 境界ルータ専用機能は Cisco IOS XE Release 3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 Cisco IOS XE Release 3.1S および 3.2S イメージで境界ルータとして使用されている Cisco ASR 1000 シリーズルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

NAT を使用したパフォーマンス ルーティングの概要

PfR および NAT

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。 このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネット サービス プロバイダー（ISP）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送（Unicast RPF）フィルタリングを使用する場合に発生します。 プライベート IP アドレスからパブリック IP アドレスへの NAT 変換が実行された後で PfR によりトラフィック クラスの発信パケット ルートの出口インターフェイスが変更されると、ユニキャスト RPF を実行する入口ルータでパケットがドロップされます。 パケットが転送されると、入口ルータ（たとえば、ISP ルータ）のユニキャスト RPF フィルタリングは、NAT により割り当てられるソース IP アドレス プールとは異なるソース IP アドレスを示し、パケットがドロップされます。 たとえば、次の図は、NAT を使用した場合の PfR の動作を示しています。

図 *14*：*NAT* を使用した *PfR*



NAT 変換は、内部ネットワークに接続されているルータで発生します。このルータには、境界ルータまたはマスター コントローラと境界ルータの組み合わせを使用できます。 PfR が、ルートを変更してトラフィック クラスパフォーマンスを最適化し、ロードバランシングを実行すると、インターフェイスを介して ISP1 にルーティングされた、上の図の境界ルータからのトラフィックは、トラフィック パフォーマンスが測定され、ポリシーしきい値が適用された後で、インターフェイスを介して ISP2 に再ルーティングされることがあります。 RPF チェックは ISP ルータで発生し、ISP2 を介してルーティングされるパケットは、ISP2 の入口ルータでの RPF チェックに失敗します。これは、送信元インターフェイスの IP アドレスが変更されたためです。

（注） 境界ルータ専用機能は Cisco IOS XE Release 2.6、3.1S および 3.2S イメージに含まれます。マスター コントローラ設定は使用できません。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。 上の図では、ルータは境界ルータです。マスター コントローラと境界ルータの組み合わせではありません。

このソリューションには、**ip nat inside source** コマンドに対して追加された新しい **oer** キーワードを使用した最小限の設定の変更が含まれています。 **oer** キーワードを設定すると、新しい NAT 変換では、パケットに対して PfR が選択したインターフェイスの発信元 IP アドレスが指定され、PfR は NAT 変換が作成されたインターフェイスを介して既存のフローがルーティングされるように強制します。 たとえば、PfR は、上の図で ISP1 の InterfaceA と ISP2 の InterfaceB の 2 つのインターフェイスがある境界ルータでトラフィックを管理するように設定されます。 PfR は、最初に、Web トラフィックを表すトラフィック クラスを制御するように設定されます。このトラフィックの NAT 変換は、InterfaceA に設定されているパケットのソース IP アドレスにすでに存在します。PfR は、トラフィック パフォーマンスを測定して、InterfaceB が現在トラフィック フローに最適な出口であると判断しますが、既存のフローを変更しません。 次に、PfR が E メール トラフィックを表すトラフィック クラスを学習および測定するように設定され、E メール トラフィックが開始されると、NAT 変換が InterfaceB で発生します。 PfR スタティック ルーティング NAT ソリューションは、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。 NAT、および Cisco IOS ソフトウェアを実行しない PIX ファイアウォールなどのデバイスを使用したネットワーク設定はサポートされていません。

ネットワーク アドレス変換（NAT）

NAT では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。 NAT は、ルータ（通常、2 つのネットワークを接続）で機能し、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート（グローバルに一意ではない）アドレスを有効なアドレスに変換します。 NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設定できます。 この機能により、そのアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT は、エンタープライズエッジでも使用され、内部ユーザのインターネットへのアクセスを許可し、メール サーバなど内部デバイスへのインターネット アクセスを許可します。

NAT の詳細については、『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring NAT for IP Address Conservation」の章を参照してください。

内部グローバル アドレスのオーバーロード

ルータで多くのローカル アドレスに 1 つのグローバル アドレスを使用できるようにすることで、内部グローバル アドレス プールのアドレスを節約できます。 このオーバーロードが設定されている場合、ルータは、より高いレベルのプロトコルから十分な情報（たとえば、TCP または UDP

ポート番号）を保持して、グローバル アドレスを正しいローカル アドレスに戻します。 複数のローカル アドレスが 1 つのグローバル アドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカル アドレスが区別されます。

NAT を使用したパフォーマンス ルーティングの設定方法

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定するには、次のタスクを実行します。 このタスクを行うと、内部ユーザによりインターネットへのアクセスを許可しつつ、PfR がトラフィック クラスを最適化できるようになります。

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。 このパケット ドロップは、スタティック ルーティングが同じルータからの複数のインターネット サービス プロバイダー（ISP）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのためにユニキャスト リバース パス転送（Unicast RPF）フィルタリングを使用する場合に発生します。

この作業では、**oer** キーワードを **ip nat inside source** コマンドに使用します。 **oer** キーワードを設定すると、新しい NAT 変換では、パケットに対して PfR が選択したインターフェイスの発信元 IP アドレスが指定され、PfR は NAT 変換が作成されたインターフェイスを介して既存のフローがルーティングされるように強制します。 このタスクでは、1 つの IP アドレスを使用していますが、IP アドレス プールを設定することもできます。 IP アドレス プールの設定例については、設定例に関する項を参照してください。

（注） この設定は、マスター コントローラ上で実施します。 境界ルータ専用機能は Cisco IOS XE Release 3.1S 以降のリリースに含まれます。マスター コントローラ設定は使用できません。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

（注） PfR スタティック ルーティング NAT ソリューションは、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

NAT の詳細については、『 *CiscoIOS IP Addressing Services Configuration Guide*』の「Configuring NAT for IP Address Conservation」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *ip-address*mask
4. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
7. **exit**
8. 必要に応じて、ステップ 4 ～ 7 を繰り返し、その他のルート マップを設定します。
9. **ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**oer**]
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat inside**
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask*
16. **ip nat outside**
17. **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。 • パスワードを入力します（要求された場合）。
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	**access-list** *access-list-number* {**permit**	**deny**} *ip-address*mask 例： `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	変換する IP アドレスを許可する標準のアクセス リストを定義します。 • アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセス リストの最後には暗黙的な「deny all」があるので注意してください）。アクセス リストでアドレスを許可しすぎると、予期しない結果になる可能性があります。

	コマンドまたはアクション	目的
ステップ 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map isp-1 permit 10`	ルート マップ コンフィギュレーション モードを開始して、ルート マップを設定します。 • 例では、BGP という名前のルートマップを作成します。
ステップ 5	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} 例： `Router(config-route-map)# match ip address access-list 1`	NAT により変換されるトラフィックを識別するアクセス リストまたはプレフィックス リスト match 句エントリをルート マップに作成します。 • 例では、ステップ 3 で作成した、一致基準として 10.1.0.0 0.0.255.255 プレフィックスを指定するアクセス リストを参照します。
ステップ 6	**match interface** *interface-type interface-number* [*...interface-type interface-number*] 例： `Router(config-route-map)# match interface GigabitEthernet 0/0/2`	ルート マップに match 句を作成して、指定されたいずれかのインターフェイスに一致するルートを分散します。 • 例では、match 句を作成して、ステップ 5 の match 句をシリアルインターフェイス 1/0 経由で通過するルートを配布します。
ステップ 7	**exit** 例： `Router(config-route-map)# exit`	ルートマップインターフェイス 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	必要に応じて、ステップ 4 ～ 7 を繰り返し、その他のルートマップを設定します。	--
ステップ 9	**ip nat inside source** {**list** {*access-list-number*| *access-list-name*} | **route-map** *map-name*} {**interface** *type number*| **pool** *name*} [**mapping-id** *map-id* | **overload**| **reversible**| **vrf** *vrf-name*][**oer**] 例： `Router(config)# ip nat inside source interface GigabitEthernet 1/0/0 overload oer`	インターフェイスを指定して、オーバーロードでのダイナミックな送信元変換を確立します。 • インターフェイスを指定するには、**interface** キーワードと、type および number 引数を使用します。 • **oer** キーワードを使用し、PfR が NAT を使用して動作し、スタティック ルーティングでトラフィック クラスを制御するようにします。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Router(config)# interface GigabitEthernet 1/0/0`	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 11	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.114.11.8 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat inside** 例： `Router(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**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 モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* 例： `Router(config)# interface GigabitEthernet 1/1/0`	別のインターフェイスを指定して、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 15	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.17.233.208 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 16	**ip nat outside** 例： `Router(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 17	**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。

NAT を使用したパフォーマンス ルーティングの設定例

ネットワーク内で NAT を使用してスタティック ルーティングでトラフィックを制御する PfR の設定例

次に、NAT を使用するネットワークで PfR がスタティック ルーティングによりトラフィックを制御できるようにマスター コントローラを設定する例を示します。 この例では、NAT 変換の IP アドレスのプールを使用する方法を示します。

（注） この設定は、マスター コントローラ上で実施します。 境界ルータ専用機能は Cisco IOS XE Release 3.1S 以降のリリースに含まれます。マスター コントローラ設定は使用できません。 境界ルータとして使用する Cisco ASR 1000 シリーズ ルータと通信するマスター コントローラは、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータでなければなりません。

この例では、境界ルータは 2 つの異なる ISP を介してインターネットに接続されています。 次の設定では、PfR は、内部ユーザのインターネットへのアクセスを許可しつつ、トラフィック クラスを最適化できます。 この例では、NAT を使用して変換されるトラフィック クラスは、アクセス リストおよびルート マップを使用して指定されます。 次に、NAT 変換のための IP アドレス プールの使用を設定し、**oer** キーワードを **ip nat inside source** コマンドに追加し、NAT が変換した発信元アドレスであるインターフェイスを介して通過する既存のトラフィック クラスを PfR が維持するように設定します。 新しい NAT 変換には、PfR がパケットに選択したインターフェイスの IP アドレスを指定できます。

（注） PfR スタティック ルーティング NAT ソリューションは、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

次の例は、Cisco IOS Release 15.0(1)M またはそれ以降の 15.0M リリースを実行するルータに設定できる稼働中のマスター コントローラで設定する必要があります。

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface serial 2/0
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 oer
Router(config)# interface FastEthernet 3/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
```

```
Router(config-if)# exit

Router(config)# interface serial 1/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface serial 2/0
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end
```

次の例は、Cisco IOS XE Release 3.3S 以降のリリースを実行する Cisco ASR 1000 シリーズ ルータで設定できます。

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# route-map isp-2 permit 10BGP permit 10
Router(config-route-map)# match ip address access-list 1
Router(config-route-map)# match interface GigabitEthernet 0/0/2
Router(config-route-map)# exit
Router(config)# ip nat pool ISP2 209.165.201.1 209.165.201.30 prefix-length 27
Router(config)# ip nat inside source route-map isp-2 pool ISP2 oer
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.11.8 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface GigabitEthernet 0/0/2
Router(config-if)# ip address 172.17.233.208 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command 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』
ベーシック PfR 設定	「ベーシック パフォーマンス ルーティングの設定」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	「パフォーマンス ルーティングの理解」モジュール
アドバンスド PfR の設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール

関連項目	マニュアル タイトル
IP SLA の概要	『*IP SLAs Configuration Guide*』
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

NAT を使用したパフォーマンス ルーティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *12* : *NAT* を使用したパフォーマンス ルーティングの機能情報

機能名	リリース	機能情報
NAT およびスタティック ルーティングのサポート[4]	Cisco IOS XE Release 2.6.1、 Cisco IOS XE Release 3.1S、 Cisco IOS XE Release 3.3S	NAT を使用するネットワークでスタティック ルーティングを使用してトラフィック クラス ルーティングを制御するように PfR を許可できます。 この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 PfR 構文は、Cisco IOS XE Release 3.1S で導入されました。 （注） Cisco IOS XE Release 3.3S では、マスターコントローラのサポートが導入されました。 この機能により、次のコマンドが変更されました。**ip nat inside source**。

[4] これはマイナーな拡張です。 マイナーな拡張は、通常 Feature Navigator に記載されません。

第 11 章

NBARCCEアプリケーション認識を使用したパフォーマンス ルーティング

NBAR CCE アプリケーション認識を使用したパフォーマンス ルーティング機能は、ネットワークベース アプリケーション認識（NBAR）を使用してアプリケーションベースのトラフィック クラスをプロファイルできる機能を導入します。 NBARは、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。たとえば、ダイナミック TCP/UDP ポート割り当てを使用する Web ベースや他の分類が困難なアプリケーションとプロトコルなどです。 パフォーマンスルーティング（PfR）ではNBARを利用して、プロトコルまたはアプリケーションを認識し、分類します。分類されたトラフィック クラスは、PfR アプリケーション データベースに追加され、パッシブ モニタリングおよびアクティブ モニタリングの対象となります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

NBAR CCE アプリケーション認識を使用した PfR の前提条件

参加するすべてのデバイスでシスコ エクスプレス フォワーディング（CEF）を有効にする必要があります。その他のスイッチング パスは、ポリシーベース ルーティング（PBR）でサポートされている場合でもサポートされません。

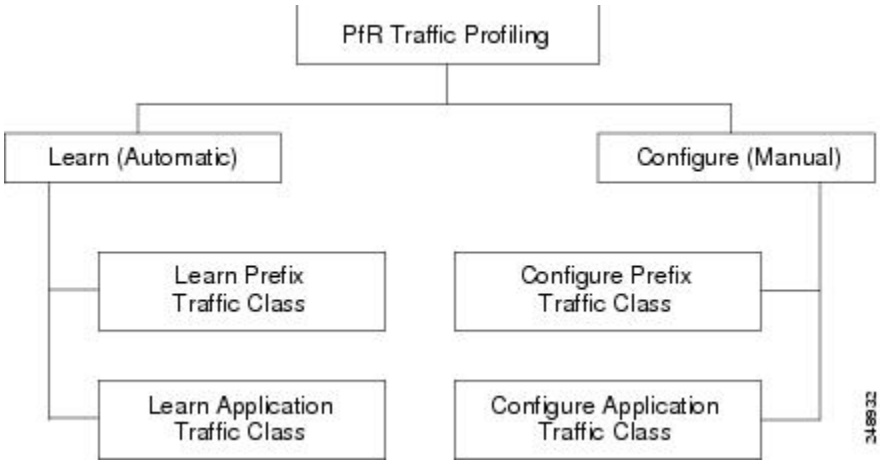
NBAR CCE アプリケーション認識を使用した PfR の概要

パフォーマンス ルーティングのトラフィック クラス プロファイリング

トラフィックを最適化する前に、パフォーマンス ルーティング（PfR）では境界ルータを介したトラフィックからトラフィック クラスを判別する必要があります。 トラフィック ルーティングを最適化するには、全トラフィックのサブセットを識別する必要があります。これらのトラフィック サブセットをトラフィック クラスと呼びます。 トラフィック クラスのエントリのリストには、監視対象トラフィック クラス（MTC）リストという名前が付けられています。 デバイスを経由したトラフィックを自動的に学習するか、トラフィック クラスを手動で設定することによって、MTC リスト内のエントリのプロファイリングを行うことができます。 学習されたトラフィック クラスと設定されたトラフィック クラスの両方が、同時に MTC リストに存在する場合があります。 トラフィック クラスの学習メカニズムと設定メカニズムのいずれも、PfR のプロファイル

フェーズで実装されます。 PfR トラフィック クラスのプロファイリング プロセスの全体構造とコンポーネントは次の図で確認できます。

図 *15* : *PfR* トラフィック クラスのプロファイリング プロセス



PfR では、トラフィック クラスを自動的に学習しながら、組み込みの NetFlow 機能を使用して境界ルータを経由したトラフィックを監視できます。 目的はトラフィックのサブセットを最適化することですが、このトラフィックの正確なパラメータをすべて把握できるわけではないので、PfR にはトラフィックを自動的に学習し、MTC リストに入力することによってトラフィック クラスを作成する方法が用意されています。 トラフィック クラスの自動学習プロセスには、次の 3 つのコンポーネントがあります。

- プレフィックスベースのトラフィック クラスの自動学習
- アプリケーションベースのトラフィック クラスの自動学習
- 学習リストを使用した、プレフィックスベースとアプリケーションベースの両トラフィック クラスの分類

モニタリングや後続の最適化用にトラフィック クラスを作成するよう、PfR を手動で設定することができます。 自動学習では通常、デフォルトのプレフィックス長 /24 が使用されますが、手動設定では正確なプレフィックスを定義することができます。 トラフィック クラスの手動設定プロセスには、次の 2 つのコンポーネントがあります。

- プレフィックスベースのトラフィック クラスの手動設定
- アプリケーションベースのトラフィック クラスの手動設定

プロファイル フェーズの最終目標は、ネットワークを経由するトラフィックのサブセットを選択することです。 このトラフィックのサブセット（MTC リスト内のトラフィック クラス）は、使用可能な最良のパフォーマンス パスに基づいてルーティングする必要のあるトラフィックのクラスを表します。

上の図のトラフィック クラスのプロファイリングの各コンポーネントの詳細については、「パフォーマンス ルーティングの理解」モジュールを参照してください。

NBAR を使用した PfR アプリケーション マッピング

パフォーマンス ルーティングでの NBAR CCE アプリケーション認識の使用機能により、NBAR を使用したアプリケーションベース トラフィック クラスのプロファイリング機能が導入されました。 ネットワークベース アプリケーション認識（NBAR）は、Web ベースやその他の動的な TCP/UDP ポート割り当てを使用する分類困難なアプリケーションおよびプロトコルを含む、多様なプロトコルおよびアプリケーションを認識して分類する分類エンジンです。 PfR では NBAR を利用して、プロトコルまたはアプリケーションを認識し、分類します。分類されたトラフィック クラスは、PfR アプリケーション データベースに追加され、パッシブ モニタリングおよびアクティブ モニタリングの対象となります。

学習リスト コンフィギュレーション モードで **traffic-class application nbar**（PfR）コマンドを使用すると、NBAR アプリケーション マッピング名に基づいてトラフィック クラスが自動的にプロファイリングされます。オプションのプレフィックス リストを使用すると、特定のトラフィック クラスを除外または許可できます。

NBAR は、次の 3 種類のプロトコルに基づいてアプリケーションを識別できます。

- 非 UDP および非 TCP IP プロトコル：総称ルーティング カプセル化（GRE）、インターネット制御メッセージ プロトコル（ICMP）など。
- スタティックに割り当てられたポート番号を使用する TCP および UDP プロトコル：CU-SeeMe デスクトップ ビデオ会議（CU-SeeMe-Server）、Post Office Protocol over TLS/SSL server（SPOP3-Server）など。
- ダイナミックにポート番号を割り当て、状態検査を必要とする TCP および UDP プロトコル：Real-Time Transport Protocol オーディオ ストリーミング（RTP-audio）、BitTorrent ファイル転送トラフィック（BitTorrent）など。

NBAR を使用して識別され、パフォーマンス ルーティング トラフィック クラスのプロファイリングに使用できるアプリケーションのリストは、絶えず進化しています。 NBAR を使用して識別できるアプリケーションが、パフォーマンス ルーティングで使用できるかどうかを判別するには、**traffic-class application nbar ?** コマンドを使用します。

次の表に、スタティック アプリケーション マッピングによる OER：アプリケーション アウェア ルーティング機能でサポートされているスタティック アプリケーションおよび、非 UDP プロトコルや非 TCP プロトコルに基づくさまざまなアプリケーションのほか、ポート番号をダイナミックに割り当てる TCP および UDP アプリケーションの部分的なリストを表示します。 これらのアプリケーションはすべて、NBAR を使用して識別し、パフォーマンス ルーティングでのトラフィック クラスのプロファイルに使用できます。

表 *13*：*NBAR* によりサポートされるアプリケーションのリスト

アプリケーション	キーワード	プロトコル	ポート
BitTorrent：ファイル共有	**bittorrent**	TCP	ダイナミック割り当てまたは 6881 ～ 6889

アプリケーション	キーワード	プロトコル	ポート
Citrix ICA：アプリケーション名別 Citrix ICA トラフィック	**citrix**	TCP/UDP	ダイナミック割り当て
Direct Connect：Direct Connect ファイル転送トラフィック	**directconnect**	TCP/UDP	411
eDonkey/eMule：eDonkey ファイル共有アプリケーション （注） また、NBAR では eMule トラフィックは eDonkey トラフィックに分類されます。	**edonkey**	TCP	4662
Exchange：Exchange 用 MS-RPC	**exchange**	TCP	79
FastTrack：FastTrack	**fasttrack**	該当なし	ダイナミック割り当て
Gnutella：Gnutella	**gnutella**	TCP	ダイナミック割り当て
H.323：H.323 テレビ会議プロトコル	**h323**	TCP	ダイナミック割り当て
KaZaA：KaZaA バージョン 2 （注） KaZaA バージョン 1 トラフィックは FastTrack を使用して分類されます。	**kazaa2**	TCP/UDP	ダイナミック割り当て
MGCP：**Media Gateway Control Protocol**	**mgcp**	TCP/UDP	2427、2428、2727
Netshow：Microsoft Netshow	**netshow**	TCP/UDP	ダイナミック割り当て

アプリケーション	キーワード	プロトコル	ポート
Novadigm：**Novadigm Enterprise Desktop Manager（EDM）**	**novadigm**	TCP/UDP	3460 ～ 3465
r コマンド：rexec、rlogin、rsh	**rcmd**	TCP	ダイナミック割り当て
RTCP：Real-Time Control Protocol	**rtcp**	TCP/UDP	ダイナミック割り当て
RTP：Real-Time Transport Protocol（ペイロード分類）	**rtp**	TCP/UDP	ダイナミック割り当て
RTP-audio：Real-Time Transport Protocol ストリーミング オーディオ	**rtp:audio**	TCP/UDP	ダイナミック割り当て
RTP-Video：**Real-Time Transport Protocol（Video ストリーミング）**	**rtp:video**	TCP/UDP	ダイナミック割り当て
RTSP：**Real-Time Streaming Protocol**	**rtsp**	TCP/UDP	ダイナミック割り当て
SCCP/Skinny：**Skinny Client Control Protocol**	**skinny**	TCP	2000、2001、2002
SIP：**Session Initiation Protocol**	**sip**	TCP/UDP	5060
Skype：ピアツーピア VoIP クライアント ソフトウェア （注） 現在サポートされているのは Skype バージョン 1 だけです	**skype**	TCP/UDP	ダイナミック割り当て
SQL*Net：Oracle 向け SQL*NET	**sqlnet**	TCP/UDP	ダイナミック割り当て

アプリケーション	キーワード	プロトコル	ポート
StreamWorks：StreamWorks オーディオおよびビデオ	**streamwork**	UDP	ダイナミック割り当て
SunRCP：Sun Remote Procedure Call	**sunrcp**	TCP/UDP	ダイナミック割り当て
TFTP：Trivial File Transfer Protocol	**tftp**	UDP	ダイナミック割り当て
VDOLive：VDOLive ストリーミング ビデオ	**vdolive**	TCP/UDP	ダイナミック割り当て
WinMX：WinMX トラフィック	**winmx**	TCP	6699
X Windows：X11、X Windows	**xwindows**	TCP	6000 ～ 6003

NBAR の詳細については、『*QoS: NBAR Configuration Guide*』の「Classifying Network Traffic Using NBAR」の項を参照してください。

NBAR CCE アプリケーション認識を使用した PfR の設定方法

NBAR アプリケーション マッピングを使用してトラフィック クラスを自動学習する学習リストの定義

NBAR により識別されるアプリケーションを使用して学習リストを定義するには、マスター コントローラで次のタスクを実行します。 学習リスト内では、NBAR は、特定のアプリケーションのトラフィック クラスの識別に使用されます。 定義される学習リストには、NBAR を使用した PfR により自動学習されるトラフィック クラスが含まれます。また、オプションのプレフィックス リストを使用して、特定のトラフィック クラスを許可または除外することもできます。

トラフィック クラスを分類できる学習リストが追加されました。学習リストを使用すると、さまざまなPfRポリシーを各学習リストに適用できます。これよりも前のバージョンでは、トラフィック クラスを分割することはできず、PfR ポリシーは、学習セッション中にプロファイルされるすべてのトラフィック クラスに適用されていました。 NBAR CCE アプリケーション認識を使用し

たパフォーマンス ルーティング機能では、NBAR を使用して識別されるアプリケーションを使用できるようになりました。

このタスクでは、Real-Time Transport Protocol ストリーミング（オーディオ）（RTP-audio）トラフィックを識別するように、学習リストが設定されています。 RTP-audio トラフィックは、NBAR を使用して識別され、結果のプレフィックスは、プレフィックス長 24 に集約されます。 Skype トラフィック クラスを識別する 2 つめの学習リストは、Skype を表すキーワードを使用して設定し、プレフィックス長 24 に集約されます。 プレフィックス リストは、Skype トラフィック クラスに適用され、10.0.0.0/8 プレフィックスからのトラフィックを許可します。 マスター コントローラは、フィルタリング対象トラフィックの最高アウトバウンドスループットに基づいてトッププレフィックスを学習するように設定され、その結果得られたトラフィック クラスが PfR アプリケーション データベースに追加されます。

次に、学習リストで RTP-audio および Skype アプリケーションの両方に対してプロファイルされるトラフィック ストリームを示します。

```
10.1.1.1
10.1.2.1
20.1.1.1
20.1.2.1
```

次に、各アプリケーションで学習されるトラフィック クラスを示します。

```
10.1.1.0/24 rtp-audio
10.1.2.0/24 rtp-audio
20.1.1.0/24 rtp-audio
20.1.2.0/24 rtp-audio
10.1.1.0/24 skype
10.1.2.0/24 skype
```

学習されるトラフィック クラスの違いは、送信先プレフィックスがプレフィックス 10.0.0.0/8 と一致する Skype アプリケーション トラフィックだけを含む、INCLUDE_10_NET プレフィックス リストによる違いです。

設定された学習リストおよび PfR によって学習されたトラフィック クラスに関する情報を表示する方法については、「NBAR を使用して識別されるトラフィック クラスに関する情報の表示およびリセット」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. **pfr master**
5. **learn**
6. **list seq** *number* **refname** *refname*
7. **traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*]
8. **aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*}
9. **throughput**
10. **exit**
11. **list seq** *number* **refname** *refname*
12. **traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*]
13. **aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*}
14. **throughput**
15. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length*	**permit** *network/length*} 例： `Device(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8`	学習するプレフィックスをフィルタリングするための IP プレフィックス リストを作成します。 • IP プレフィックス リストを学習リスト コンフィギュレーション モードで使用すると、学習される IP アドレスをフィルタリングすることができます。 • 例では、PfR に INCLUDE_10_NET という IP プレフィックス リストが作成され、プレフィックス 10.0.0.0/8 のプロファイリングが行われます。

	コマンドまたはアクション	目的
ステップ 4	**pfr master** 例： `Device(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、マスター コントローラとして Cisco ルーティング デバイスを設定し、マスター コントローラ ポリシーおよびタイマー設定を設定します。
ステップ 5	**learn** 例： `Device(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、トラフィック クラスを自動的に学習します。
ステップ 6	**list seq** *number* **refname** *refname* 例： `Device(config-pfr-mc-learn)# list seq 10 refname LEARN_RTP_AUDIO_TC`	PfR 学習リストを作成し、学習リスト コンフィギュレーション モードを開始します。 • 学習リスト基準が適用される順番の決定に使用されるシーケンス番号を指定するには、**seq** キーワードおよび *number* 引数を使用します。 • 学習リストの参照名を指定するには、**refname** キーワードおよび *refname* 引数を使用します。 • 例では、LEARN_RTP_AUDIO_TC という名前の学習リストが作成されます。
ステップ 7	**traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*] 例： `Device(config-pfr-mc-learn-list)# traffic-class application nbar rtp:audio`	NBAR により識別できるアプリケーションを使用して PfR トラフィック クラスを定義します。 • *nbar-app-name* 引数を使用して、NBAR を使用して識別される 1 つ以上のアプリケーションを指定します。 • 例では、RTP-audio トラフィックを含むトラフィック クラスが定義されます。
ステップ 8	**aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*} 例： `Device(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	（任意）トラフィック フロータイプに基づいて学習済みのプレフィックスを集約するように、マスター コントローラを設定します。 • **bgp** キーワードは、BGP ルーティング テーブル内のエントリに基づいてプレフィックスを集約するように設定します。 このキーワードは、BGP ピアリングがネットワーク内でイネーブルの場合に使用されます。 • **non-bgp** キーワードは、スタティック ルートに基づいて学習済みのプレフィックスを集約するように設定します。 このキーワードが入力された場合、BGP ルーティング テーブル内のエントリは無視されます。

	コマンドまたはアクション	目的
		• **prefix-length** キーワードは、指定したプレフィックス長に基づいて集約するように設定します。 有効な値の範囲は、1 ～ 32 です。 • このコマンドが指定されない場合、デフォルトの集約が、/24 のプレフィックス長に基づいて実行されます。 • 例では、/24 のプレフィックス長に基づいて、プレフィックス長の集約が設定されます。
ステップ 9	**throughput** 例： `Device(config-pfr-mc-learn-list)# throughput`	最高アウトバウンド スループットに基づいてトップ プレフィックスを学習するように、マスター コントローラを設定します。 • このコマンドをイネーブルにすると、マスター コントローラでは最高アウトバウンド スループットに従ってすべての境界ルータのトップ プレフィックスが学習されます。 • 例では、LEARN_RTP_AUDIO_TC トラフィック クラスの最高アウトバウンドスループットに基づいてトッププレフィックスを学習するように、マスター コントローラが設定されます。
ステップ 10	**exit** 例： `Device(config-pfr-mc-learn-list)# exit`	学習リスト コンフィギュレーション モードを終了し、PfR Top Talker/Top Delay 学習コンフィギュレーション モードに戻ります。
ステップ 11	**list seq** *number* **refname** *refname* 例： `Device(config-pfr-mc-learn)# list seq 10 refname LEARN_SKYPE_TC`	PfR 学習リストを作成し、学習リスト コンフィギュレーション モードを開始します。 • 学習リスト基準が適用される順番の決定に使用されるシーケンス番号を指定するには、**seq** キーワードおよび *number* 引数を使用します。 • 学習リストの参照名を指定するには、**refname** キーワードおよび *refname* 引数を使用します。 • 例では、LEARN_SKYPE_TC という名前の学習リストが作成されます。
ステップ 12	**traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] [**filter** *prefix-list-name*] 例： `Device(config-pfr-mc-learn-list)#`	NBAR により識別できるアプリケーションを使用して PfR トラフィック クラスを定義します。 • *nbar-app-name* 引数を使用して、NBAR を使用して識別される 1 つ以上のアプリケーションを指定します。

	コマンドまたはアクション	目的
	`traffic-class application nbar skype filter INCLUDE_10_NET`	• 例では、NBAR を使用して識別され、プレフィックス リスト INCLUDE_10_NET で定義されているプレフィックスと一致するトラフィック クラスを Skype トラフィックに含めるように定義しています。
ステップ 13	**aggregation-type** {**bgp** | **non-bgp** | **prefix-length** *prefix-mask*} 例： `Device(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	（任意）トラフィック フロータイプに基づいて学習済みのプレフィックスを集約するように、マスター コントローラを設定します。 • **bgp** キーワードは、BGP ルーティング テーブル内のエントリに基づいてプレフィックスを集約するように設定します。 このキーワードは、BGP ピアリングがネットワーク内でイネーブルの場合に使用されます。 • **non-bgp** キーワードは、スタティック ルートに基づいて学習済みのプレフィックスを集約するように設定します。 このキーワードが入力された場合、BGP ルーティング テーブル内のエントリは無視されます。 • **prefix-length** キーワードは、指定したプレフィックス長に基づいて集約するように設定します。 有効な値の範囲は、1 ～ 32 です。 • このコマンドが指定されない場合、デフォルトの集約が、/24 のプレフィックス長に基づいて実行されます。 • 例では、/24 のプレフィックス長に基づいて、プレフィックス長の集約が設定されます。
ステップ 14	**throughput** 例： `Device(config-pfr-mc-learn-list)# throughput`	最高アウトバウンド スループットに基づいてトップ プレフィックスを学習するように、マスター コントローラを設定します。 • このコマンドをイネーブルにすると、マスター コントローラでは最高アウトバウンド スループットに従ってすべての境界ルータのトップ プレフィックスが学習されます。 • 例では、LEARN_SYKPE_TC トラフィック クラスの最高アウトバウンドスループットに基づいたトッププレフィックスを学習するようにマスター コントローラを設定しています。
ステップ 15	**end** 例： `Device(config-pfr-mc-learn-list)# end`	学習リスト 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。

NBARアプリケーション マッピングを使用したトラフィック クラスの手動選択

NBARアプリケーションマッピングを使用してトラフィック クラスを手動選択するには、次のタスクを実行します。次のタスクは、トラフィック クラスに選択する送信先プレフィックスおよびNBAR により識別されるアプリケーションが判明している場合に実行します。 次のタスクでは、IP プレフィックス リストを作成して、送信先プレフィックスを定義し、NBAR により識別されるアプリケーション、BitTorrent および Direct Connect を、**match traffic-class application**（PfR）コマンドを使用して定義します。 PfR マップを使用して、各プレフィックスを各アプリケーションに対応付けて、トラフィック クラスを作成します。

この例のトラフィック クラスは、NBAR を使用して識別され、プレフィックス リスト LIST1 で指定される送信先プレフィックス 10.1.1.0/24 と一致する BitTorrent および Direct Connect トラフィックで構成されます。 BitTorrent および Direct Connect アプリケーションと送信先プレフィックスの両方に一致するトラフィックだけが学習されます。

NBAR を使用して識別され、PfR によって学習される手動設定のトラフィック クラスに関する情報を表示する方法については、「NBAR を使用して識別されるトラフィック クラスに関する情報の表示およびリセット」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. 必要に応じて、追加のプレフィックス リスト エントリに対し、ステップ 3 を繰り返します。
5. **pfr-map** *map-name sequence-number*
6. **match traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] **prefix-list** *prefix-list-name*
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。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} 例： `Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24`	送信先プレフィックスベースのトラフィック クラスを指定するために、プレフィックス リストを作成します。 • 例では、アプリケーション トラフィック クラスのフィルタリングに使用する送信先プレフィックス 10.1.1.0/24 が指定されます。
ステップ 4	必要に応じて、追加のプレフィックス リスト エントリに対し、ステップ 3 を繰り返します。	—
ステップ 5	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map APPL_NBAR_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • permit シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 6 で **match traffic-class application nbar**（PfR）コマンドを使用して適用します。 • 例では、APPL_NBAR_MAP という名前の PfR マップが作成されます。
ステップ 6	**match traffic-class application nbar** *nbar-app-name* [*nbar-app-name...*] **prefix-list** *prefix-list-name* 例： `Router(config-pfr-map)# match traffic-class application nbar bittorrent directconnect prefix-list LIST1`	NBAR を使用してプレフィックス リストの一致条件として識別できる 1 つ以上のアプリケーションを手動設定して、PfR マップを使用してトラフィック クラスを作成します。 • *nbar-app-name* 引数を使用して、NBAR を使用して識別できる 1 つ以上のアプリケーションを指定します。 • 例では、トラフィック クラスを送信先プレフィックス Y のアプリケーション X として定義します。ここで、X は BitTorrent または Direct Connect ファイル転送トラフィックで、Y は LIST1 という名前の IP プレフィックス リストで定義されている宛先アドレスです。
ステップ 7	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

NBAR を使用して識別されるトラフィック クラスに関する情報の表示およびリセット

このタスクのすべてのコマンドは省略可能です。これらのコマンドは、学習リストが設定されてトラフィック クラスが自動的に学習された後で、またはPfRマップを使用してトラフィック クラスが手動設定された後で入力できます。ほとんどのコマンドは、マスターコントローラで入力されますが、一部のコマンドは境界ルータで入力されます。次の手順に、各コマンドを入力するデバイスを示します。

手順の概要

1. マスター コントローラを設定したルータに移動します。
2. **enable**
3. **show pfr master traffic-class application nbar** *nbar-app-name* [*prefix*] [**active passive status** | **detail**]
4. **show pfr master nbar application**
5. **show pfr master defined application**
6. **clear pfr master traffic-class application nbar** [*nbar-appl-name*[*prefix*]]
7. PfR ネットワークの一部として設定される境界ルータに移動します。
8. **enable**
9. **show pfr border routes** {**bgp** | **cce** | **static**}
10. **show pfr border defined application**

手順の詳細

ステップ 1 マスター コントローラを設定したルータに移動します。

ステップ 2 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 3 **show pfr master traffic-class application nbar** *nbar-app-name* [*prefix*] [**active passive status** | **detail**]
このコマンドは、NBARを使用して識別され、PfRマスター コントローラにより監視および制御されるアプリケーション トラフィック クラスに関する情報を表示するために使用されます。 次の例に、Real-Time Transport Protocol ストリーミング（オーディオ）（RTP-audio）トラフィックで構成されるトラフィック クラスに関する情報を示します。

例：

```
Device# show pfr master traffic-class application nbar rtp:audio

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
```

```
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
           Flags             State     Time             CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
------------------------------------------------------------------------------
10.1.1.0/28       RTP-Audio defa    N           N           N 0.0.0.0/0
                            DEFAULT*      461         10.11.1.2    Et1/0        U
              U        U        0        0        1        2
            150      130        0        0       15        0
10.1.1.16/28      RTP-Audio defa    N           N           N 0.0.0.0/0
                            DEFAULT*      461         10.11.1.2    Et1/0        U
              U        U        0        0        1        2
            250      200        0        0       30        0
```

ステップ 4 **show pfr master nbar application**

このコマンドは、各 PfR 境界ルータで NBAR を使用して識別されるアプリケーションのステータスに関する情報を表示するために使用されます。 次の出力の一部を示した例に、IP アドレスにより識別される 3 つの PfR 境界ルータで NBAR を使用して識別されるアプリケーションのステータスに関する情報を示します。 NBAR アプリケーションが 1 つ以上の境界ルータでサポートされていない場合、その NBAR アプリケーションに関するすべてのトラフィック クラスに非アクティブのマークが付けられます。これは、PfR を使用して最適化できません。

例：

```
Device# show pfr master nbar application

NBAR Appl                  10.1.1.4        10.1.1.2        10.1.1.3
-------------------------------------------------------------------
aarp                        Invalid         Invalid         Invalid
appletalk                   Invalid         Invalid         Invalid
arp                         Invalid         Invalid         Invalid
bgp                           Valid           Valid           Valid
bittorrent                    Valid           Valid           Valid
bridge                      Invalid         Invalid         Invalid
bstun                       Invalid         Invalid         Invalid
cdp                         Invalid         Invalid         Invalid
citrix                      Invalid         Invalid         Invalid
clns                          Valid         Invalid         Invalid
clns_es                     Invalid         Invalid         Invalid
clns_is                     Invalid         Invalid         Invalid
cmns                        Invalid         Invalid         Invalid
compressedtcp               Invalid         Invalid         Invalid
cuseeme                     Invalid         Invalid         Invalid
.
.
.
```

ステップ 5 **show pfr master defined application**

このコマンドは、PfR で使用されるユーザ定義アプリケーションの定義に関する情報を表示するために使用されます。

例：

```
Device# show pfr master defined application
```

```
OER Defined Applications:
Name                 Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
-----------------------------------------------------------------------------
telnet                     1 defa  tcp       23-23     1-65535 0.0.0.0/0
telnet                     1 defa  tcp     1-65535       23-23 0.0.0.0/0
ftp                        2 defa  tcp       21-21     1-65535 0.0.0.0/0
ftp                        2 defa  tcp     1-65535       21-21 0.0.0.0/0
cuseeme                    4 defa  tcp   7648-7648     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp   7649-7649     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp     1-65535   7648-7648 0.0.0.0/0
cuseeme                    4 defa  tcp     1-65535   7649-7649 0.0.0.0/0
dhcp                       5 defa  udp       68-68       67-67 0.0.0.0/0
dns                        6 defa  tcp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  tcp     1-65535       53-53 0.0.0.0/0
dns                        6 defa  udp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  udp     1-65535       53-53 0.0.0.0/0
finger                     7 defa  tcp       79-79     1-65535 0.0.0.0/0
finger                     7 defa  tcp     1-65535       79-79 0.0.0.0/0
gopher                     8 defa  tcp       70-70     1-65535 0.0.0.0/0
.
.
.
```

ステップ 6 **clear pfr master traffic-class application nbar** [*nbar-appl-name*[*prefix*]]

このコマンドは、PfR の制御対象トラフィック クラスをマスター コントローラ データベースからクリアするために使用されます。 次に、NBAR を使用して識別される RTP-Audio アプリケーションで定義され、10.1.1.0/24 プレフィックスによりフィルタリングされる PfR トラフィック クラスをクリアする例を示します。

例：

```
Device# clear pfr master traffic-class application nbar rtp:audio 10.1.1.0/24
```

ステップ 7 PfR ネットワークの一部として設定される境界ルータに移動します。

ステップ 8 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 9 **show pfr border routes** {**bgp** | **cce** | **static**}

このコマンドは、NBAR を使用して識別されるアプリケーションの PfR 制御対象ルートに関する情報を表示するために使用されます。 次に、境界ルータの CCE 制御ルートを表示する例を示します。

例：

```
Device# show pfr border routes cce

Class-map pfr-class-acl-pfr_cce#2-stile-telnet, permit, sequence 0, mask 24
  Match clauses:
    ip address (access-list): pfr_cce#2
    stile: telnet
  Set clauses:
    ip next-hop 10.1.3.2
    interface Ethernet2/3
```

```
  Statistic:
    Packet-matched: 60
```

ステップ 10 **show pfr border defined application**

このコマンドは、PfR 境界ルータにより監視されるすべてのユーザ定義アプリケーションを表示するときに使用されます。

例：

```
Device# show pfr border defined application

OER Defined Applications:
Name                 Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
-------------------------------------------------------------------------------
telnet                     1 defa  tcp       23-23     1-65535 0.0.0.0/0
telnet                     1 defa  tcp     1-65535       23-23 0.0.0.0/0
ftp                        2 defa  tcp       21-21     1-65535 0.0.0.0/0
ftp                        2 defa  tcp     1-65535       21-21 0.0.0.0/0
cuseeme                    4 defa  tcp   7648-7648     1-65535 0.0.0.0/0
cuseeme                    4 defa  tcp   7649-7649     1-65535 0.0.0.0/0
dhcp                       5 defa  udp       68-68       67-67 0.0.0.0/0
dns                        6 defa  tcp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  tcp     1-65535       53-53 0.0.0.0/0
dns                        6 defa  udp       53-53     1-65535 0.0.0.0/0
dns                        6 defa  udp     1-65535       53-53 0.0.0.0/0
finger                     7 defa  tcp       79-79     1-65535 0.0.0.0/0
finger                     7 defa  tcp     1-65535       79-79 0.0.0.0/0
gopher                     8 defa  tcp       70-70     1-65535 0.0.0.0/0
.
.
.
```

NBAR CCE アプリケーション認識を使用した PfR の設定例

例：NBAR アプリケーション マッピングを使用してトラフィック クラスを自動的に学習するための学習リストの定義

次に、NBAR アプリケーション マッピングを使用してアプリケーション トラフィック クラスを定義する例を示します。 この例では、次の 2 つの PfR 学習リストが定義されます。

- LEARN_RTP_AUDIO_TC：RTP-Audio により表されるリアルタイム ストリーミングのオーディオ トラフィック。
- LEARN_SKYPE_TC：Skype および 10.0.0.0/8 プレフィックスにより表されるリモート オーディオおよびビデオ トラフィック。

目的は、1 つのポリシー（STREAM_AUDIO）を使用してリアルタイム ストリーミングのオーディオ トラフィックを最適化することと、別のポリシー（REMOTE_AUDIO_VIDEO）を使用してリ

モート オーディオおよびビデオ トラフィックを最適化することです。 次のタスクでは、最高遅延に基づいたトラフィック クラスの学習が設定されます。

次に、学習リストで RTP-Audio および Skype アプリケーションの両方に対してプロファイルされるトラフィック ストリームを示します。

```
10.1.1.1
10.1.2.1
20.1.1.1
20.1.2.1
```

次に、各アプリケーションで学習されるトラフィック クラスを示します。

```
10.1.1.0/24 rtp-audio
10.1.2.0/24 rtp-audio
20.1.1.0/24 rtp-audio
20.1.2.0/24 rtp-audio
10.1.1.0/24 skype
10.1.2.0/24 skype
```

学習されるトラフィック クラスの違いは、送信先プレフィックスがプレフィックス 10.0.0.0/8 と一致する Skype アプリケーション トラフィックだけを含む、INCLUDE_10_NET プレフィックス リストによる違いです。

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
pfr master
 learn
  list seq 10 refname LEARN_RTP_AUDIO_TC
   traffic-class application nbar rtp-audio
   aggregation-type prefix-length 24
   delay
   exit
  list seq 20 refname LEARN_SKYPE_TC
   traffic-class application nbar skype filter INCLUDE_10_NET
   aggregation-type prefix-length 24
   delay
   exit
  exit
 exit
pfr-map STREAM_AUDIO 10
 match learn list LEARN_RTP_AUDIO_TC
 exit
pfr-map REMOTE_AUDIO_VIDEO 20
 match learn list LEARN_SKYPE_TC
 end
```

例：NBAR アプリケーション マッピングを使用した、トラフィック クラスの手動選択

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、NBAR を使用して識別され、プレフィックス リスト LIST1 で指定されている送信先プレフィックス 10.1.1.0/24、10.1.2.0/24 および 172.16.1.0/24 と一致するファイル転送 BitTorrent または Direct Connect アプリケーション トラフィックを含めるように PfR マップを設定する例を示します。 BitTorrent および Direct Connect アプリケーションと送信先プレフィックスの両方に一致するトラフィックだけが学習されます。

```
ip prefix-list LIST1 permit 10.1.1.0/24
ip prefix-list LIST1 permit 10.1.2.0/24
ip prefix-list LIST1 permit 172.16.1.0/24
pfr-map PREFIXES 10
```

```
match traffic-class application nbar bittorrent directconnect prefix-list LIST1
end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

NBAR CCE アプリケーション認識を使用した PfR の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *14*：*NBAR CCE* アプリケーション認識を使用した *PfR* の機能情報

機能名	リリース	機能の設定情報
NBAR/CCE アプリケーション認識を使用したパフォーマンス ルーティング	12.4(20)T Cisco IOS XE Release 3.7S	NBAR CCE アプリケーション認識を使用したパフォーマンス ルーティング機能は、ネットワークベース アプリケーション認識（NBAR）を使用してアプリケーションベースのトラフィック クラスをプロファイルできる機能を導入します。NBARは、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。たとえば、ダイナミック TCP/UDP ポート割り当てを使用する Web ベースや他の分類が困難なアプリケーションとプロトコルなどです。 PfR では NBARを利用して、プロトコルまたはアプリケーションを認識し、分類します。分類されたトラフィック クラスは、PfRアプリケーション データベースに追加され、パッシブ モニタリングおよびアクティブ モニタリングの対象となります。 この機能により、次のコマンドが導入または変更されました。**application define（PfR）**、**clear pfr master traffic-class application nbar**、**match traffic-class application nbar（PfR）**、**show pfr border routes**、**show pfr master nbar application**、**show pfr master traffic-class application nbar**、**traffic-class application nbar（PfR）**。

第 12 章

パフォーマンス ルーティング：Protocol Independent Route Optimization（PIRO）

Protocol Independent Route Optimization（PIRO）は、パフォーマンス ルーティング（PfR）で IP ルーティング情報ベース（RIB）の親ルート（完全一致ルート、またはそれより一致度が低いルート）を検索し、OSPF および IS-IS などの内部ゲートウェイ プロトコル（IGP）を含む IP ルート環境に PfR を導入できる機能を導入しました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンス ルーティング PIRO の概要

Protocol Independent Route Optimization（PIRO）

PfR：Protocol Independent Route Optimization（PIRO）機能が追加され、PfR でトラフィック クラスを識別および制御できるようになりました。 PIRO より前に、PfR は、BGP またはスタティック ルート データベースで親ルート（完全一致ルート、またはそれより一致度が低いルート）を持つトラフィック クラスのパスを最適化します。 PIRO を使用して、PfR は親ルートの IP ルーティング情報ベース（RIB）を検索できます。これにより、OSPF や IS-IS などの内部ゲートウェイ プロトコル（IGP）を含む任意の IP ルーティング環境に PfR を導入することができます。

親ルートの検索は、BGP ルーティング データベースから始まります。ここで見つからなかった場合は、スタティック ルート データベースが検索されます。 ここでも親ルートが見つからなかった場合は RIB が検索されます。 RIB を検索して親ルートが見つかると、ポリシーベース ルーティング（PBR）を使用して、ルート制御がトラフィック クラスに適用され、ダイナミック ルート マップが作成されます。

PfR ルート制御モードがイネーブルの場合、PIRO をイネーブルにするために新たにカスタマー設定を行う必要ありません。

マスター コントローラで、**show pfr master prefix** コマンドを使用すると、出力に「RIB-PBR」として PIRO ルートが表示されます。

パフォーマンス ルーティング PIRO の設定方法

Protocol Independent Route Optimization のルート制御変更の確認およびデバッグ

PfR ルート制御モードがイネーブルの場合、PIRO をイネーブルにするために新たにカスタマー設定を行う必要ありません。親ルートが RIB に存在し、ポリシーベース ルーティングを使用して制御される PIRO ルートをデバッグする場合は、この任意のタスクのステップを実行します。 すべてのステップは任意ですが、順番は任意ではありません。 これらのステップから得られる情報では、トラフィック クラスに関連付けられた特定のプレフィックスが、PIRO を使用して識別されたか、または PfR によって制御されているかを確認できます。 最初の 2 つの CLI コマンドは、マスター コントローラで入力します。他のコマンドは、境界ルータで入力します。

手順の概要

1. マスター コントローラから開始します。
2. **enable**
3. **show pfr master traffic-class**
4. 境界ルータに移動して、次のステップを開始します。
5. **enable**
6. **show ip route**
7. **show route-map dynamic**
8. **show ip access-list dynamic**
9. **debug pfr border routes** {**bgp** | **static** | **piro**[**detail**]}

手順の詳細

ステップ 1 マスター コントローラから開始します。

ステップ 2 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 3 **show pfr master traffic-class**
このコマンドは、PfR マスター コントローラにより監視および制御されるトラフィック クラスに関する情報を表示するときに使用されます。 このコマンドの出力には、トラフィック クラスの送信先 IP アドレスおよびプレフィックス長、このトラフィック クラスに関連付けられるプレフィックスがルーティングされるときの境界ルータの IP アドレスおよびインターフェイス、トラフィック クラスの状態、プロトコルに関する情報が示されます。 この例では、プレフィックス 10.1.1.0 に表示されるプロトコルは RIB-PBR です。つまり、トラフィック クラスの親ルートが RIB に存在し、ポリシーベース ルーティングがプレフィックスの制御に使用されています。 このステップでは、次のタスクに関連する構文だけを示します。 **show pfr master prefix** コマンドを使用しても同様の情報を表示できます。

例：

```
Router# show pfr master traffic-class

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
```

```
------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
                          INPOLICY        0           10.2.1.2 Gi0/0/1  RIB-PBR
               N        N        N        N        N        N        N        N
               1        1        0        0        N        N        N        N
```

ステップ 4 境界ルータに移動して、次のステップを開始します。
次のコマンドは、マスター コントローラではなく、境界ルータで入力します。

ステップ 5 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 6 **show ip route**
ルーティング テーブルの現在の状態を表示します。 このコマンドを使用すると、親ルートが RIB に存在するか確認できます。

例：

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, GigabitEthernet0/0/1
     192.168.0.0/24 is subnetted, 1 subnets
O       192.168.50.0 [110/20] via 10.10.10.3, 00:20:32, GigabitEthernet0/2/2
     10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O       10.1.4.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
O       10.1.5.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
O       10.1.6.1/32 [110/31] via 10.40.40.2, 00:20:32, GigabitEthernet0/0/2
B       10.1.1.0/24 [20/0] via 10.40.40.2, 00:38:08
     10.1.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/40] via 10.40.40.2, 00:20:33, GigabitEthernet0/0/2
```

ステップ 7 **show route-map dynamic**
ダイナミック ルートマップを表示しても、ルート制御が PIRO ルートにどのように適用されるか確認できます。 このダイナミック ルート マップの出力では、アクセス リストは pfr#6 という名前です。 このステップでは、次のタスクに関連する構文だけを示します。

例：

```
Router# show route-map dynamic

 route-map OER-04/21/09-21:42:55.543-6-OER, permit, sequence 0, identifier 1755354068
  Match clauses:
    ip address (access-lists): pfr#6
  Set clauses:
```

```
    ip next-hop 10.40.40.2
    interface GigatbitEthernet0/0/2
  Policy routing matches: 2314 packets, 138840 bytes
 Current active dynamic routemaps = 1
```

ステップ 8 **show ip access-list dynamic**

このコマンドは、この境界ルータで作成されるダイナミック IP アクセス リストを表示します。 この出力では、pfr#6 という名前のダイナミック アクセス リストが表示されます。これは、プレフィックス 10.1.1.0 のトラフィックがこの境界ルータを介してルーティングされることを許可します。 アクセス リスト pfr#6 は、前のステップの **show route-map dynamic** コマンドで識別されました。 このステップでは、次のタスクに関連する構文だけを示します。

例：

```
Router# show ip access-list dynamic

Extended IP access list pfr#6
    1073741823 permit ip any 10.1.1.0 0.0.0.255 (2243 matches)
```

ステップ 9 **debug pfr border routes** {**bgp** | **static** | **piro**[**detail**]}

このコマンドは、境界ルータで入力します。 このコマンドは、RIB で親ルートが特定された場合に、親ルートの検索と既存の親ルートへのルート変更をデバッグするときに使用されます。 この例では、詳細なデバッグ情報は、ステップ 2 の出力で示されるプレフィックス 10.1.1.0 の親ルートが RIB にあり、アプリケーションを制御するルート マップが作成されることを示しています。 スタティックおよび BGP ルート制御、詳細なボーダー PBR デバッグもアクティブであることに注意してください。

例：

```
Router# debug pfr border routes piro detail

Apr 21 21:41:25.667: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
Apr 21 21:42:55.539: OER STATIC: No parent found, network 10.1.1.0/24
Apr 21 21:42:55.539: PFR PIRO: Control Route, 10.1.1.0/24, NH 0.0.0.0,
IF GigabitEthernet0/0/2
Apr 21 21:42:55.539: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
Apr 21 21:42:55.539: OER BR PBR(det): control app: 10.1.1.0/24, nh 0.0.0.0, if
GigabitEthernet0/0/2,ip prot 256,dst opr 0,src opr 0, 0 0 0 0,rc net 0.0.0.0/0,dscp 0/0
Apr 21 21:42:55.543: OER BR PBR(det): Create rmap 65DC1CE8
Apr 21 21:42:55.547: PFR PIRO: Parent lookup found parent 10.1.1.0, mask 24, nexthop
10.40.40.2
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンス ルーティング PIRO の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *15*：パフォーマンス ルーティング *PIRO* の機能情報

機能名	リリース	機能情報
PfR：Protocol Independent Route Optimization（PIRO）	Cisco IOS XE Release 3.3S	PIRO は、PfR で IP ルーティング情報ベース（RIB）の親ルート（完全一致ルート、またはそれより一致度が低いルート）を検索し、OSPF および IS-IS などの内部ゲートウェイ プロトコル（IGP）を含む IP ルート環境に PfR を導入できる機能を導入しました。 この機能により、次のコマンドが変更されました。**debug pfr border routes** および **show pfr master prefix**。

第 13 章

PfR RSVP コントロール

PfR RSVP コントロール機能により、リソース予約プロトコル（RSVP）によって制御されるトラフィックのアプリケーション アウェア パスの選択を実行する機能が導入されています。 この機能を使用すると、パフォーマンス ルーティング（PfR）によって RSVP フローを学習し、PfR マスター コントローラが PfR ポリシーを使用して最良の出口を決定後にプロトコル Path メッセージをリダイレクトできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR RSVP コントロールの概要

PfR および RSVP コントロール

PfR RSVP コントロール機能により、リソース予約プロトコル（RSVP）フローを学習、監視、および最適化するパフォーマンス ルーティング（PfR）の機能が導入されています。 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、ネットワーク エッジで複数の ISP または WAN 接続を使用する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。

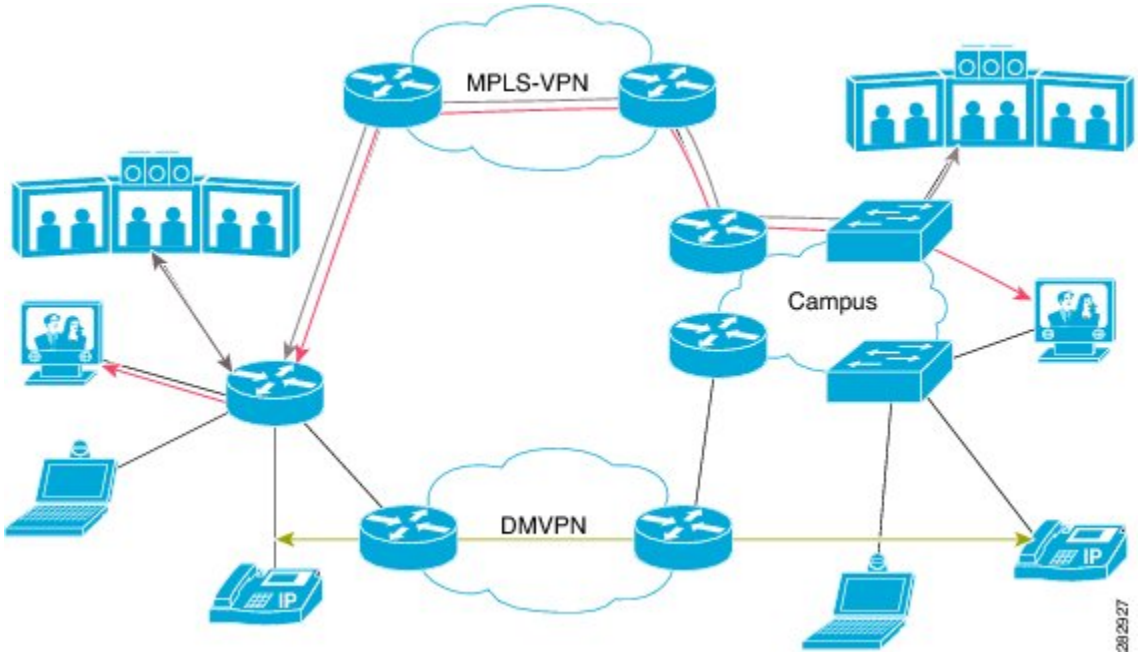
PfR は、設定された、またはネットワークを通過するトラフィックを観察することで学習されたアプリケーションおよびプレフィックスを監視し、制御できます。 マスター コントローラ（MC）は、境界ルータ（BR）を経由するさまざまなトラフィック クラスに対してポリシーの定義および適用を行う、一元化されたポリシー デシジョン ポイントです。 MC は、ネットワーク上のトラフィック クラス学習し、制御するように設定できます。 MC は出口選択を行い、その出口選択を実施するように BR に指示します。 最新の PfR 実装は音声/ビデオ トラフィックを最適化するために使用できますが、PfR によって行われる制御は RSVP などの技術に対応していません。 PfR と RSVP の統合により、PfR が提供できるアプリケーション固有のルート制御を RSVP が利用できるようになります。

RSVP は、音声/ビデオ トラフィックの信頼性を向上させるためにリソースを予約できる標準ベースの制御プロトコルです。 RSVP は、実際のデータ フローに先立ってデータ フローのリソースを予約するために、トラフィック プロファイルをシグナリングして、これを実現します。 メディア パスでエンドツーエンドのリソース予約を確立することで、RSVP は必要ときにリソースを使用できることを保証できます。 RSVP は、メディア フローとのパスの一致を実現するために、フォワーディング プレーン データベース（または CEF）を確認します。 CEF データベース内のルートは、ルーティング プロトコルによって主に決定されます。この場合、最適なルートを決定する唯一のメトリックは、該当パスのリンクの累積コストです。

次の図では、左側のネットワークの 2 つのパスが右側のキャンパス ネットワークに到達しています。 1 つのパスは DMVPN クラウドを使用し、もう 1 つのパスは MPLS-VPN クラウド使用しています。 必要な速度と帯域幅によっては、ビデオ アプリケーションを MPLS-VPN ネットワーク経由でルーティングし、音声アプリケーションを DMVPN ネットワーク経由でルーティングしたほうがいい場合があります。 この種のアプリケーション アウェア パスの選択は CEF では不可能で

すが、PfR はパフォーマンス基準に基づいて特定のアプリケーション トラフィックの最適パスを決定できます。

図 *16*：アプリケーション アウェア パスの選択



RSVP の統合により、PfR は RSVP フローを学習、監視、および最適化します。 RSVP は、新しい学習ソースとして含まれます。 PfR は、内部および外部インターフェイスを経由する RSVP フローを学習します。 各 RSVP フローは PfR トラフィック クラスとして学習され、他の RSVP フローとは独立して制御されます。学習したフローのフィルタリングは、プレフィックス リストとルート マップでサポートされていますが、RSVP フローの集約は推奨されません。 PfR マスター コントローラ（MC）は、設定された PfR ポリシーに基づいて最良の出口を選択し、トラフィックをリダイレクトするためのルート マップをインストールします。 いずれかの RSVP フローがポリシー違反（OOP）状態になると、PfR は新しい出口を見つけて、RSVP フローをその出口に切り替えます。 RSVP は、リフレッシュ時（通常 30 秒以内）に、または Fast Local Repair（FLR）ケースとして 5 秒未満で、新しいパスに予約を再インストールします。

PfR RSVP コントロール機能の目的は、ルータが RSVP Path メッセージを受信したときにルート マップを識別し、インストールすることです。 ルート マップはデータ トラフィックをキャプチャし、RSVP は Path メッセージにこのパスを使用します。

RSVP フローは、送信元アドレス、送信元ポート、送信先アドレス、送信先ポート、および IP プロトコルで識別できる単一のアプリケーション フローとして定義された PfR トラフィック クラスとして学習されます。 このマイクロフローは、PfR によってアプリケーションとして最適化され、このトラフィック クラスを選択した出口経由で転送するために、PfR によってダイナミック ポリシー ルートが作成されます。

すべての RSVP フローは、検討されている出口に十分な帯域幅があることを PfR がチェックした後でのみ最適化されます。 この情報は、BR から MC に定期的にプッシュされます。 BR 自体では、RSVP は、インターフェイスの帯域幅プールが変わるたびに PfR に通知します。

同等パス ラウンドロビン リゾルバ

PfR では、PfR RSVP コントロール機能を備えた新しいリゾルバが導入されました。 デフォルトでは、PfR はランダム リゾルバを使用して、PfR ポリシーで決定されたものと同じコストを持つ、同等のパス、出口の決定を行います。 **equivalent-path-round-robin** コマンドを使用してラウンドロビン リゾルバが設定されると、次の出口（ネクスト ホップ インターフェイス）が選択され、実行中の PfR ポリシーと比較されます。 ラウンドロビン リゾルバは、同等の出口の配列を渡され、その配列からラウンドロビン方式で選択します。 出口は、現在と同じ方式で各リゾルバによってプルーニングされます。 出口がポリシーに一致した場合、その出口が最良の出口となります。 ラウンドロビン リゾルバは特定の RSVP チェックは行いません。 再度ランダム リゾルバを使用する場合は、**equivalent-path-round-robin** コマンドの no 形式を入力します。

すべての PfR トラフィック クラスがラウンドロビン リゾルバを使用して、PfR ポリシーによって決定される複数の同等パスのロードバランシング スキームを提供できます。

最良パス選択用の RSVP ダイヤル後遅延タイマー

PfR RSVP コントロール機能では、PfR マスター コントローラ上で RSVP フローの学習がイネーブルになっている場合に境界ルータで実行される RSVP ダイヤル後遅延タイマーの値を設定するための **rsvp post-dial-delay** コマンドが導入されました。 このタイマーは、各 PfR 学習サイクルの開始時に境界ルータで更新されます。また、ルーティング パスが RSVP に戻るまでの遅延（ミリ秒単位）を決定します。 PfR と RSVP の統合がイネーブルになっている場合、PfR は遅延タイマーの期限が切れる前に、学習するすべての RSVP フローの最良のパスを見つけようとします。 現在のパスが最良のパスでない場合、PfR は新しいパスをインストールしようとします。 RSVP は、Fast Local Repair（FLR）のケースとしてこのポリシー ルートの挿入に対応し、新しい予約パスを再度シグナリングします。

代替予約パスに対する RSVP シグナリングの再試行

PfR RSVP コントロール機能では、新しいコマンド **rsvp signaling-retries** が導入されました。このコマンドはマスター コントローラ上で設定され、RSVP 予約がエラー状態を返したときに代替予約パスを提供するように PfR に指示するために使用されます。 代替パスが PfR によって提供されると、RSVP は予約信号を再送信できます。 デフォルトの再試行回数は 0 に設定されます。シグナリングの再試行は許可されず、予約障害が発生すると予約エラー メッセージが送信されます。

PfR コマンドからのパフォーマンス統計情報

PfR マスター コントローラは、境界ルータを経由する IP トラフィックを学習し、監視します。マスター コントローラは、設定されたポリシー、および境界ルータから受信したパフォーマンス情報に基づいてトラフィック フローの最良の出口を選択します。 次のコマンドを使用して、マスター コントローラによって収集されたパフォーマンス データの一部を確認できます。

- **show pfr master active-probes**
- **show pfr master border**
- **show pfr master exits**
- **show pfr master statistics**
- **show pfr master traffic-class**
- **show pfr master traffic-class performance**

これらのコマンドはすべて、マスター コントローラで入力します。一部のコマンドには、出力をフィルタリングするためのキーワードと引数があります。 これらのコマンドの詳細については、『Cisco IOS Performance Routing Command Reference』を参照してください。

PfR RSVP コントロールの設定方法

学習リストを使用した PfR RSVP コントロールの設定

RSVP フローに基づき自動的に学習され、プレフィックス リストによってフィルタリングされるトラフィック クラスを含む学習リストを定義するには、マスターコントローラでこのタスクを実行します。 このタスクの目的は、RSVP フローから学習するすべてのビデオ トラフィックを最適化することです。

ビデオ トラフィック クラスは、10.100.0.0/16 または 10.200.0.0/16 と一致するプレフィックスとして定義され、POLICY_RSVP_VIDEO という名前の PfR ポリシーが作成されます。

学習リストは、PfR マップを使用して PfR ポリシー内で参照され、**policy-rules** (PfR) コマンドを使用してアクティブ化されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. **pfr master**
5. **policy-rules** *map-name*
6. **rsvp signaling-retries** *number*
7. **rsvp post-dial-delay** *msecs*
8. **learn**
9. **list seq** *number* **refname** *refname*
10. **traffic-class prefix-list** *prefix-list-name* [**inside**]
11. **rsvp**
12. **exit**
13. ステップ 9 ～ 12 を繰り返して、追加の学習リストを設定します。
14. **exit**
15. 必要に応じて、グローバル コンフィギュレーション モードに戻るには**exit** コマンドを使用します。
16. **pfr-map** *map-name sequence-number*
17. **match pfr learn list** *refname*
18. **set mode route control**
19. **set resolve equivalent-path-round-robin**
20. **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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}	学習するプレフィックスをフィルタリングするための IP プレフィックス リストを作成します。

	コマンドまたはアクション	目的
	例： `Router(config)# ip prefix-list RSVP_VIDEO seq 10 permit 10.100.0.0/16`	• IPプレフィックス リストを学習リスト コンフィギュレーション モードで使用すると、学習される IP アドレスをフィルタリングすることができます。 • 例では、RSVP_VIDEO という名前の IP プレフィックス リストが作成され、PfR で 10.100.0.0/16 プレフィックスのプロファイリングが行われます。
ステップ 4	**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、マスター コントローラとして Cisco ルータを設定し、マスター コントローラ ポリシーおよびタイマー設定を設定します。
ステップ 5	**policy-rules** *map-name* 例： `Router(config-pfr-mc)# policy-rules POLICY_RSVP_VIDEO`	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、PfR マップを選択し設定を適用します。 • アクティブ化する PfR マップ名を指定するには、*map-name* 引数を使用します。 • 例では、このタスクで設定した学習リストを含んでいる POLICY_RSVP_VIDEO という名前の PfR マップが適用されます。
ステップ 6	**rsvp signaling-retries** *number* 例： `Router(config-pfr-mc)# rsvp signaling-retries 1`	予約エラー状態が検出されたときに、PfR が RSVP 予約に提供する代替パスの数を指定します。 • 代替パスの数を指定するには、*number* 引数を使用します。 • このタスクの設定例は、RSVP シグナリングの再試行に対する代替パスの数を 1 に設定するように PfR を設定する方法を示しています。
ステップ 7	**rsvp post-dial-delay** *msecs* 例： `Router(config-pfr-mc)# rsvp post-dial-delay 100`	RSVP ダイヤル後遅延タイマーを設定して、PfR が RSVP にルーティング パスを返すまでの遅延時間を設定します。 • ミリ秒単位で遅延時間を指定するには、*msecs* 引数を使用します。 • このタスクの設定例は、RSVP ダイヤル後遅延タイマーを 100 ミリ秒に設定するように PfR を設定する方法を示しています。

	コマンドまたはアクション	目的
ステップ 8	**learn** 例： `Router(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、トラフィック クラスを自動的に学習します。
ステップ 9	**list seq** *number* **refname** *refname* 例： `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_RSVP_VIDEO`	PfR 学習リストを作成し、学習リスト コンフィギュレーション モードを開始します。 • 学習リスト基準が適用される順番の決定に使用されるシーケンス番号を指定するには、**seq** キーワードおよび *number* 引数を使用します。 • 学習リストの参照名を指定するには、**refname** キーワードおよび *refname* 引数を使用します。 • 例では、LEARN_RSVP_VIDEO という名前の学習リストが作成されます。
ステップ 10	**traffic-class prefix-list** *prefix-list-name* [**inside**] 例： `Router(config-pfr-mc-learn-list)# traffic-class prefix-list RSVP_VIDEO`	送信先プレフィックスのみに基づき、トラフィックを自動的に学習するようにマスター コントローラを設定します。 • プレフィックス リストを指定するには、*prefix-list-name* 引数を使用します。 • 例では、RSVP_VIDEO という名前のプレフィックス リストを使用してトラフィック クラスが定義されます。
ステップ 11	**rsvp** 例： `Router(config-pfr-mc-learn-list)# rsvp`	RSVP フローに基づいてトップ プレフィックスを学習するように、マスター コントローラを設定します。 • このコマンドをイネーブルにすると、マスター コントローラでは最高アウトバウンド スループットに従ってすべての境界ルータのトップ プレフィックスが学習されます。 • 例では、LEARN_RSVP_VIDEO 学習リストの RSVP フローに基づいてトップ プレフィックスを学習するように、マスター コントローラが設定されます。
ステップ 12	**exit** 例： `Router(config-pfr-mc-learn-list)# exit`	学習リスト コンフィギュレーション モードを終了し、PfR Top Talker/Top Delay 学習コンフィギュレーション モードに戻ります。
ステップ 13	ステップ 9 ～ 12 を繰り返して、追加の学習リストを設定します。	--

	コマンドまたはアクション	目的
ステップ 14	**exit** 例： `Router(config-pfr-mc-learn)# exit`	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、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 15	必要に応じて、グローバル コンフィギュレーション モードに戻るには**exit** コマンドを使用します。	--
ステップ 16	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map POLICY_RSVP_VIDEO 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 例では、POLICY_RSVP_VIDEO という名前の PfR マップが作成されます。
ステップ 17	**match pfr learn list** *refname* 例： `Router(config-pfr-map)# match pfr learn list LEARN_RSVP_VIDEO`	学習済みの PfR プレフィックスに一致させるために、PfR マップ内で match 句エントリを作成します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、LEARN_RSVP_VIDEO という名前の PfR 学習リストに定義されている基準を使用して、トラフィック クラスが定義されます。 （注） ここでは、このタスクに関連する構文だけを使用しています。
ステップ 18	**set mode route control** 例： `Router(config-pfr-map)# set mode route control`	一致したトラフィックのルート制御を設定するために、set 句エントリを作成します。 • 制御モードでは、マスター コントローラが監視対象プレフィックスを分析し、ポリシー パラメータに基づいて変更を実行します。
ステップ 19	**set resolve equivalent-path-round-robin** 例： `Router(config-pfr-map)# set resolve equivalent-path-round-robin`	set 句エントリを作成して、同等パス ラウンドロビン リゾルバを使用することを指定します。 • このタスクでは、ランダム リゾルバの代わりに、同等パス ラウンドロビン リゾルバが同等パス間での選択に使用されます。

	コマンドまたはアクション	目的
ステップ 20	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

PfR RSVP コントロール情報の表示

PfR RSVP コントロール機能はマスター コントローラ上に設定されますが、実際にパフォーマンス情報を収集するのは境界ルータです。**show** および **debug** コマンドを使用して、マスター コントローラと境界ルータの両方の RSVP 情報を表示できます。 このタスクの最初のいくつかのコマンドは、マスターコントローラで入力します。残りのコマンドには、アプリケーショントラフィックが経由する境界ルータに移動するためのステップがあります。 **show** コマンドと **debug** コマンドは、任意の順序で入力できます。

手順の概要

1. **enable**
2. **show pfr master traffic-class** [**rsvp**] [**active** | **passive** | **status**] [**detail**]
3. **show pfr master policy** [*sequence-number* | *policy-name* | **default** | **dynamic**]
4. **debug pfr master rsvp**
5. RSVP トラフィックが経由する境界ルータに移動します。
6. **enable**
7. **show pfr border rsvp**
8. **show pfr border routes rsvp-cache**
9. **debug pfr border rsvp**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr master traffic-class** [**rsvp**] [**active** | **passive** | **status**] [**detail**]
このコマンドは、RSVP トラフィック クラスとして学習される PfR トラフィック クラスに関する情報を表示するために使用します。

例：

```
Router# show pfr master traffic-class rsvp

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
-------------------------------------------------------------------------------
10.1.0.10/32              N    N  tcp       75-75       75-75 10.1.0.12/32
                          INPOLICY       @0         10.1.0.24 Tu24            PBR
               U        U        0        0        0        0        0        0
               1        1        0        0        N        N        N        N
```

ステップ 3 **show pfr master policy** [*sequence-number* | *policy-name* | **default** | **dynamic**]

このコマンドを使用すると、ポリシー情報が表示されます。 次の例では、**dynamic** キーワードを使用して、プロバイダー アプリケーションがダイナミックに作成したポリシーを表示します。 RSVP コンフィギュレーション コマンドに注意してください。

例：

```
Router# show pfr master policy dynamic

Dynamic Policies:

  proxy id 10.3.3.3
  sequence no. 18446744069421203465, provider id 1001, provider priority 65535
    host priority 65535, policy priority 101, Session id 9
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
  proxy id 10.3.3.3
  sequence no. 18446744069421269001, provider id 1001, provider priority 65535
    host priority 65535, policy priority 102, Session id 9
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
```

```
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
  proxy id 10.3.3.4
  sequence no. 18446744069421334538, provider id 1001, provider priority 65535
    host priority 65535, policy priority 103, Session id 10
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
```

ステップ 4 **debug pfr master rsvp**

PfR マスター コントローラ上の PfR RSVP イベントに関するデバッグ情報を表示します。

例：

```
Router# debug pfr master rsvp

Jan 23 21:18:19.439 PST: PFR_MC_RSVP: recvd a RSVP flow
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Processing 1 rsvp flows
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Resolve: src: 10.1.0.12 dst: 10.1.25.19 pr
oto: 17 sport min: 1 sport max: 1 dport min: 1 dport max: 1 from BR 10.1.0.23
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Marking: 10.1.0.23, FastEthernet1/0
Jan 23 21:18:19.439 PST: %OER_MC-5-NOTICE: Uncontrol Prefix 10.1.25.19/32, Probe frequency changed
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Marked: 10.1.0.23, FastEthernet1/0 as current
Jan 23 21:18:19.467 PST: PFR_MC_RSVP: recv new pool size
Jan 23 21:18:19.467 PST: PFR_MC_RSVP: Update from 10.1.0.23, Fa1/0: pool 8999
Jan 23 21:18:20.943 PST: %OER_MC-5-NOTICE: Prefix Learning WRITING DATA
Jan 23 21:18:21.003 PST: %OER_MC-5-NOTICE: Prefix Learning STARTED
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: RSVP resolver invoked
Jan 23 21:18:22.475 PST: PFR RSVP MC:  10.1.25.19/32 Appl 17 [1, 1][1, 1] 0:
        BR 10.1.0.23, Exit Fa1/0, is current exit
Jan 23 21:18:22.475 PST: PFR RSVP MC:  10.1.25.19/32 Appl 17 [1, 1][1, 1] 0:
        BR 10.1.0.23, Exit Fa1/0, is current exit
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.23 Exit:Fa1/0pool size : 8999
est : 8999 tc->tspec: 1, fit: 8999
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.24 Exit:Tu24pool size : 9000
est : 9000 tc->tspec: 1, fit: 8999
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.23 Exit:Fa1/1pool size : 9000
est : 9000 tc->tspec: 1, fit: 8999
```

ステップ 5 RSVP トラフィックが経由する境界ルータに移動します。

ステップ 6 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 7 **show pfr border rsvp**

次の例は、PfR 境界ルータの RSVP ダイヤル後タイムアウト タイマーおよびシグナリングの再試行の現在値を表示します。

例：

```
Router# show pfr border rsvp

PfR BR RSVP parameters:
       RSVP Signaling retries:         1
       Post-dial-timeout(msec):        0
```

ステップ 8 **show pfr border routes rsvp-cache**

このコマンドは、PfR が認識しているすべての RSVP パスを表示するために使用します。

（注） この例に適した構文のみ表示されています。

例：

```
Router# show pfr border routes rsvp-cache

SrcIP       DstIP       Protocol Src_port Dst_port Nexthop       Egress I/F PfR/RIB
----------- ----------- -------- -------- -------- ------------- ---------- --------
10.1.25.19  10.1.35.5   UDP      1027     1027     10.1.248.5    Gi1/0       RIB*
10.1.0.12   10.1.24.10  UDP      48       48       10.1.248.24   Gi1/0       PfR*
10.1.0.12   10.1.42.19  UDP      23       23       10.1.248.24   Gi1/0       PfR*
10.1.0.12   10.1.18.10  UDP      12       12       172.16.43.2   Fa1/1       PfR*
```

ステップ 9 **debug pfr border rsvp**

PfR 境界ルータ上の PfR RSVP イベントに関するデバッグ情報を表示します。

例：

```
Router# debug pfr border rsvp

Jan 23 21:18:19.434 PST: PfR RSVP:RESOLVE called for src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1; tspec 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:Searching flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:Add flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:Searching flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:successfully added the flow to the db
Jan 23 21:18:19.434 PST: PfR RSVP:flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1 lookup; topoid: 0
Jan 23 21:18:19.434 PST: PfR RSVP(det):ret nh: 10.185.252.1, idb: 35
Jan 23 21:18:19.434 PST: PfR RSVP:Adding new context
Jan 23 21:18:19.434 PST: PfR RSVP(det):Num contexts: 0
Jan 23 21:18:19.434 PST: PfR RSVP(det):Num contexts: 1
Jan 23 21:18:19.434 PST: PfR RSVP:flow src: 10.1.0.12 dst: 10.1.25.19
```

```
 proto: 17 sport: 1 dport: 1 now pending notify
Jan 23 21:18:19.434 PST: PfR RSVP:Resolve on flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:Filtering flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
```

PfR パフォーマンスおよび統計情報の表示

このタスクのコマンドは、PfR トラフィック クラスまたは出口に関する詳細なパフォーマンスまたは統計情報を表示するために入力します。 コマンドは、各セクション内で任意の順序で入力できます。

手順の概要

1. **enable**
2. **show pfr master traffic-class** [**policy** *policy-seq-number* | *rc-protocol* | **state** {**hold**| **in** | **out** | **uncontrolled**}] [**detail**]
3. **show pfr master traffic-class performance** [**application** *application-name* [*prefix*] | **history** [**active** | **passive**] | **inside** | **learn** [**delay** | **inside** | **list** *list-name* | **rsvp** | **throughput**] | **policy** *policy-seq-number* | *rc-protocol* | **state** {**hold** | **in** | **out** | **uncontrolled**} | **static**] [**detail**]
4. **show pfr master exits**
5. **show pfr master active-probes** [**assignment** | **running**] [**forced** *policy-sequence-number* | **longest-match**]
6. **show pfr master border** [*ip-address*] [**detail** | **report** | **statistics** | **topology**]
7. **show pfr master statistics** [**active-probe** | **border** | **cc** | **exit** | **netflow** | **prefix** | **process** | **system** | **timers**]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr master traffic-class** [**policy** *policy-seq-number* | *rc-protocol* | **state** {**hold**| **in** | **out** | **uncontrolled**}] [**detail**]

このコマンドは、PfR マスター コントローラにより監視および制御されるトラフィック クラスに関する情報を表示するときに使用されます。 この例では、ポリシー準拠状態にあるトラフィック クラスのみ表示するように出力をフィルタリングするために、**state in** キーワードが使用されています。

例：

```
Router# show pfr master traffic-class state in

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
```

```
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
-------------------------------------------------------------------------------
10.1.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.1 Et0/0           BGP
              14       14        0        0        0        0       78        9
               N        N        N        N        N        N

10.2.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.2 Et0/0           BGP
              14       14        0        0        0        0       75        9
               N        N        N        N        N        N

10.3.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.3 Et0/0           BGP
              14       14        0        0        0        0       77        9
               N        N        N        N        N        N

10.4.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.4 Et0/0           BGP
              14       14        0        0        0        0       77        9
               N        N        N        N        N        N

10.1.8.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.3 Et0/0           BGP
              14       14    62500    73359        0        0        5        1
               N        N        N        N        N        N

10.1.1.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.2 Et0/0           BGP
              14       14     9635     9386     1605     1547       34        4
               N        N        N        N        N        N
```

ステップ 3 **show pfr master traffic-class performance** [**application** *application-name* [*prefix*] | **history** [**active** | **passive**] | **inside** | **learn** [**delay** | **inside** | **list** *list-name* | **rsvp** | **throughput**] | **policy** *policy-seq-number* | *rc-protocol* | **state** {**hold** | **in** | **out** | **uncontrolled**} | **static**] [**detail**]

このコマンドは、PfR マスター コントローラによって監視および制御されるトラフィック クラスに関するパフォーマンス情報を表示します。

（注） この例に適用できる構文のみ表示されています。

例：

次の出力は、直前の 60 分間の現在の出口におけるトラフィック クラスのパフォーマンス履歴を示しています。

```
Router# show pfr master traffic-class performance history

Prefix: 10.70.0.0/16
efix performance history records
 Current index 1, S_avg interval(min) 5, L_avg interval(min) 60

Age       Border          Interface       OOP/RteChg Reasons
Pas: DSum  Samples  DAvg  PktLoss  Unreach   Ebytes   Ibytes     Pkts    Flows
Act: Dsum Attempts  DAvg    Comps  Unreach   Jitter LoMOSCnt   MOSCnt
00:00:33  10.1.1.4        Et0/0
```

```
Pas: 6466      517    12        2       58  3400299   336921    10499     2117
Act:    0        0     0        0        0        N        N        N
00:01:35  10.1.1.4        Et0/0
Pas:15661     1334    11        4      157  4908315   884578    20927     3765
Act:    0        0     0        0        0        N        N        N
00:02:37  10.1.1.4        Et0/0
Pas:13756     1164    11        9      126  6181747   756877    21232     4079
Act:    0        0     0        0        0        N        N        N
00:03:43  10.1.1.1        Et0/0
Pas:14350     1217    11        6      153  6839987   794944    22919     4434
Act:    0        0     0        0        0        N        N        N
00:04:39  10.1.1.3        Et0/0
Pas:13431     1129    11       10      122  6603568   730905    21491     4160
Act:    0        0     0        0        0        N        N        N
00:05:42  10.1.1.2        Et0/0
Pas:14200     1186    11        9      125  4566305   765525    18718     3461
Act:    0        0     0        0        0        N        N        N
00:06:39  10.1.1.3        Et0/0
Pas:14108     1207    11        5      150  3171450   795278    16671     2903
Act:    0        0     0        0        0        N        N        N
00:07:39  10.1.1.4        Et0/0
Pas:11554      983    11       15      133  8386375   642790    23238     4793
Act:    0        0     0        0        0        N        N        N
```

ステップ 4 **show pfr master exits**

このコマンドは、PfR トラフィック クラスに使用された出口に関する情報（境界ルータの IP アドレスとインターフェイス、出口のポリシー、および出口のパフォーマンスデータを含む）を表示するために使用します。 次の例は、RSVP プール情報を示しています。

例：

```
Router# show pfr master exits

PfR Master Controller Exits:

General Info:
=============
  E - External
  I - Internal
  N/A - Not Applicable
                                                                                  Up/
   ID Name         Border          Interface   ifIdx IP Address      Mask Policy      Type Down
  --- ------------ --------------- ----------- ----- --------------- ---- ----------- ---- ----
    6              10.1.0.23       Fa1/0           9 10.185.252.23     27 Util          E  UP
    5              10.1.0.23       Fa1/1          10 172.16.43.23      27 Util          E  UP
    4              10.1.0.24       Tu24           33 10.20.20.24       24 Util          E  UP

Global Exit Policy:
===================
    Range Egress:      In Policy - No difference between exits - Policy 10%
   Range Ingress:      In Policy - No difference between entrances - Policy 0%
     Util Egress:      In Policy
    Util Ingress:      In Policy
            Cost:      In Policy

Exits Performance:
==================
                  Egress                                          Ingress
    ------------------------------------------------- -----------------------------------
 ID Capacity  MaxUtil    Usage   %      RSVP POOL    OOP Capacity  MaxUtil    Usage   %  OOP
 --- -------- -------- -------- --- -------------- ----- -------- -------- -------- --- -----
  6   100000    90000       66   0           9000    N/A   100000   100000       40   0  N/A
  5   100000    90000       34   0           8452    N/A   100000   100000       26   0  N/A
  4   100000    90000      128   0           5669    N/A   100000   100000      104   0  N/A

TC and BW Distribution:
=======================
                      # of TCs                 BW (kbps)            Probe   Active
```

```
     Name/ID   Current Controlled InPolicy    Controlled       Total  Failed  Unreach
                                                                      (count) (fpm)
        ----   --------------------------   ----------------------  ------  --------
           6        0          0        0            0             66       0          0
           5      548        548      548            0             34       0          0
           4     3202       3202     3202            0            128       0          0

Exit Related TC Stats:
======================
                              Priority
                            highest       nth
                           ------------------
  Number of TCs with range:        0         0
   Number of TCs with util:        0         0
   Number of TCs with cost:        0         0

       Total number of TCs:     3800
```

ステップ 5 **show pfr master active-probes** [**assignment** | **running**] [**forced** *policy-sequence-number* | **longest-match**]

次の例は、作成済みまたは実行中のすべてのプローブのステータスを示しています。

例：

```
Router# show pfr master active-probes running

PfR Master Controller running probes:

Border          Interface   Type     Target         TPort Codec    Freq Forced Pkts DSCP
                                                                      (Pol
                                                                       Seq)
--------------- ----------- -------- -------------- ----- -------- ---- ------ ---- ----
10.100.100.200 Ethernet1/0 tcp-conn 10.100.200.100 65535 g711alaw 10   20     100  ef
10.2.2.3       Ethernet1/0 tcp-conn 10.1.5.1       23    N        56   10     1    defa
10.1.1.1       Ethernet1/0 tcp-conn 10.1.5.1       23    N        30   N      1    defa
10.1.1.2       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
10.2.2.3       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
10.1.1.1       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
```

ステップ 6 **show pfr master border** [*ip-address*] [**detail** | **report** | **statistics** | **topology**]

このコマンドは、マスターコントローラで入力すると、すべての境界ルータに関する統計情報を表示します。

例：

```
Router# show pfr master border statistics

PFR Master Controller Border
 MC Version: 2.3
 Keepalive : 5 second
 Keepalive : DISABLED

                                                    Last
Border           Status Up/Down UpTime   AuthFail  Receive  Version
---------------- ------ ------- -------- --------  -------- -------
10.200.200.200   ACTIVE UP      03:12:12        0  00:00:04 2.2
10.1.1.2         ACTIVE UP      03:10:53        0  00:00:10 2.2
10.1.1.1         ACTIVE UP      03:12:12        0  00:01:00 2.2

Border Connection Statistics
============================

                         Bytes         Bytes    Msg    Msg    Sec Buf
Border                    Sent         Recvd   Sent  Recvd Bytes Used
---------------- -------------- ------------- ------ ------ ----------
10.200.200.200           345899        373749      5     10          0
```

```
10.1.1.2                345899        373749      5     10          0
10.1.1.1                345899        373749      5     10          0

                 Socket Invalid   Context
Border           Closed Message Not Found
---------------- ------ ------- ---------
10.200.200.200        5      10       100
10.1.1.2              5      10       100
10.1.1.1              5      10       100
```

ステップ 7 **show pfr master statistics** [**active-probe** | **border** | **cc** | **exit** | **netflow** | **prefix** | **process** | **system** | **timers**]

このコマンドは、マスター コントローラの統計情報を表示します。 表示情報をフィルタリングするにはキーワードを使用します。 次の例では、**system** キーワードで PfR システムの統計情報を表示しています。

例：

```
Router# show pfr master statistics system

   Active Timers: 14
    Total Traffic Classes = 65, Prefixes = 65, Appls =0
   TC state:
    DEFAULT = 0, HOLDDOWN = 11, INPOLICY = 54, OOP = 0, CHOOSE = 0,
    Inside = 1, Probe all = 0, Non-op = 0, Denied = 0
    Controlled 60, Uncontrolled 5, Alloced 65, Freed 0, No memory 0
   Errors:
    Invalid state = 0, Ctrl timeout = 0, Ctrl rej = 0, No ctx = 7616,
    Martians = 0
    Total Policies = 0
    Total Active Probe Targets = 325
    Total Active Probes Running = 0
   Cumulative Route Changes:
    Total  : 3246
    Delay  : 0
    Loss   : 0
    Jitter : 0
    MOS    : 0
    Range  : 0
    Cost   : 0
    Util   : 0
   Cumulative Out-of-Policy Events:
    Total  : 0
    Delay  : 0
    Loss   : 0
    Jitter : 0
    MOS    : 0
    Range  : 0
    Cost   : 0
    Util   :
```

PfR RSVP コントロールの設定例

RSVP フローを使用したトラフィック クラスの定義例

マスター コントローラ上で設定された次の例では、RSVP フローに基づき自動的に学習され、プレフィックスリストによってフィルタリングされるトラフィック クラスを含む学習リストが定義

されます。 この例の目的は、POLICY_RSVP_VIDEO という名前のポリシーを使用して、すべてのビデオ トラフィックを最適化することです。RSVP_VIDEO トラフィック クラスは、10.100.0.0/16 または 10.200.0.0/16 と一致するプレフィックスとして定義され、RSVP フローから学習されます。

次の例では、RSVP トラフィック フローに基づきプレフィックス学習が設定されます。

```
ip prefix-list RSVP_VIDEO permit seq 10 10.100.0.0/16
ip prefix-list RSVP_VIDEO permit seq 20 10.200.0.0/16
pfr master
 policy-rules POLICY_RSVP_VIDEO
 rsvp signaling-retries 1
 rsvp post-dial-delay 100
 learn
 list seq 10 refname LEARN_RSVP_VIDEO
 traffic-class prefix-list RSVP_VIDEO
 rsvp
 exit
 exit
pfr-map POLICY_RSVP_VIDEO 10
 match learn list LEARN_RSVP_VIDEO
 set mode route control
 set resolve equivalent-path-round-robin
 end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール

関連項目	マニュアル タイトル
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR RSVP コントロールの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *16* : *PfR RSVP* コントロールの機能情報

機能名	リリース	機能情報
PfR RSVP コントロール	Cisco IOS XE Release 3.4S	PfR RSVP コントロール機能は、アプリケーション アウェア PfR 技術を使用した RSVP フローの最適化をサポートします。 この機能により、次のコマンドが導入または変更されました。**debug pfr border rsvp**、**debug pfr master rsvp**、**rsvp (PfR)**、**rsvp post-dial-delay**、**rsvp signaling-retries**、**resolve (PfR)**、**set resolve (PfR)**、**show pfr border rsvp**、**show pfr border routes**、**show pfr master active-probes**、**show pfr master border**、**show pfr master exits**、**show pfr master policy**、**show pfr master statistics**、**show pfr master traffic-class**、および **show pfr master traffic-class performance**。

第 14 章

アプリケーション トラフィック クラスの PfR スケーリングの向上

アプリケーション トラフィック クラスの PfR スケーリングの向上機能は、各パフォーマンス ルーティング（PfR）境界ルータ（BR）でサポートされるアプリケーション トラフィック クラス（TC）の数に対するスケーリングの拡張機能を導入します。 新しい PfR およびダイナミック ルート マップ スケーリングの向上により、BR は最大 20,000 のアプリケーション トラフィック クラス（TC）と最大 500 のダイナミック ルート マップ シーケンスをサポートできます。 現在は、5000 のアプリケーション トラフィック クラスと 32 のルート マップ エントリのみ許可されています。 Route Processor 2 (RP2)/ESP40 では、最大 500 のブランチと 20,000 のアプリケーション トラフィック クラスを推奨します。 Route Processor 1 (RP1)/ESP10 では、最大 500 のブランチと 10,000 のアプリケーション トラフィック クラスを推奨します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

アプリケーション トラフィック クラスの PfR スケーリングの向上の概要

PfR と PBR のスケーリングの拡張機能

アプリケーション トラフィック クラスの PfR スケーリングの向上機能は、Cisco ASR 1000 シリーズ ルータ用の各パフォーマンス ルーティング（PfR）境界ルータ（BR）でサポートされるアプリケーション トラフィック クラス（TC）の数に対するスケーリングの拡張機能を導入します。 新しい PfR およびダイナミック ルート マップ スケーリングの向上により、BR は最大 20,000 のアプリケーション トラフィック クラス（TC）と最大 500 のダイナミック ルート マップ シーケンスをサポートできます。 現在は、5000 のアプリケーション トラフィック クラスと 32 のルート マップ エントリのみ許可されています。 次の表は、ルート プロセッサごとの新しい最大制限値を示しています。

表 *17*：ルート プロセッサごとの *PfR* と *PBR* のスケーリング

ルート プロセッサ	アプリケーション TC の最大数	ルート マップ エントリの最大数
RP2/ESP40	20,000	500
RP1/ESP10	10,000	500

パフォーマンス ルーティング（PfR）マスター コントローラが監視または学習するプレフィックスの最大数をより高く設定するには、**max prefix (PfR)** コマンドを使用します。 デフォルトでは、監視するプレフィックスは 5000、学習するプレフィックスは最大 2500 に設定されますが、前述の表に示されているように、これら両方の値は、ルート プロセッサのタイプに応じて最大 20,000 に設定できます。

アプリケーション トラフィック クラスの PfR スケーリングの向上の設定方法

PfR アプリケーション トラフィック クラス スケーリングの設定

パフォーマンス ルーティング（PfR）が監視または学習するアプリケーション トラフィック クラスの最大数を増やすには、マスター コントローラでこのタスクを実行します。 大規模なネットワークではスケーラブルなソリューションが要求されており、アプリケーション トラフィック クラスの PfR スケーリングの向上機能は、Cisco ASR 1000 シリーズ ルータ用の各 PfR 境界ルータ（BR）でサポートされるアプリケーション トラフィック クラスの数に対するスケーリングの拡張機能を導入します。新しいPfRおよびダイナミック ルートマップ スケーリングの向上により、BR は最大 20,000 のアプリケーション トラフィック クラスと最大 500 のダイナミック ルート マップ シーケンスをサポートできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max prefix total** *number* [**learn** *number*]
5. **end**
6. **show platform hardware qpf active feature pbr class-group** [*cg-id*] [**class** [*class-id*]]

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスターコントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 4	**max prefix total** *number* [**learn** *number*] 例： `Device(config-pfr-mc)# max prefix total 15000 learn 12000`	PfR マスター コントローラが監視または学習するプレフィックスの最大数を設定します。 • この例では、PfR は 15,000 プレフィックス（アプリケーション トラフィック クラス）を監視し、最大 12,000 プレフィックスを学習するように設定されます。
ステップ 5	**end** 例： `Device(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show platform hardware qpf active feature pbr class-group** [*cg-id*] [**class** [*class-id*]] 例： `Device# show platform hardware qpf active feature pbr class-group 2 class 6`	（任意）アクティブな Cisco QuantumFlow Processor（QFP）のポリシーベース ルーティング（PBR）クラス グループの情報を表示します。

例

次に、アクティブな Cisco Quantum Flow Processor（QFP）のポリシーベース ルーティング（PBR）クラス グループの情報を表示するために **show platform hardware qpf active feature pbr** コマンドを使用した出力例を示します。 この例では、class-group 2 とクラス ID 6 に関する情報が表示されています。

```
Device# show platform hardware qpf active feature pbr class-group 2 class 6

Class ID: 6
  hw flags enabled: action, prec
  hw flags value: (0x0000000a)
  tos: 0
  precedence: 160
  nexthop: 0.0.0.0
  adj_id: 0
  table_id: 0
  extra_action_size: 0
  cpp_num: 0
  extra_ppe_addr: 0x00000000
  stats_ppe_addr: 0x8bc6a090
```

PfR と PBR のスケーリングの拡張機能の表示と検証

パフォーマンス ルーティング（PfR）およびポリシーベース ルーティング（PBR）アプリケーション トラフィック クラスに関するプラットフォーム固有の設定および統計情報を表示するには、このタスクを実行します。 変更されたコマンドおよび既存のコマンドは、学習リストが設定されてトラフィック クラスが自動的に学習された後で、またはPfRマップを使用してトラフィック クラスが手動で設定されたときにマスターコントローラに入力できます。 コマンドは、任意の順番で入力できます。すべてのコマンドは、省略可能です。

手順の概要

1. **enable**
2. **show platform software pbr** *slot* {**active** {**class-group** {**all** | *cg-id* | **interface** {**all** | **name** *intf-name*} | **route-map** {**all** | **name** *rmap-name* | **sequence** *cgm-class-id*} | **statistics**} | **standby statistics**}
3. **show platform software route-map** {**client** | **counters** | *slot*} {**active** | **standby**} {**cgm-filter** | **feature-references** | **map** | **stats** | **summary**}
4. **show platform hardware qpf active feature pbr class-group** [*cg-id*] [**class** [*class-id*]]

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show platform software pbr** *slot* {**active** {**class-group** {**all** | *cg-id* | **interface** {**all** | **name** *intf-name*} | **route-map** {**all** | **name** *rmap-name* | **sequence** *cgm-class-id*} | **statistics**} | **standby statistics**}
このコマンドは、ポリシーベース ルーティング（PBR）情報を表示するために使用します。 次の出力例は、組み込みサービス プロセッサのもので、すべてのアクティブなルート マップの情報が示されています。

例：

```
Device# show platform software pbr fp active route-map all

Route-map: rtmap-test
CG_id: 1, AOM obj id: 278
Sequence      CGM class ID    AOM ID    Action AOM ID
10            1               327       328
Interface                          AOM id
GigabitEthernet0/0/2                 281
Route-map: test
CG_id: 2, AOM obj id: 608
Sequence      CGM class ID    AOM ID    Action AOM ID
10            2               609       610
20            3               611       612
30            4               613       614
40            5               615       616
```

```
50              6               617       618
60              7               619       620
70              8               621       622
Interface                            AOM id
GigabitEthernet0/0/0.773             630
```

ステップ 3 **show platform software route-map** {**client** | **counters** | *slot*} {**active** | **standby**} {**cgm-filter** | **feature-references** | **map** | **stats** | **summary**}

このコマンドは、Cisco ASR 1000 シリーズ ルータのルート マップ情報に関連するプラットフォーム固有の設定および統計情報を表示するために使用します。 この例では、組み込みのサービス プロセッサに関するアクティブなルート マップ機能に関する情報が表示されます。

例：

```
Device# show platform software route-map fp active feature-references

Name                    Feature     Class-group      Class       VRF id
------------------------------------------------------------------------
test                    PBR         2                0           0
rtmap-test              PBR         1                0           0
```

ステップ 4 **show platform hardware qpf active feature pbr class-group** [*cg-id*] [**class** [*class-id*]]

このコマンドは、アクティブなCisco QuantumFlow Processor（QFP）のポリシーベース ルーティング（PBR）クラス グループ情報を表示するために使用します。 次の出力例では、class-group 2 とクラス ID 6 に関する情報が表示されています。

例：

```
Device# show platform hardware qfp active feature pbr class-group 2 class 6

Class ID: 6
  hw flags enabled: action, prec
  hw flags value: (0x0000000a)
  tos: 0
  precedence: 160
  nexthop: 0.0.0.0
  adj_id: 0
  table_id: 0
  extra_action_size: 0
  cpp_num: 0
  extra_ppe_addr: 0x00000000
  stats_ppe_addr: 0x8bc6a090
```

アプリケーション トラフィック クラスの PfR スケーリングの向上の設定例

例：PfR アプリケーション トラフィック クラス スケーリングの設定

次の例では、PfR は 15,000 プレフィックス（アプリケーション トラフィック クラス）を監視し、最大 2500 プレフィックスを学習するように設定されます。

```
Device> enable
Device# configure terminal
Device(config)# pfr master
Device(config)# max prefix total 20000 learn 2500
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

アプリケーション トラフィック クラスの PfR スケーリングの向上の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *18* : アプリケーション トラフィック クラスの *PfR* スケーリングの向上の機能情報

機能名	リリース	機能情報
アプリケーション トラフィック クラスの PfR スケーリングの向上	Cisco IOS XE Release 3.8S	アプリケーション トラフィック クラスの PfR スケーリングの向上機能は、各パフォーマンス ルーティング（PfR）境界ルータでサポートされるアプリケーション トラフィック クラスの数に対するスケーリングの拡張機能を導入します。 次のコマンドが導入または変更されました。**max prefix (PfR)**、**show platform software route-map**、**show platform software pbr**、**show platform hardware qfp active feature pbr**。

第 15 章

PfR 簡素化のフェーズ 1

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 IP ルーティング テクノロジー（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Routing Information Protocol Version 2（RIPv2）、ボーダー ゲートウェイ プロトコル（BGP）など）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これら従来の IP 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、平均オピニオン評点（MOS）スコア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、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。 従来の IP ルーティング テクノロジーでは、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ています。

PfR は自動的に IP SLA または NetFlow テクノロジーをイネーブルにしますが、PfR の初期設定は、PfR ポリシー定義および多数のパフォーマンス パラメータの設定を伴うため、従来の IP ルーティング テクノロジーよりも複雑です。 シスコでは、PfR の設定の複雑さを低減するためにカスタマーからのフィードバックを使用し、カスタマーの要件に合うようにデフォルト値を調整しています。 PfR 簡素化のフェーズ 1 のプロジェクトでは、PfR 境界ルータ間のダイナミック トンネル、デフォルト値の修正、一部 CLI の削除、およびデフォルトの動作の変更を導入していいます。 これらの変更により、ネットワークに PfR を実装する前の設定手順が削減されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR 簡素化のフェーズ 1 の概要

PfR を簡素化するための CLI およびデフォルト値の変更

CSCtr26978 では、PfR の設定を簡素化するために設計された一連の CLI およびデフォルト値の変更が導入されました。 一部のコマンドとキーワードは削除され、カスタマー環境を反映するようにデフォルトが変更されました。

デフォルトでルート制御を適用

カスタマーのフィードバックに対応して、CSCtr26978 では、**mode route control** コマンドが **mode route observe** コマンドの代わりにデフォルトの動作になっています。 制御モードでは、マスター コントローラは境界ルータからの情報を調整し、ポリシーを決定します。マスター コントローラは、デフォルトおよびユーザ定義のポリシーに基づきプレフィックスと出口を監視し、プレフィックスを最適化し、最良の出口を選択するための変更を実装します。

パッシブに監視し、変更を加えずにレポートを作成する場合でも、観察モードを使用するように PfR を設定できます。 観察モードでは、マスター コントローラはデフォルトおよびユーザ設定のポリシーに基づいてプレフィックスと出口リンクを監視し、ネットワークのステータスと必要な決定事項をレポートします。ただし、変更は何も実装されません。

Mode Verify Bidirectional CLI に対するデフォルトの変更

カスタマーのフィードバックに対応して、CSCtr26978 では、双方向トラフィックの確認をディセーブルにするようにデフォルトの動作が変更されています。 双方向トラフィックを確認する必要がある場合は、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、**mode verify bidirectional** コマンドを設定します。

PfR を簡素化するための CLI デフォルト値の変更

コマンド	CSCtr26978 より前のデフォルト値	CSCtr26978 以降のデフォルト値
backoff	300、3000、300 秒	90、900、90 秒
holddown	300 秒	90 秒
max-xmit-utilization	75 %	90%
monitor-period	5 分	1 分
periodic-interval	120 分	0 分

PfR API およびプロキシ CLI の削除

PfR アプリケーション プログラミング インターフェイス（API）およびプロキシ プロセスに関係するすべての CLI コマンドと機能は、PfR を簡素化するために削除されました。 CSCtr26978 では、次の CLI コマンドが削除されました。

- **api provider (PfR)**
- **debug pfr api**
- **host-address (PfR)**
- **show api provider (PfR)**
- **show pfr proxy**

OER CLI の削除

ほとんどのイメージでは、Optimized Edge Routing（OER）構文は PfR 構文で置き換えられていますが、OER 構文は依然として認識されます。 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。 CSCtr26978 では、OER 構文は削除されています。

出口選択モード CLI の削除

ほとんどのカスタマーの導入では、パッシブ モニタリング モードでの select-exit best の出口選択の使用は推奨しません。これは、すべてのリンクが検査されるまでに統計情報が変化していて、決定が正確でない可能性があるためです。 PfR の設定を簡素化するために、CSCtr26978 では、最初のポリシー準拠リンクが選択される select-exit good がデフォルトの動作になっています。 **mode select-exit** コマンドと **best** および **good** キーワードは削除されました。

リンク グループおよびリゾルバのロード バランシングの変更

CSCtr33991 では、PfR の設定と理解を容易にするために、PfR リンク グループおよびリゾルバの動作に対する変更が導入されました。 範囲リゾルバとリンクのグループ化を同時に設定する際の制限も削除されました。 リンク グループの設定を認識することなく、すべてのリンクでロード バランシングが実行されます。 リンク グループにより、出口リンクのグループを優先リンク セットとして、または PfR 用フォールバック リンク セットとして定義し、PfR ポリシーで指定されたトラフィック クラスを最適化する際に使用できるようになりました。

さらに PfR を簡素化するために、CSCtr33991 では、範囲リゾルバがパフォーマンス リゾルバ後に考慮される動作（遅延、スループット、損失など）を変更しました。

（注） コスト リゾルバはパフォーマンス リゾルバと共に設定することはできません。

遅延リゾルバ、範囲リゾルバ、および使用率リゾルバの変更

CSCtr3399 より前	CSCtr3399 以降
使用率リゾルバおよび範囲リゾルバのサポート。	CSCtr33991 では、使用率リゾルバおよび範囲リゾルバのサポートをディセーブルにするために、**resolve** および **set resolve** コマンドの **range** および **utilization** キーワードが削除されました。
遅延リゾルバ、範囲リゾルバ、および使用率リゾルバは、デフォルト グローバル ポリシーのデフォルト リゾルバです。	PfR は自動的にロード バランシングを実行します。デフォルトのリゾルバは、デフォルト グローバル ポリシーから削除されました。

パフォーマンス リゾルバとリンク グループのロード バランシング

PfR が使用可能な出口間でのトラフィックのロード バランシングを実行する前に、設定済みのパフォーマンス リゾルバ（遅延や損失など）および設定済みのリンク グループを検討するためのルールが CSCtr33991 で導入されました。 ルールは、次の順序で評価されます。

1. パフォーマンス リゾルバが設定されておらず、リンク グループが使用されていない場合、PfR はすべてのリンク間のロード バランシングを自動的に実行します。
2. パフォーマンス リゾルバが設定されておらず、リンク グループが使用されている場合、PfR はプライマリ リンク グループ内のロード バランシングを自動的に実行します。
3. パフォーマンス リゾルバが設定されていて、リンク グループが使用されていない場合、PfR はそれらのパフォーマンス リゾルバの後に認定されたリンク間のロード バランシングを自動的に実行します。

4 パフォーマンス リゾルバが設定されていて、リンク グループが使用されている場合、PfR はプライマリ リンク グループ内の認定されたリンク間のロード バランシングを自動的に実行します。

リンク グループ内のロード バランシング

CSCtr33991 では、ある出口の負荷を他のすべての出口と比較して、出口のポリシー違反（OOP）範囲をトリガーする動作が、ある出口の負荷を同じリンク グループ内のすべての出口と比較するように変更されました。

PfR 管理対象のすべての出口リンクの最大使用率（ソフト制限）は、PfR がリゾルバを呼び出す前にチェックされ、ソフト制限未満の出口がない場合、出口選択はソフト制限を無視して実行されます。

トラフィック負荷のバランスをとるためにトラフィック クラスを移動する既存の動作は、トラフィック負荷のバランスをとるためにリンク グループ（プライマリまたはフォールバック）内のトラフィック クラスを移動する機能に置き換えられました。

パフォーマンス リゾルバが設定されている場合は、次のルールが指定された順序で適用されます。

1 1つの認定されたリンクのみプライマリ グループに含まれている場合、このリンクにトラフィック クラスを移動します。

2 複数の認定されたリンクがプライマリ グループに含まれている場合、トラフィック クラスを移動し、これらのリンク間でロード バランシングを実行します。

3 複数の認定されたリンクがフォールバック グループに含まれている場合、フォールバック グループ リンクのいずれかにトラフィック クラスを移動します。

4 認定されたリンクがプライマリ グループにもフォールバック グループも含まれていない場合、トラフィック クラスを移動しません。

5 プライマリまたはフォールバック リンク グループの最大使用率（ソフト制限）未満のリンクがない場合、ソフト制限を無視して、最良のリンクにトラフィック クラスを移動します。

パフォーマンス リゾルバが設定されていない場合は、次のルールが指定された順序で適用されます。

1 複数の認定されたリンクがプライマリ グループの最大使用率未満の場合、プライマリ グループ内のそれらのリンク間でロード バランシングを実行します。

2 複数の認定されたリンクがフォールバック グループに含まれている場合、フォールバック グループ リンクのいずれかにトラフィック クラスを移動します。

3 プライマリまたはフォールバック リンク グループの最大使用率（ソフト制限）未満のリンクがない場合、プライマリ グループ リンク間でロード バランシングを実行します。

スループットの学習の自動イネーブル化

PfR の設定を簡素化するため、CSCtr2697 ではデフォルトで、スループットベースの学習を使用する PfR 学習モードがイネーブルになっています。

カスタマーからのフィードバックを受け、デフォルトの定期的な間隔は 120 分から 90 分に変更され、デフォルトの監視期間は 5 分から 1 分に変更されました。

PfR 学習モードの自動イネーブル化は、手動設定を希望する場合は、**no learn** コマンドを使用してオフにできます。

親ルートが存在しない場合の自動 PBR ルート制御

PfR マスター コントローラ（MC）が BGP プロトコルを使用してプレフィックスを制御することを決定した場合（たとえば、選択した PfR 境界ルータ（BR）に制御要求を送信する場合）。 MC は BR から正常な制御通知を受信すると、他のすべての BR にプレフィックスを除外するように通知します。 一部の BR には、このプレフィックスへの同じプロトコル経由での親ルートがない場合があります。 プレフィックスの親ルートが存在しない場合、これは RIB の不一致として検出され、プレフィックスはデフォルト状態に移動し、再度制御手順が開始されます。

PfR を簡素化するために、CSCtr26978 では、親ルートが検出されない場合の新しい動作が導入されました。 この状況では、PfR は、BGP、EIGRP、スタティック、および PBR の順序で他のすべてのルーティングプロトコルを試行する代わりに、ダイナミックなポリシーベースルーティング（PBR）を使用するように自動的に切り替えます。 CSCtr26978 では、既存の **mode route protocol pbr** コマンドの動作はデフォルトでイネーブルになっています。 **no mode route protocol pbr** コマンドの設定では、トラフィック クラスを最初に制御解除状態に設定します。PfR は次に単一のプロトコルを使用して、BGP、EIGRP、スタティック、および PBR の順序でトラフィック クラスを制御します。

PfR のダイナミックな PBR のサポート

PfR BR の自動隣接機能により、ダイナミックな PBR のサポートが導入されています。 ダイナミック ルート マップでは、インターフェイスとネクスト ホップ情報の両方に対する PBR の要件は単一の set 句で PfR によって提供されるようになりました。 ルート マップまたはポリシー情報を表示するには、**show route-map dynamic** コマンドまたは **show ip policy** コマンドを使用します。

PfR 簡素化のフェーズ 1 の設定方法

PfR ルート観察モードのイネーブル化

CSCtr26978 では、**mode route control** コマンドの動作がデフォルトです。 デフォルトのルート制御モードの代わりにルート観察モードを使用するように PfR を設定するには、マスター コント

ローラでこのタスクを実行します。ルート観察モードでは、マスターコントローラはデフォルトおよびユーザ設定のポリシーに基づいてプレフィックスと出口リンクを監視し、ネットワークのステータスと必要な決定事項をレポートします。ただし、変更は何も実装されません。 ルート制御モードでは、マスター コントローラは境界ルータからの情報をルート観察モードと同じ方法で調整します。ただし、PfR 管理のネットワークのルーティングを変更してポリシー決定を実装するために、境界ルータにコマンドが返されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode route observe**
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**mode route observe** 例： `Router(config-pfr-mc)# mode route observe`	パッシブに監視し、変更を加えずにレポートを作成するように PfR を設定します。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

自動 PBR ルート制御のディセーブル化

RIB の不一致が検出され、単一プロトコルを使用してトラフィック クラスを制御することを PfR に許可する場合に、デフォルトのルート制御の動作をディセーブルにするには、マスター コントローラでこのタスクを実行します。

（注） CSCtr26978 では、**no mode route protocol pbr** コマンドの動作はデフォルトでイネーブルになっています。 デフォルトの動作を上書きするには、このタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **no mode route protocol pbr**
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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 4	**no mode route protocol pbr** 例： `Router(config-pfr-mc)# no mode route protocol pbr`	自動 PBR ルート制御をディセーブルにします。 • トラフィック クラスを制御解除状態に設定します。PfR は BGP、EIGRP、スタティック、および PBR の順序で単一のプロトコルを使用して、トラフィック クラスを制御します。
ステップ 5	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR 簡素化のフェーズ 1 の設定例

例：PfR 簡素化のデフォルトの変更の確認

次の出力例は特権 EXEC モードからのもので、PfR を簡素化するために導入された新しいデフォルト値と動作を示しています。

次の部分的な出力は、CSCtr26978 で導入されたデフォルトの動作を示しています。バックオフ タイマー値は 90、900、および 90 秒、ホールドダウンは 90 秒に設定され、mode route control はイネーブル、mode select-exit best は削除されています。

```
.
.
.
Default Policy Settings:
  backoff 90 900 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  number of jitter probe packets 100
  mode route control
  mode monitor both
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  resolve delay priority 11 variance 20
  resolve range priority 12 variance 0
  resolve utilization priority 13 variance 20
.
.
.
```

次の部分的な出力は、CSCtr26978 で導入された新しいデフォルトの動作を示しています。学習モードはイネーブル、監視期間は 1 分、定期的な間隔は 0 分に設定されています。

```
.
.
.
Learn Settings:
  current state : ENABLED
  time remaining in current state : 0 seconds
  throughput
  no delay
  no inside bgp
  monitor-period 1
  periodic-interval 0
  aggregation-type prefix-length 24
  prefixes 100 appls 100
  expire after time 720
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR 簡素化のフェーズ 1 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *19* : *PfR* 簡素化のフェーズ *1* の機能情報

機能名	リリース	機能情報
PfR BR の自動隣接	15.2(2)S 15.2(3)T Cisco IOS XE Release 3.6S	PfR BR の自動隣接機能により、ダイナミックな PBR のサポートが導入されています。ダイナミック ルート マップでは、インターフェイスとネクスト ホップ情報の両方に対する PBR の要件は単一の set 句で PfR によって提供されるようになりました。 追加または変更されたコマンドはありません。

第 16 章

PfR SNMP MIB v1.0（読み取り専用）

PfR SNMP MIB v1.0（読み取り専用）機能により、パフォーマンス ルーティング（PfR）をサポートするための管理情報ベース（MIB）が導入されています。 CISCO-PFR-MIB という名前の PfR MIB では、読み取り専用モードで SNMPv2 を使用して PfR の管理および制限付きの制御が可能です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR SNMP MIB v1.0（読み取り専用）の概要

PfR MIB のサポート

パフォーマンス ルーティング（PfR）をサポートする管理情報ベース（MIB）は CISCO-PFR-MIB です。このサポートは、PfR SNMP MIB v1.0（読み取り専用）機能で導入されました。 PfR MIB では、SNMPv2 を使用した PfR の管理および制限付きの制御が可能です。

パフォーマンス ルーティング マネージャ（PRM）は、管理クライアントと PfR コンポーネント コード間の共通のコントロール ポイントとして機能する新しいサブシステムです。 PRM では、次の 5 つのインターフェイスが公開されます。

- クライアント サービス インターフェイス：PfR エンティティ（境界ルータ（BR）、出口、PfR マップ、および他の管理対象エンティティ）と関連付けられた管理対象データの取得と変更をサポートする MIB サブシステムのインターフェイス。
- Config サービス インターフェイス：クライアント サービス インターフェイス経由で MIB から要求された PfR 管理対象エンティティ関連の設定データに PRM が変更を加えるためのインターフェイス。
- ステータス サービス インターフェイス：PRM が PfR 管理対象エンティティのステータスを取得できるインターフェイス。 PRMは、PfRシステムにオブジェクトを登録および登録解除するためにもこのインターフェイスを使用します。
- メトリック サービス インターフェイス：パッシブ（NetFlow）またはアクティブ（IP SLA）パフォーマンス モニタリング コンポーネントによって、PfR トラフィック クラス（TC）のために収集されたパフォーマンス メトリックを PRM が取得するためのインターフェイス。
- 通知サービス インターフェイス：PRM が PfR SNMP トラップの生成を保証するイベントの通知を受け取るインターフェイス。

PfR MIB テーブル

マスター コントローラ テーブル

cpfrMCTable は、PfR マスター コントローラ（MC）の管理をサポートします。 このテーブルには、実際の PfR マスター コントローラ コンフィギュレーションに応じて次の MIB 変数が含まれます。

- cpfrMCAdminStatus
- cpfrMCConnStatus
- cpfrMCEntry
- cpfrMCIndex

- cpfrMCKeepAliveTime
- cpfrMCLearnStateTimeRemain
- cpfrMCMapIndex
- cpfrMCMaxPrefixLearn
- cpfrMCMaxPrefixTotal
- cpfrMCMaxRangeReceivePercent
- cpfrMCMaxRangeUtilPercentMax
- cpfrMCNumofBorderRouters
- cpfrMCNumofExits
- cpfrMCOperStatus
- cpfrMCPortNumber
- cpfrMCPrefixConfigured
- cpfrMCPrefixCount
- cpfrMCPrefixLearned
- cpfrMCRowStatus
- cpfrMCTracerouteProbeDelay

境界ルータ テーブル

cpfrBRTable は、PfR 境界ルータ（BR）の管理をサポートします。 このテーブルには、実際の PfR 境界ルータ コンフィギュレーションに応じて次の MIB 変数が含まれます。

- cpfrBRAddress
- cpfrBRAddressType
- cpfrBRAuthFailCount
- cpfrBRConnFailureReason
- cpfrBRConnStatus
- cpfrBREntry
- cpfrBRIndex
- cpfrBRKeyName
- cpfrBROperStatus
- cpfrBRRowStatus
- cpfrBRStorageType
- cpfrBRUpTime

アクティブ プローブ テーブル

cpfrActiveProbeTableテーブルには、アクティブ プローブを表すオブジェクトが含まれます。 テーブルの各エントリには、次のようにインデックス値が割り当てられています。

- cpfrActiveProbeIndex

出口テーブル

cpfrExitTable テーブルには、PfR 出口を表すオブジェクトが含まれます。 テーブルの各エントリには、次のようにインデックス値が割り当てられています。

- cpfrExitIndex

出口コスト テーブル

cpfrExitCostTable テーブルには、PfR 出口コスト データを表すオブジェクトが含まれます。 テーブルの各エントリには、次のようにインデックス値が割り当てられています。

- cpfrExitCostIndex

学習テーブル

cpfrLearnTable テーブルには、マスター コントローラの PfR 学習パラメータを表すオブジェクトが含まれます。 テーブルの各エントリには、次のようにインデックス値が割り当てられています。

- cpfrLearnIndex

学習リスト テーブル

cpfrLearnListTable テーブルには、マスター コントローラの PfR 学習リスト パラメータを表すオブジェクトが含まれます。 テーブルの各エントリには、次のようにインデックス値が割り当てられています。

- cpfrLearnListIndex

マップ テーブル

cpfrMapTable テーブルは、PfR マップの管理をサポートします。 このテーブルには、PfR マップを表すオブジェクトが含まれます。 PfR マップ テーブルの値は、**show oer master traffic-class** コマンドの出力の値と一致する必要があります。

- cpfrMapIndex

Match テーブル

cpfrMatchTable テーブルには、match 句を表すオブジェクトが含まれます。 match オブジェクトのテーブル エントリは、適切なマップ オブジェクトを使用して割り当てられます。

解決テーブル

cpfrResolveTableテーブルには、PfRリゾルバのプライオリティを表すオブジェクトが含まれます。match オブジェクトのテーブル エントリは、適切なマップ オブジェクトを使用して割り当てられます。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR SNMP MIB v1.0（読み取り専用）の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *20*：***PfR SNMP MIB v1.0***（読み取り専用）の機能情報

機能名	リリース	機能情報
PfR SNMP MIB v1.0（読み取り専用）	15.2(2)T Cisco IOS XE Release 3.5S	PfR SNMP MIB v1.0（読み取り専用）機能によって、読み取り専用モードでのCISCO-PfR-MIBが導入されました。 次のコマンドが導入または変更されました。**debug pfr mib error**、**debug pfr mib info**。

第 17 章

PfR SNMP トラップ v1.0

PfR SNMP トラップ v1.0 機能により、既存のパフォーマンス ルーティング（PfR）MIB にトラップ機能が追加され、新しい MIB、CISCO-PFR-TRAPS-MIB が導入されています。 簡易ネットワーク管理プロトコル（SNMP）トラップは、ネットワーク オペレータがアクションを実行する、または潜在的なトレンドや問題を特定するために必要とする PfR イベントに対して生成されます。 新しい CLI コマンドの設定を使用すると、特定の PfR トラフィック クラス イベントに対してトラップを生成することもできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR v1.0 SNMP トラップの概要

SNMP のコンポーネント

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。 SNMP はネットワーク デバイスのモニタリングや管理に使用される標準化されたフレームワークと共通言語を提供します。

SNMP フレームワークは、次の 3 つの部分から成ります。

PfR SNMP トラップ オブジェクト

マスター コントローラの管理状態の変更通知

cpfrMCEntryNotify トラップは、特定のパフォーマンス ルーティング（PfR）マスター コントローラ（MC）イベント（MC が管理ステータスを変更するイベント、MC がクリアされるイベント、MC が前回クリアされたイベント、MC が観察またはルート制御モードに変わるイベント、および MC ロギングがイネーブルになるイベント）に対して生成されます。 次のオブジェクトが通知に含まれます。

- cpfrMCAdminStatus
- cpfrMCClear
- cpfrMCControlMode
- cpfrMCLastClearTime
- cpfrMCLogLevel

境界ルータ エントリの通知

cpfrBREntryNotify トラップは、境界ルータ（BR）がアップ状態またはダウン状態に移行すると生成されます。 次のオブジェクトが通知に含まれます。

- cpfrBRAddress
- cpfrBRAddressType
- cpfrBRConnFailureReason
- cpfrBRConnStatus
- cpfrBROperStatus

インターフェイス エントリの通知

cpfrInterfaceEntryNotify トラップは、外部または内部インターフェイスがアップ状態またはダウン状態に移行すると生成されます。 次のオブジェクトが通知に含まれます。

- cpfrBRAddress
- cpfrBRAddressType
- cpfrExitName
- cpfrExitOperStatus
- cpfrExitType

トラフィック クラス ステータス エントリの通知

cpfrTrafficClassStatusEntryNotify トラップは、次の条件下で生成されます。

- **trap-enable** コマンドがグローバル コンフィギュレーション モードで設定されていて、トラフィック クラスがプライマリ リンクからフォールバック リンクに移行する、またはデフォルトやポリシー違反ステータスに移行する場合。
- **set trap-enable** コマンドが PfR マップ モードで設定されていて、トラフィック クラスがプライマリ リンクからフォールバック リンクに移行する、またはデフォルトやポリシー違反ステータスに移行する場合。

次のオブジェクトが通知に含まれます。

- cpfrBRAddress
- cpfrBRAddressType
- cpfrExitName
- cpfrLinkGroupType
- cpfrTCLastOOPReason
- cpfrTCStatus

PfR v1.0 SNMP トラップの設定方法

PfR SNMP トラップの生成のイネーブル化

ネットワーク オペレータがアクションを実行する必要がある PfR イベントの簡易ネットワーク管理プロトコル（SNMP）トラップの生成をイネーブルにするには、グローバル コンフィギュレーション モードでこのタスクを実行します。

特定のトラフィック クラスベースのトラップを生成するには、「PfR トラフィック クラスの SNMP トラップのイネーブル化」のタスクまたは「PfR マップを使用した PfR トラフィック クラスの SNMP トラップのイネーブル化」のタスクを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name* | **traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**pfr**]
4. **snmp-server enable traps pfr**
5. **exit**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 host** {*hostname* | *ip-address*} [**vrf** *vrf-name* | **traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**pfr**] 例： `Device(config)# snmp-server host 10.2.2.2 traps public pfr`	受信者への SNMP 通知の送信をイネーブルにします。 • この例では、PfR SNMP トラップは、IP アドレス 10.2.2.2 のデバイスに送信されます。
ステップ 4	**snmp-server enable traps pfr** 例： `Device(config)# snmp-server enable traps pfr`	PfR SNMP 通知の生成をイネーブルにします。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

PfR トラフィック クラスの SNMP トラップの生成のイネーブル化

PfR トラフィック クラスのイベントに対する簡易ネットワーク管理プロトコル（SNMP）トラップの生成をイネーブルにするには、このタスクを実行します。

cpfrTrafficClassStatusEntryNotify トラップは、次の条件下で生成されます。

- **trap-enable** コマンドが PfR マスター コントローラ コンフィギュレーション モードで設定されている場合。
- トラフィック クラスがプライマリ リンクからフォールバック リンクに移行した場合。
- トラフィック クラスがデフォルトまたはポリシー違反スタータスに移行した場合。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **trap-enable**
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、シスコ ルータをマスター コントローラとして設定します。
ステップ 4	**trap-enable** 例： `Device(config-pfr-mc)# trap-enable`	PfR トラフィック クラスの SNMP トラップの生成をイネーブルにします。 • SNMP トラップは、トラフィック クラスがプライマリ リンクからフォールバック リンクに移行、デフォルト ステータ

	コマンドまたはアクション	目的
		スに移行、またはポリシー違反（OOP）ステータスに移行すると生成されます。
ステップ 5	**end** 例： `Device(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

PfR マップを使用した PfR トラフィック クラスの SNMP トラップの生成のイネーブル化

PfR マップ内で PfR 簡易ネットワーク管理プロトコル（SNMP）トラップをイネーブルにするには、このタスクを実行します。

cpfrTrafficClassStatusEntryNotify トラップは、次の条件下で生成されます。

- **set trap-enable** コマンドが PfR マップ コンフィギュレーション モードで設定されている場合。
- トラフィック クラスがプライマリ リンクからフォールバック リンクに移行した場合。
- トラフィック クラスがデフォルトまたはポリシー違反スタータスに移行した場合。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn** {**delay** | **inside** | **list** *ref-name* | **throughput**}
5. **set trap-enable**
6. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr-map** *map-name sequence-number* 例： `Device(config)# pfr-map TRAP_1 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。
ステップ 4	**match pfr learn** {**delay** | **inside** | **list** *ref-name* | **throughput**} 例： `Device(config-pfr-map)# match pfr learn list TRAP_1`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。
ステップ 5	**set trap-enable** 例： `Device(config-pfr-map)# set trap-enable`	PfR マップに set 句を作成して、PfR トラフィック クラスのトラップの生成をイネーブルにします。 • PfR SNMP トラップは、トラフィック クラスがプライマリ リンクからフォールバック リンクに移行、デフォルト ステータスに移行、またはポリシー違反（OOP）ステータスに移行すると生成されます。
ステップ 6	**end** 例： `Device(config-pfr-map)# end`	（任意）PfR マップ 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。

PfR SNMP トラップ v1.0 の設定例

例：PfR SNMP トラップの生成のイネーブル化

次に、PfR 簡易ネットワーク管理プロトコル（SNMP）トラップの生成をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 10.2.2.2 traps public pfr
Device(config)# snmp-server enable traps pfr
```

例：PfR トラフィック クラスの SNMP トラップの生成のイネーブル化

次に、PfR トラフィック クラスのイベントの簡易ネットワーク管理プロトコル（SNMP）トラップの生成をイネーブルにするために使用するコマンドの例を示します。

```
Device> enable
Device# configure terminal
Device(config)# pfr-master
Device(config-pfr-mc)# trap-enable
```

例：PfR マップを使用した PfR トラフィック クラスの SNMP トラップの生成のイネーブル化

次に、PfR マップを使用して PfR トラフィック クラスのイベントに対する簡易ネットワーク管理プロトコル（SNMP）トラップの生成をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# pfr-map TRAPMAP 20
Device(config-pfr-map)# match pfr learn list TRAP-LIST
Device(config-pfr-map)# set mode monitor passive
Device(config-pfr-map)# set delay threshold 150
Device(config-pfr-map)# set resolve delay priority 1 variance 1
Device(config-pfr-map)# set trap-enable
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR SNMP トラップ v1.0 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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、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。

表 *21*：*PfR SNMP* トラップ *v1.0* の機能情報

機能名	リリース	機能情報
PfR SNMP トラップ v1.0	Cisco IOS XE 3.7S	PfR SNMP トラップ v1.0 機能により、既存の PfR MIB にトラップ機能が追加されています。SNMP トラップは、ネットワーク オペレータがアクションを実行する、または潜在的なトレンドや問題を特定するために必要とする PfR イベントに対して生成されます。 次のコマンドが導入または変更されました。**set trap-enable**、**snmp-server host**、**snmp-server enable traps pfr**、**trap-enable**。

第 18 章

パフォーマンス ルーティングを使用したスタティック アプリケーション マッピング

OER：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング機能により、パフォーマンス ルーティング（PfR）が自動的に学習できるトラフィック クラスまたは手動で設定できるトラフィック クラスの設定を容易にするために、1つのキーワードだけで標準アプリケーションを設定できるようになりました。 この機能により、学習リストにプロファイリングされたトラフィック クラスにパフォーマンス ルーティング（PfR）ポリシーを適用できる学習リスト コンフィギュレーション モードも導入されました。 異なるポリシーを各学習リストに適用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンスルーティングを使用したスタティックアプリケーション マッピングの前提条件

参加するすべてのデバイスでシスコ エクスプレス フォワーディング（CEF）を有効にする必要があります。その他のスイッチング パスは、ポリシーベース ルーティング（PBR）でサポートされている場合でもサポートされません。

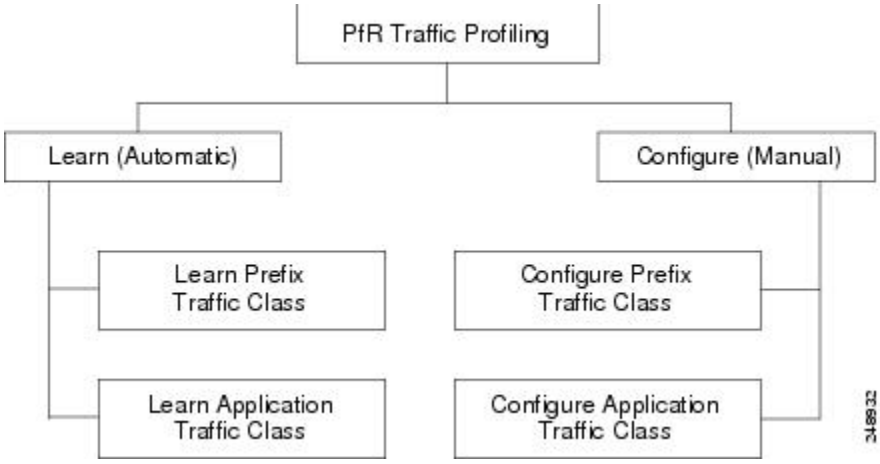
パフォーマンスルーティングを使用するスタティックアプリケーション マッピングの概要

パフォーマンス ルーティングのトラフィック クラス プロファイリング

トラフィックを最適化する前に、パフォーマンス ルーティング（PfR）では境界ルータを介したトラフィックからトラフィック クラスを判別する必要があります。 トラフィック ルーティングを最適化するには、全トラフィックのサブセットを識別する必要があります。これらのトラフィック サブセットをトラフィック クラスと呼びます。 トラフィック クラスのエントリのリストには、監視対象トラフィック クラス（MTC）リストという名前が付けられています。 デバイスを経由したトラフィックを自動的に学習するか、トラフィック クラスを手動で設定することによって、MTC リスト内のエントリのプロファイリングを行うことができます。 学習されたトラフィック クラスと設定されたトラフィック クラスの両方が、同時に MTC リストに存在する場合があります。 トラフィック クラスの学習メカニズムと設定メカニズムのいずれも、PfR のプロファイル

フェーズで実装されます。PfR トラフィック クラスのプロファイリング プロセスの全体構造とコンポーネントは次の図で確認できます。

図 *17*：*PfR* トラフィック クラスのプロファイリング プロセス



PfR では、トラフィック クラスを自動的に学習しながら、組み込みの NetFlow 機能を使用して境界ルータを経由したトラフィックを監視できます。 目的はトラフィックのサブセットを最適化することですが、このトラフィックの正確なパラメータをすべて把握できるわけではないので、PfR にはトラフィックを自動的に学習し、MTC リストに入力することによってトラフィック クラスを作成する方法が用意されています。 トラフィック クラスの自動学習プロセスには、次の 3 つのコンポーネントがあります。

- プレフィックスベースのトラフィック クラスの自動学習
- アプリケーションベースのトラフィック クラスの自動学習
- 学習リストを使用した、プレフィックスベースとアプリケーションベースの両トラフィック クラスの分類

モニタリングや後続の最適化用にトラフィック クラスを作成するよう、PfR を手動で設定することができます。 自動学習では通常、デフォルトのプレフィックス長 /24 が使用されますが、手動設定では正確なプレフィックスを定義することができます。 トラフィック クラスの手動設定プロセスには、次の 2 つのコンポーネントがあります。

- プレフィックスベースのトラフィック クラスの手動設定
- アプリケーションベースのトラフィック クラスの手動設定

プロファイル フェーズの最終目標は、ネットワークを経由するトラフィックのサブセットを選択することです。 このトラフィックのサブセット（MTC リスト内のトラフィック クラス）は、使用可能な最良のパフォーマンス パスに基づいてルーティングする必要のあるトラフィックのクラスを表します。

上の図のトラフィック クラスのプロファイリングの各コンポーネントの詳細については、「パフォーマンス ルーティングの理解」モジュールを参照してください。

PfR を使用したスタティック アプリケーション マッピング

OER：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング機能により、アプリケーションベースのトラフィック クラスの設定を容易にするために、キーワードを使用してアプリケーションを定義できるようになりました。 PfR では、よく知られているアプリケーションと固定ポートを使用します。複数のアプリケーションを同時に設定することもできます。 パフォーマンス ルーティング トラフィック クラスのプロファイルに使用できるスタティック アプリケーションのリストは、常に変化しています。 **traffic-class application ?** コマンドを使用して、スタティック アプリケーションがパフォーマンス ルーティングに使用できるかどうかを判別します。

次の表に、パフォーマンス ルーティングで設定できるスタティック アプリケーションのリストの一部を示します。 アプリケーションがスタティックと見なされる理由は、表に示されているとおり、それらのアプリケーションに固定ポートとプロトコルが定義されているためです。 設定は、マスター コントローラに対して学習リスト コンフィギュレーション モードで行われます。

表 *22*：スタティック アプリケーションのリスト

アプリケーション	キーワード	プロトコル	ポート
CU-SeeMe-Server：CU-SeeMe デスクトップ ビデオ会議	**cuseeme**	[TCP]、[UDP]	7648 7649 7648 7649 24032
DHCP-Client：Dynamic Host Configuration Protocol クライアント	**dhcp (Client)**	UDP/TCP	68
DHCP-Server：Dynamic Host Configuration Protocol サーバ	**dhcp (Server)**	UDP/TCP	67
DNS：ドメイン ネーム サーバ ルックアップ	**dns**	UDP/TCP	53
FINGER-Server：Finger サーバ	**finger**	TCP	79
FTP：ファイル転送プロトコル	**ftp**	TCP	20、21
GOPHER-Server：Gopher サーバ	**gopher**	TCP/UDP	70

アプリケーション	キーワード	プロトコル	ポート
HTTP：ハイパーテキスト転送プロトコル、ワールドワイドウェブ トラフィック	**http**	TCP/UDP	80
HTTPSSL-Server：Hypertext Transfer Protocol over TLS/SSL、セキュア ワールドワイドウェブ トラフィック サーバ	**secure-http**	TCP	443
IMAP-Server：Internet Message Access Protocol サーバ	**imap**	TCP/UDP	143 220
SIMAP-Server：Secure Internet Message Access Protocol サーバ	**secure-imap**	TCP/UDP	585 993（優先）
IRC-Server：インターネット リレーチャット サーバ	**irc**	TCP/UDP	194
SIRC-Server：セキュア インターネット リレーチャット サーバ	**secure-irc**	TCP/UDP	994
Kerberos-Server：Kerberos サーバ	**kerberos**	TCP/UDP	88 749
L2TP-Server：L2F/L2TP トンネル Layer 2 Tunnel Protocol サーバ	**l2tp**	UDP	1701
LDAP-Server：Lightweight Directory Access Protocol サーバ	**ldap**	TCP/UDP	389
SLDAP-Server：Secure Lightweight Directory Access Protocol サーバ	**secure-ldap**	TCP/UDP	636

アプリケーション	キーワード	プロトコル	ポート
MSSQL-Server：MS SQL サーバ	**mssql**	TCP	1443
NETBIOS-Server：NETBIOS サーバ	**netbios**	UDP TCP	137 138 137 139
NFS-Server：Network File System サーバ	**nfs**	TCP/UDP	2049
NNTP-Server：Network News Transfer Protocol	**nntp**	TCP/UDP	119
SNNTP-Server：Network News Transfer Protocol over TLS/SSL	**secure-nntp**	TCP/UDP	563
NOTES-Server：Lotus Notes サーバ	**notes**	TCP/UDP	1352
NTP-Server：ネットワーク タイムプロトコル サーバ	**ntp**	TCP/UDP	123
PCanywhere-Server：Symantec pcANYWHERE	**pcany**	UDP TCP	22 5632 65301 5631
POP3-Server：Post Office Protocol サーバ	**pop3**	TCP/UDP	110
SPOP3-Server：Post Office Protocol over TLS/SSL サーバ	**secure-pop3**	TCP/UDP	123
PPTP-Server：Point-to-Point Tunneling Protocol サーバ	**pptp**	TCP	17233
SSH：Secured Shell	**ssh**	TCP	22
SMTP-Server：Simple Mail Transfer Protocol サーバ	**smtp**	TCP	25
Telnet：Telnet	**telnet**	TCP	23

マスターコントローラは、フィルタリング対象トラフィックの最高アウトバウンドスループットまたは最高遅延に基づいてトップ プレフィックスを学習するように設定され、その結果得られたトラフィック クラスが PfR アプリケーション データベースに追加されてパッシブ モニタリングおよびアクティブ モニタリングの対象となります。

学習リスト コンフィギュレーション モード

学習リスト機能によって、学習リストという新しいコンフィギュレーション モードが導入されました。 学習リストは、学習したトラフィック クラスを分類する手段です。 各学習リストでは、プレフィックス、アプリケーションの定義、フィルタ、および集約パラメータなど、トラフィック クラスを学習するためのさまざまな基準を設定できます。 トラフィック クラスは、PfR によって各学習リスト基準に基づいて自動的に学習されます。各学習リストには、シーケンス番号が設定されます。 シーケンス番号によって、適用される学習リスト基準の順番が決定します。 学習リストごとに異なる PfR ポリシーを適用できます。以前のリリースではトラフィック クラスを分類することはできず、1 つの PfR ポリシーが、学習されたすべてのトラフィック クラスに適用されていました。

自動的に学習されるか、または手動で設定する 4 種類のトラフィック クラスをプロファイルできます。

- 送信先プレフィックスに基づいたトラフィック クラス
- アクセス リストを使用してカスタム アプリケーションの定義を示すトラフィック クラス
- 送信先プレフィックスを定義するオプションのプレフィックス リスト付きのスタティック アプリケーション マッピング名に基づいたトラフィック クラス

traffic-class コマンドを学習リスト モードで使用すると、トラフィック クラスの自動学習が簡素化されます。 学習リストごとに指定できる **traffic-class** コマンドのタイプは 1 つだけです。 **throughput**（PfR）コマンドと **delay**（PfR）コマンドも、学習リスト内で同時に使用することはできません。

match traffic-class コマンドを PfR マップ コンフィギュレーション モードで使用すると、トラフィック クラスの手動設定が簡素化されます。 PfR マップごとに指定できる **match traffic-class** コマンドのタイプは 1 つだけです。

（注） トラフィックをプロファイリングし、学習リスト パラメータを設定するほかに、学習リストを PfR ポリシー内で参照する必要があります。参照するには、PfR マップと **match pfr learn** コマンド（**list** キーワード指定）を使用します。 ポリシーをアクティブ化するには、**policy-rules**（PfR）コマンドを使用します。

パフォーマンスルーティングを使用したスタティックアプリケーション マッピングの設定方法

スタティック アプリケーション マッピングを使用してトラフィック クラスを自動的に学習するための学習リストの定義

マスター コントローラでこのタスクを実行すると、スタティック アプリケーション マッピングを使用して学習リストを定義できます。 学習リスト内では、アプリケーションを示すキーワードを使用して特定のアプリケーション トラフィック クラスを識別することができます。 定義済みの学習リストには、スタティック アプリケーションマッピングを使用してPfRで自動的に学習されたトラフィック クラスが表示されます。 表示されたトラフィック クラスは、必要に応じてプレフィックス リストによってフィルタリングすることができます。

このタスクでは、スタティックアプリケーションマッピングのキーワードを使用してトラフィック クラスを作成するように学習リストを設定します。 学習リストごとに異なるPfRポリシーを適用できます。 結果として得られた作成されたプレフィックスは、プレフィックス長24に集約されます。 プレフィックス リストがトラフィック クラスに適用されて、10.0.0.0/8プレフィックスからのトラフィックが許可されます。マスターコントローラは、フィルタリング対象トラフィックの最高アウトバウンドスループットに基づいてトッププレフィックスを学習するように設定され、その結果得られたトラフィック クラスがPfRアプリケーション データベースに追加されます。

学習リストは、PfRポリシー内でPfRマップを使用して参照され、**policy-rules**（PfR）コマンドを使用してアクティブ化されます。

PfRによって学習された設定済みの学習リストおよびトラフィック クラスに関する情報を表示するには、「トラフィック クラスおよび学習リストの情報の表示とリセット」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length* }
4. **pfr master**
5. **policy-rules** *map-name*
6. **learn**
7. **list seq** *number* **refname** *refname*
8. **traffic-class application** *application-name...* [**filter** *prefix-list-name*]
9. **aggregation-type** {**bgp non-bgp prefix-length**} *prefix-mask*
10. **throughput**
11. **exit**
12. ステップ 7 ～ 11 を繰り返して、追加の学習リストを設定します。
13. **exit**
14. ステップ 13 を繰り返し、グローバル コンフィギュレーション モードに戻ります。
15. **pfr-map** *map-name sequence-number*
16. **match pfr learn list** *refname*
17. **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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length* } 例： `Router(config)# ip prefix-list INCLUDE_10_NET permit 10.0.0.0/8`	学習するプレフィックスをフィルタリングするための IP プレフィックス リストを作成します。 • IP プレフィックス リストを学習リスト コンフィギュレーション モードで使用すると、学習される IP アドレスをフィルタリングすることができます。 • 例では、PfR に INCLUDE_10_NET という IP プレフィックス リストが作成され、プレフィックス 10.0.0.0/8 のプロファイリングが行われます。

	コマンドまたはアクション	目的
ステップ 4	**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、マスター コントローラとして Cisco ルータを設定し、マスター コントローラ ポリシーおよびタイマー設定を設定します。
ステップ 5	**policy-rules** *map-name* 例： `Router(config-pfr-mc)# policy-rules LL_REMOTE_MAP`	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、PfR マップを選択し設定を適用します。 • アクティブ化する PfR マップ名を指定するには、*map-name* 引数を使用します。 • 例では、このタスクで設定した学習リストを含んでいる LL_REMOTE_MAP という名前の PfR マップが適用されます。
ステップ 6	**learn** 例： `Router(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、トラフィック クラスを自動的に学習します。
ステップ 7	**list seq** *number* **refname** *refname* 例： `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_REMOTE_LOGIN_TC`	PfR 学習リストを作成し、学習リスト コンフィギュレーション モードを開始します。 • 学習リスト基準が適用される順番の決定に使用されるシーケンス番号を指定するには、**seq** キーワードおよび *number* 引数を使用します。 • 学習リストの参照名を指定するには、**refname** キーワードおよび *refname* 引数を使用します。 • 例では、LEARN_REMOTE_LOGIN_TC という名前の学習リストが作成されます。
ステップ 8	**traffic-class application** *application-name...* [**filter** *prefix-list-name*] 例： `Router(config-pfr-mc-learn-list)# traffic-class application telnet ssh`	事前定義されたスタティック アプリケーションを使用して、PfR トラフィック クラスを定義します。 • *application-name* 引数を使用して、事前定義されたスタティック アプリケーションを示す 1 つまたは複数のキーワードを指定します。 省略符号は、複数のアプリケーション キーワードを指定できることを示すときに使用します。 • 例では、telnet および ssh トラフィックを含むトラフィック クラスが定義されます。

	コマンドまたはアクション	目的
ステップ 9	**aggregation-type** {**bgp** **non-bgp** **prefix-length**} *prefix-mask* 例： `Router(config-pfr-mc-learn-list)# aggregation-type prefix-length 24`	（任意）トラフィック フロー タイプに基づいて学習済みのプレフィックスを集約するように、マスター コントローラを設定します。 • **bgp** キーワードは、BGP ルーティング テーブル内のエントリに基づいてプレフィックスを集約するように設定します。 このキーワードは、BGP ピアリングがネットワーク内でイネーブルの場合に使用されます。 • **non-bgp** キーワードは、スタティック ルートに基づいて学習済みのプレフィックスを集約するように設定します。このキーワードが入力された場合、BGP ルーティング テーブル内のエントリは無視されます。 • **prefix-length** キーワードは、指定したプレフィックス長に基づいて集約するように設定します。 この引数に設定できる値の範囲は、1 ～ 32 のプレフィックス マスクです。 • このコマンドが指定されない場合、デフォルトの集約が、/24 のプレフィックス長に基づいて実行されます。 • 例では、/24 のプレフィックス長に基づいて、プレフィックス長の集約が設定されます。
ステップ 10	**throughput** 例： `Router(config-pfr-mc-learn-list)# throughput`	最高アウトバウンド スループットに基づいてトップ プレフィックスを学習するように、マスター コントローラを設定します。 • このコマンドをイネーブルにすると、マスター コントローラでは最高アウトバウンド スループットに従ってすべての境界ルータのトップ プレフィックスが学習されます。 • 例では、LEARN_REMOTE_LOGIN_TC トラフィック クラスの最高アウトバウンドスループットに基づいてトッププレフィックスを学習するように、マスター コントローラが設定されます。
ステップ 11	**exit** 例： `Router(config-pfr-mc-learn-list)# exit`	学習リスト コンフィギュレーション モードを終了し、PfR Top Talker/Top Delay 学習コンフィギュレーション モードに戻ります。
ステップ 12	ステップ 7 ～ 11 を繰り返して、追加の学習リストを設定します。	--

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Router(config-pfr-mc-learn)# exit`	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、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 14	ステップ 13 を繰り返し、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 15	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map LL_REMOTE_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、LL_REMOTE_MAP という名前の PfR マップが作成されます。
ステップ 16	**match pfr learn list** *refname* 例： `Router(config-oer-map)# match pfr learn list LEARN_REMOTE_LOGIN_TC`	学習済みの PfR プレフィックスに一致させるために、PfR マップ内で match 句エントリを作成します。 • 例では、LEARN_REMOTE_LOGIN_TC という名前の PfR 学習リストに定義されている条件を使用して、トラフィック クラスが定義されます。 （注） ここでは、このタスクに関連する構文だけを使用しています。
ステップ 17	**end** 例： `Router(config-oer-map)# end`	（任意）OER マップ 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。

例

この例では、2 つの学習リストが、リモート ログイン トラフィックとファイル転送トラフィックを識別するように設定されます。 Telnet および Secure Shell（SSH）トラフィックを示すキーワードを使用してリモート ログイン トラフィック クラスが設定され、その結果得られたプレフィックスがプレフィックス長 24 に集約されます。 ファイル転送トラフィック クラスは、FTP を示すキーワードを使用して設定し、同様にプレフィックス長 24 に集約されます。 プレフィックス リストがファイル転送トラフィック クラスに適用されて、10.0.0.0/8プレフィックスからのトラフィックが許可されます。マスターコントローラは、フィルタリング対象トラフィックの最高アウトバウンドスループットに基づいてトッププレフィックスを学習するように設定され、その結果得ら

れたトラフィック クラスが PfR アプリケーション データベースに追加されます。 PfR マップは学習リストに一致するように設定され、ファイル転送トラフィック クラスは **policy-rules** (PfR) コマンドを使用してアクティブ化されます。

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
pfr master
 policy-rules LL_FILE_MAP
 learn
  list seq 10 refname LEARN_REMOTE_LOGIN_TC
   traffic-class application telnet ssh
   aggregation-type prefix-length 24
   throughput
   exit
  list seq 20 refname LEARN_FILE_TRANSFER_TC
   traffic-class application ftp filter INCLUDE_10_NET
   aggregation-type prefix-length 24
   throughput
   exit
  exit
 exit
pfr-map LL_REMOTE_MAP 10
 match pfr learn list LEARN_REMOTE_LOGIN_TC
 exit
pfr-map LL_FILE_MAP 20
 match pfr learn list LEARN_FILE_TRANSFER_TC
 end
```

スタティック アプリケーション マッピングを使用した、トラフィック クラスの手動選択

このタスクを実行すると、スタティックアプリケーションマッピングを使用して手動でトラフィック クラスを選択できます。 次のタスクは、トラフィック クラスに選択する送信先プレフィックスおよびアプリケーションが判明している場合に実行します。 このタスクでは、送信先プレフィックスを定義する IP プレフィックス リストが作成され、**match traffic-class application** (PfR) コマンドを使用してスタティック アプリケーションが定義されます。 PfR マップを使用して、各プレフィックスを各アプリケーションに対応付けて、トラフィック クラスを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. 必要に応じて、追加のプレフィックス リスト エントリに対し、ステップ 3 を繰り返します。
5. **pfr-map** *map-name sequence-number*
6. **match traffic-class application** *application-name* **prefix-list** *prefix-list-name*
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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} 例： `Router(config)# ip prefix-list LIST1 permit 10.1.1.0/24`	送信先プレフィックスベースのトラフィック クラスを指定するために、プレフィックス リストを作成します。 • 例では、アプリケーション トラフィック クラスのフィルタリングに使用する送信先プレフィックス 10.1.1.0/24 が指定されます。
ステップ 4	必要に応じて、追加のプレフィックス リストエントリに対し、ステップ 3 を繰り返します。	--
ステップ 5	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map APPLICATION_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • permit シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 6 で **match traffic-class** コマンドを使用して適用します。 • 例では、APPLICATION_MAP という名前の PfR マップが作成されます。
ステップ 6	**match traffic-class application** *application-name* **prefix-list** *prefix-list-name* 例： `Router(config-pfr-map)# traffic-class application telnet ssh prefix-list LIST1`	PfR マップを使用してトラフィック クラスを作成するには、プレフィックス リストに対する一致基準として 1 つまたは複数のスタティック アプリケーションを手動で設定します。 • *application-name* 引数を使用して、事前定義されたスタティック アプリケーションを示す 1 つまたは複数のキーワードを指定します。

	コマンドまたはアクション	目的
		• 例では、送信先プレフィックスが Y のアプリケーション X としてトラフィック クラスが定義されます。X は Telnet または Secure Shell、Y は LIST1 という名前の IP プレフィックス リストに定義されている送信先アドレスです。
ステップ 7	**end** 例： `Router(config-pfr-map)# end`	（任意）PfR マップ 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。

トラフィック クラスおよび学習リストの情報の表示とリセット

トラフィック クラスおよび学習リストの情報を表示し、任意で一部のトラフィック クラス情報をリセットするには、次の作業を実行します。 これらのコマンドは、学習リストが設定されてトラフィック クラスが自動的に学習された後で、または PfR マップを使用してトラフィック クラスが手動で設定されたときに入力できます。 コマンドは、任意の順番で入力できます。すべてのコマンドは、省略可能です。

手順の概要

1. **enable**
2. **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]
3. **show pfr master learn list** [*list-name*]
4. **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 **show pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*] | **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**] | **prefix** *prefix*| **prefix-list** *prefix-list-name*] [**active**| **passive**| **status**] [**detail**]

このコマンドは、学習済みのトラフィック クラス、または PfR 学習リスト コンフィギュレーション モードで手動設定されたトラフィック クラスに関する情報を表示するために使用されます。

例：

```
Router# show pfr master traffic-class
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
          Flags              State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS
--------------------------------------------------------------------------------
10.1.1.0/24               N defa    N           N           N N
              #           OOPOLICY       32         10.11.1.3  Gi0/0/1      BGP
              N        N         N        N        N         N        N      IBwN
            130      134         0        0        N         N
```

ステップ 3 **show pfr master learn list** [*list-name*]

このコマンドは、設定された PfR 学習リストの 1 つまたはすべてを表示するために使用されます。 この例では、2 つの学習リストに関する情報が表示されます。

例：

```
Router# show pfr master learn list
Learn-List LIST1 10
   Configuration:
    Application: ftp
    Aggregation-type: bgp
    Learn type: thruput
    Policies assigned: 8 10
   Stats:
    Application Count: 0
    Application Learned:
 Learn-List LIST2 20
   Configuration:
    Application: telnet
    Aggregation-type: prefix-length 24
    Learn type: thruput
    Policies assigned: 5 20
   Stats:
    Application Count: 2
    Application Learned:
     Appl Prefix 10.1.5.0/24 telnet
     Appl Prefix 10.1.5.16/28 telnet
```

ステップ 4 **clear pfr master traffic-class** [**access-list** *access-list-name*| **application** *application-name*[*prefix*]| **inside** | **learned**[**delay** | **inside** | **list** *list-name*| **throughput**]| **prefix** *prefix*| **prefix-list** *prefix-list-name*]

このコマンドは、PfR の制御対象トラフィック クラスをマスター コントローラ データベースからクリアするために使用されます。 次の例では、Telnet アプリケーションおよび 10.1.1.0/24 プレフィックスによって定義されたトラフィック クラスがクリアされます。

例：

```
Router# clear pfr master traffic-class application telnet 10.1.1.0/24
```

パフォーマンスルーティングを使用したスタティックアプリケーション マッピングの設定例

スタティック アプリケーション マッピングを使用してトラフィック クラスを自動的に学習するための学習リストの定義例

次の例では、スタティック アプリケーション マッピングを使用してアプリケーション トラフィック クラスが定義されます。 この例では、次の 2 つの PfR 学習リストが定義されます。

- LEARN_REMOTE_LOGIN_TC：Telnet および SSH で表されるリモート ログイン トラフィック。
- LEARN_FILE_TRANSFER_TC：FTP で表され、10.0.0.0/8 プレフィックスによってフィルタリングされるファイル転送トラフィック。

目的は、1 つのポリシー（POLICY_REMOTE）を使用してリモート ログイン トラフィックを最適化することと、別のポリシー（POLICY_FILE）を使用してファイル転送トラフィックを最適化することです。次のタスクでは、最高遅延に基づいたトラフィック クラスの学習が設定されます。 **policy-rules**（PfR）コマンドは、リモート トラフィック クラスの学習リストをアクティブ化します。 ファイル転送トラフィック クラスをアクティブ化するには、**policy-rules**（PfR）コマンドを使用して、POLICY_REMOTE マップ名を POLICY_FILE マップ名に置き換えます。

```
ip prefix-list INCLUDE_10_NET 10.0.0.0/8
pfr master
 policy-rules POLICY_REMOTE 10
 learn
 list seq 10 refname LEARN_REMOTE_LOGIN_TC
 traffic-class application telnet ssh
 aggregation-type prefix-length 24
 delay
 exit
 list seq 20 refname LEARN_FILE_TRANSFER_TC
 traffic-class application ftp filter INCLUDE_10_NET
 aggregation-type prefix-length 24
 delay
 exit
 exit
pfr-map POLICY_REMOTE 10
 match pfr learn list LEARN_REMOTE_LOGIN_TC
 exit
pfr-map POLICY_FILE 20
 match pfr learn list LEARN_FILE_TRANSFER_TC
 end
```

自動的に学習されたプレフィックスベースのトラフィッククラスの学習リストの定義例

マスターコントローラ上で設定された次の例では、プレフィックスリストだけに基づいて自動的に学習されたトラフィック クラスを含む学習リストが定義されます。 この例では、3 つの支社があり、支社 A および B へのすべてのトラフィックを 1 つのポリシー（Policy1）を使用して最適化し、支社 C へのトラフィックを別のポリシー（Policy2）を使用して最適化することが目的です。

支社 A は、10.1.0.0./16 に一致するすべてのプレフィックスとして定義され、支社 B は、10.2.0.0./16 に一致するすべてのプレフィックスとして定義されます。支社 C は、10.3.0.0./16 に一致するすべてのプレフィックスとして定義されます。

次のタスクでは、最高アウトバウンド スループットに基づいたプレフィックスの学習が設定されます。 **policy-rules**（PfR）コマンドは、支社 A および B 用に設定されたトラフィック クラス学習リストをアクティブ化します。

```
ip prefix-list BRANCH_A_B permit seq 10 10.1.0.0/16
ip prefix-list BRANCH_A_B permit seq 20 10.2.0.0/16
ip prefix-list BRANCH_C permit seq 30 10.3.0.0/16
pfr master
 policy-rules POLICY1
 learn
  list seq 10 refname LEARN_BRANCH_A_B
   traffic-class prefix-list BRANCH_A_B
   throughput
   exit
  list seq 20 refname LEARN_BRANCH_C
   traffic-class prefix-list BRANCH_C
   throughput
   exit
  exit
 exit
pfr-map POLICY1 10
 match pfr learn list LEARN_BRANCH_A_B
 exit
pfr-map POLICY2 10
 match pfr learn list LEARN_BRANCH_C
 end
```

アクセス リストを使用して自動的に学習されたアプリケーション トラフィック クラスの学習リストの定義例

次の例では、カスタム アプリケーション トラフィック クラスを定義するアクセス リストが作成されます。 この例のカスタム アプリケーションは、次の 4 つの基準で構成されます。

- 宛先ポート 500 上のすべての TCP トラフィック
- 700 ～ 750 の範囲のポート上のすべての TCP トラフィック
- 送信元ポート 400 上のすべての UDP トラフィック
- ef の DSCP ビットでマーキングされた、すべての IP パケット

ここでの目的は、POLICY_CUSTOM_APP という名前の PfR ポリシー内で参照されている学習リストを使用して、カスタム アプリケーション トラフィックを最適化することです。 次のタスクでは、最高アウトバウンドスループットに基づいたトラフィック クラスの学習が設定されます。**policy-rules**（PfR）コマンドは、カスタム アプリケーション トラフィック クラスの学習リストをアクティブ化します。

```
ip access-list extended USER_DEFINED_TC
 permit tcp any any 500
 permit tcp any any range 700 750
 permit udp any eq 400 any
 permit ip any any dscp ef
 exit
pfr master
 policy-rules POLICY_CUSTOM_APP
 learn
  list seq 10 refname CUSTOM_APPLICATION_TC
   traffic-class access-list USER_DEFINED_TC
   aggregation-type prefix-length 24
   throughput
   exit
  exit
 exit
pfr-map POLICY_CUSTOM_APP 10
 match pfr learn list CUSTOM_APPLICATION_TC
 end
```

スタティック アプリケーション マッピングを使用した、トラフィック クラスの手動選択例

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、Telnet または Secure Shell として定義され、10.1.1.0/24 ネットワーク、10.1.2.0/24 ネットワーク、および 172.16.1.0/24 ネットワークのプレフィックスを宛先とするアプリケーション トラフィックを含めるように PfR マップを設定する例を示します。

```
ip prefix-list LIST1 permit 10.1.1.0/24
ip prefix-list LIST1 permit 10.1.2.0/24
ip prefix-list LIST1 permit 172.16.1.0/24
pfr-map PREFIXES 10
 match traffic-class application telnet ssh prefix-list LIST1
 end
```

プレフィックス リストを使用した、プレフィックスベースのトラフィック クラスの手動選択例

次の例は、マスターコントローラ上で設定されます。トラフィック クラスが、送信先プレフィックスだけに基づいて手動で選択されます。次のタスクは、トラフィック クラスに選択する送信先プレフィックスが判明している場合に実行します。送信先プレフィックスを定義するために IP プレフィックス リストが作成され、PfR マップを使用してこのトラフィック クラスのプロファイリングが行われます。

```
ip prefix-list PREFIX_TC permit 10.1.1.0/24
ip prefix-list PREFIX_TC permit 10.1.2.0/24
ip prefix-list PREFIX_TC permit 172.16.1.0/24
```

```
pfr-map PREFIX_MAP 10
 match traffic-class prefix-list PREFIX_TC
 end
```

アクセス リストを使用したアプリケーション トラフィック クラスの手動選択例

次の例は、マスター コントローラ上で設定されます。トラフィック クラスが、アクセス リストを使用して手動で選択されます。アクセス リストの各エントリは、トラフィック クラスであり、送信先プレフィックスが必ず含まれています。他の省略可能なパラメータが含まれていることもあります。

```
ip access-list extended ACCESS_TC
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800any any dscp ef
 exit
pfr-map ACCESS_MAP 10
 match traffic-class access-list ACCESS_TC
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール

関連項目	マニュアル タイトル
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンスルーティングを使用したスタティックアプリケーション マッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *23*：パフォーマンス ルーティングを使用したスタティック アプリケーション マッピングの機能情報

機能名	リリース	機能の設定情報
OER：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング	Cisco IOS XE Release 3.3S	OER：スタティック アプリケーション マッピングを使用したアプリケーション アウェア ルーティング機能により、1 つのキーワードだけを使用して標準アプリケーションを設定できるようになりました。 この機能により、学習リストにプロファイリングされたトラフィック クラスにパフォーマンス ルーティング（PfR）ポリシーを適用できる学習リスト コンフィギュレーション モードも導入されました。 異なるポリシーを各学習リストに適用できます。 PfR が自動的に学習できるトラフィック クラス、または手動で設定するトラフィック クラスの設定を容易にするため、**traffic-class** コマンドおよび **match traffic-class** コマンドが新たに導入されました。 この機能により、次のコマンドが導入または変更されました。**clear pfr master traffic-class**、**count (PfR)**、**delay (PfR)**、**list (PfR)**、**match traffic-class access-list (PfR)**、**match traffic-class application (PfR)**、**match traffic-class prefix-list (PfR)**、**show pfr border defined application**、**show pfr master defined application**、**show pfr master learn list**、**show pfr master traffic-class**、**throughput (PfR)**、**traffic-class access-list (PfR)**、**traffic-class application (PfR)**、 **traffic-class prefix-list (PfR)**。

パフォーマンス ルーティングを使用したスタティック アプリケーション マッピングの機能情報

第 19 章

PfR ターゲット検出 v1.0

パフォーマンス ルーティング ターゲット検出 v1.0 機能により、IP SLA Responder の特定および設定の自動化、パフォーマンス ルーティング（PfR）アクティブ プローブの使用を最適化して、大企業のブランチ ネットワーク間のビデオおよび音声アプリケーションのパフォーマンスを管理するためのスケーラブルなソリューションが導入されています。音声およびビデオ トラフィックを使用してメディア アプリケーションを最適化するために、PfR では、ジッター、損失、および遅延の測定値が使用されます。 IP SLA udp ジッター プローブではこれらの測定値が提供されますが、IP SLA Responder が必要です。 各送信先プレフィックスの IP SLA Responder アドレスの手動設定は、大企業のブランチ ネットワークに拡張性の問題をもたらします。 PfR ターゲット検出 v1.0 機能では、マスター コントローラ（MC）ピアリングを導入し、EIGRP Service Advertisement Framework（SAF）経由で Service Routing（SR）を使用して、IP SLA Responder および関連付けられた送信先 IP プレフィックスをアドバタイズ、検出、および自動設定します。

（注） パフォーマンス ルーティング（PfR）ターゲット検出 v1.0 機能では、Cisco ASR1000 プラットフォームのプレフィックスの検出はサポートされていません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

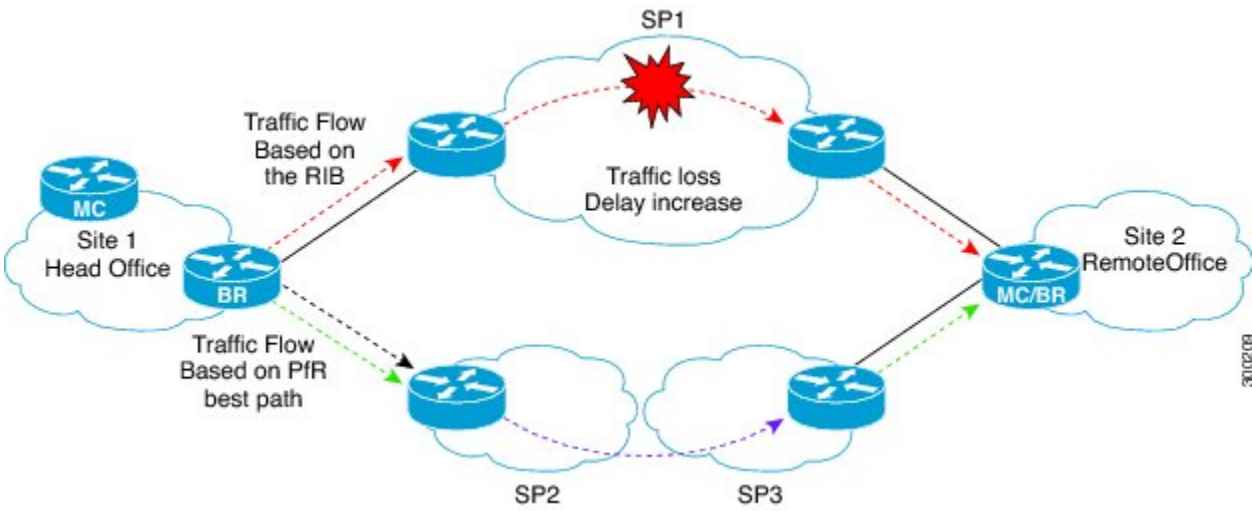
PfR ターゲット検出の概要

PfR ターゲット検出

Cisco Performance Routing（PfR）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。 次の図は、PfR と従来の IP ルーティング テクノロジーの違いを示しています。次の図では、トラフィックはサイト 1 の本社からサイト 2 のリモート オフィスに向かっています。 従来のルーティング テクノロジーは、ルーティング テーブル情報を使用して、パスが短いサービス プロバイダー 1 を経由してトラフィックをルーティングします。 ただし、大きな輻輳があるとトラフィックの損失につながり、SP1 経由での遅延が増加します。従来のルーティング テクノロジーでは、パフォーマンスの低下を認識できず、引き続き SP1 経由でトラフィックがルーティングされます。 PfR は、到達可能性、遅延、損失、ジッター、MOS、スループット、および負荷などのデータ測定値、および金銭的コストとユーザ定義のポリシーを考慮する能力によって決定される最良のパスを使用して、ネットワーク間でトラフィックをルーティングします。 従来の IP ルーティング テクノロジーとは異なり、PfR はリアルタイムのパフォーマンス メトリックに基づく適応型ルーティングの調整を提供します。 たとえば、次の図では、PfR は SP1 を経由するトラフィックのパフォーマンス測定値が悪いため、最良のパスである SP2 および SP3 経由でトラフィックを再ルーティングします。

（注） 次のネットワーク図は、小規模な企業ネットワーク向けのMPLS VPNネットワークとインターネット サービス プロバイダー（ISP）内の両方の SP に関連しています。

図 *18* : *PfR* と従来のルーティング テクノロジー



音声およびビデオ アプリケーションを最適化するために、PfR では、ジッター、損失、および遅延の測定値を使用して、最適なメディア パスを決定します。 IP SLA udp ジッター プローブではこれらの測定値が提供されますが、IP SLA Responder が必要です。 PfR は、音声およびビデオ トラフィック クラスの送信先プレフィックスに最も近い IP SLA Responder の IP アドレスを認識している必要があります。 各 PfR アプリケーション ポリシー内の送信先 IP プレフィックスの範囲ごとに IP SLA Responder を手動で設定するのは、WAN を介した何百または何千ものブランチ サイトがある企業ネットワークではスケーラブルなソリューションとは見なされません。

このような手動設定の問題に対応するために、PfR ターゲット検出では、マスター コントローラのピアリングを導入し、IP SLA Responder の IP アドレスをアドバタイズするために EIGRP Service Advertisement Framework（SAF）を使用して、レスポンダと関連付けられた送信先 IP プレフィックスの範囲の自動検出と設定を可能にします。

ターゲット検出データの配信

PfR ターゲット検出は、次の 2 つの利点をもたらすデータ配信メカニズムを使用します。

- 送信先とポリシーごとの IP SLA ターゲット コンフィギュレーションの削減。
- 複数ポリシー間でプローブ データを共有することによる、IP SLA プローブ効率の向上。

ターゲット検出を実行する各 PfR マスター コントローラ（MC）は、他の MC が WAN 経由で検出または学習するために、既知のローカル IP プレフィックスの範囲およびローカル IP SLA Responder をアドバタイズします。 ターゲット検出を実行する各 MC は、他の MC からアドバタイズされた

IP SLA Responder および関連付けられた送信先 IP プレフィックスの範囲も学習し、IP SLA Responder からのプローブ データを必要とするポリシーを動的に設定します。 PfR は、Cisco Service Routing（SR）および Service Advertisement Framework（SAF）を使用して、IP SLA ターゲット情報を配信および検出します。

SAF の詳細については、『*Service Advertisement Framework Configuration Guide*』を参照してください。

SAF を使用したマスター コントローラのピアリング

PfR マスター コントローラのピアリングは、Service Advertisement Framework（SAF）上で実行されます。 異なるサイトにある MC 間のピアリングを確立するために、各マスター コントローラで Service Routing（SR）フォワーダを使用します。MC のピアリングにより、PfR ターゲット検出データのアドバタイズメントと検出が可能になります。

ハブ サイト（ヘッドエンドとして知られる）およびブランチ オフィスのターゲット検出対応 MC は、SR 内部クライアントおよび SR フォワーダの両方として機能します。 いずれかのターゲット検出サービスをアドバタイズする前に、MC は SR フォワーダとして、SR ピアリング用に設定する必要があります。 MC のピアリングが確立されると、MC はローカル情報をアドバタイズして、他の MC がターゲット検出および自動設定を実行できるようにします。

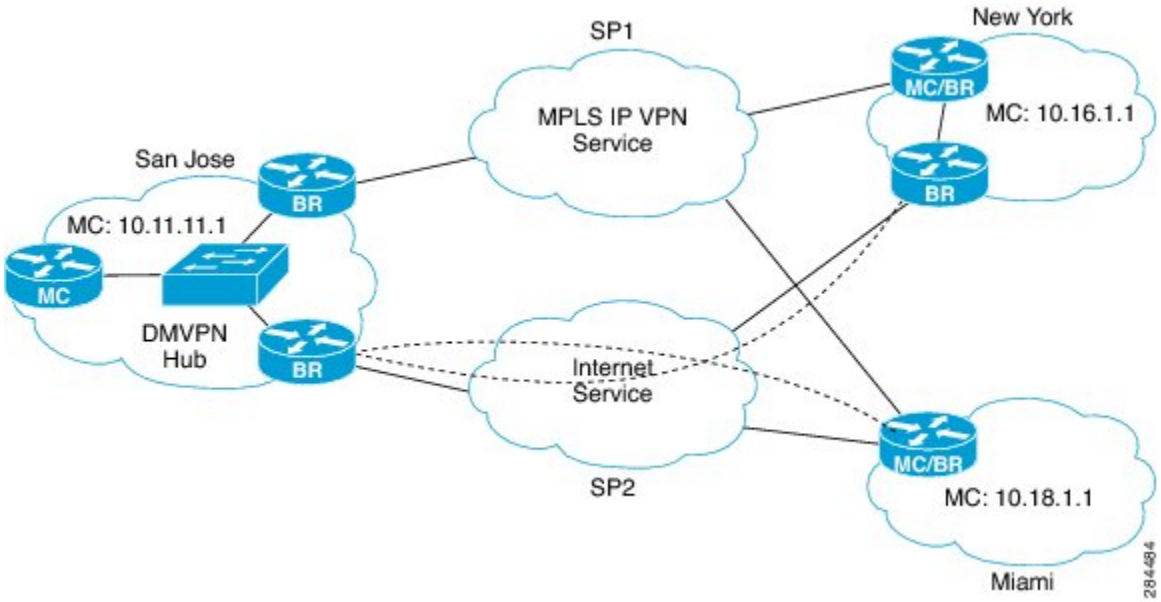
ネットワークの導入はカスタマーごとに異なり、導入ごとに、SR トポロジコンフィギュレーションを設定するさまざまな方法があります。 カスタマーがネットワークに使用している導入モデルにより、SR フォワーダの設定方法が決まります。 ターゲットの検出機能の MC-MC ピアリング アスペクトは、2 つの異なるカスタマー ネットワークの導入をサポートしています。

- マルチホップ：カスタマー ヘッドエンドおよびブランチ オフィスがカスタマーの管理下にない、または SAF 対応でない 1 台以上のルータで分離されているネットワーク。 例としては、MPLS VPN WAN サービスです。
- SAF-Everywhere：ヘッドエンド MC からブランチ オフィス MC への隣接パスにある EIGRP SAF に対してすべてのルータがイネーブルになっているネットワーク。 例としては、DMVPN WAN です。

次の図のトポロジは、マルチホップ タイプのネットワークでの MC のピアリングの導入例を示しています。 ハブ サイト（サンノゼ）MC システムとブランチ オフィス サイト（ニュー ヨークとマイアミ）MC システムは、論理的なユニキャスト トポロジ間でピアリングします。 このモデル

では、ハブ サイトとブランチ サイトは、EIGRP SR フォワーダが設定されていないネットワーク（通常はサービス プロバイダー（SP））によって分離されています。

図 *19*：***MPLS IP VPN*** および ***DMVPN*** を使用したマルチホップ ネットワーク トポロジ

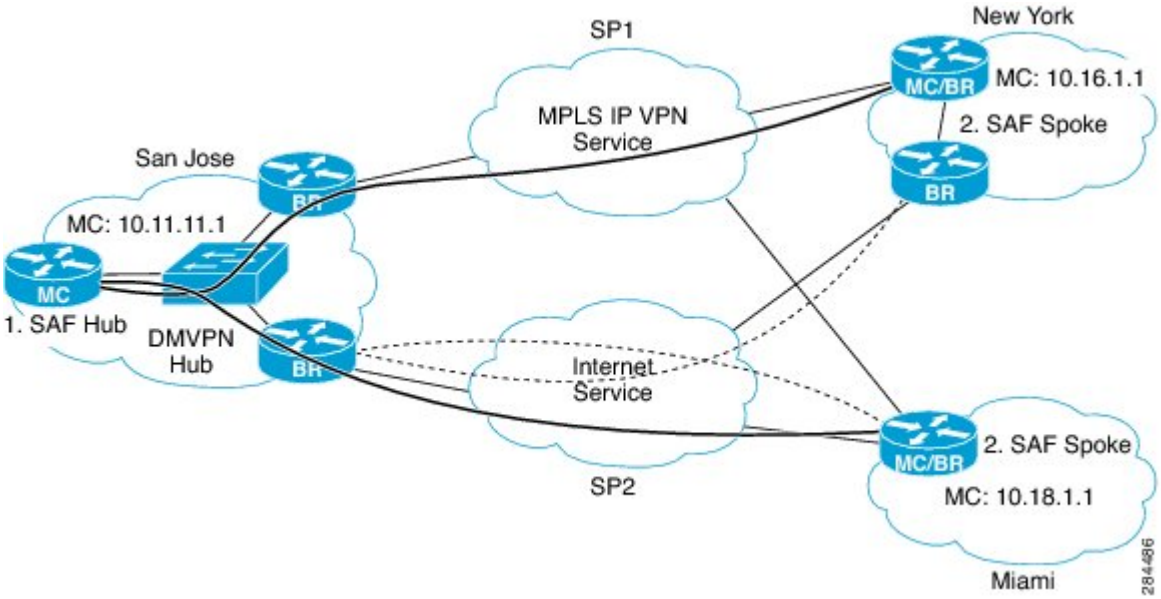


次の図は、前述の図の MPLS IP VPN および DMVPN を実行している同じ企業 WAN ネットワークに実装されている PfR ターゲット検出を示しています。 MC のピアリングをイネーブルにすると、サンノゼのマスター コントローラは SAF ハブ フォワーダになり、ニューヨークとマイアミの MC はサンノゼの MC とピアリングされます。 ターゲット検出では、各 MC が SAF を使用してローカル IP プレフィックスおよび IP SLA Responder をアドバタイズできます。各 MC は SAF からリモート IP プレフィックスおよび IP SLA Responder を学習します。 PfR は、ネットワーク パフォーマンスを測定するためにリモート サイトの IP SLA Responder をプローブします。

マルチホップ ネットワーク経由の MC のピアリングは、BGP ルート リフレクタに似たオーバーレイ モデルです。 MC のピアリング システムは、ネットワーク経由で到達可能（ルーティング可

能）であるIPアドレスを指定して、送信元ループバック インターフェイスを設定する必要があります。

図 *20*：マルチホップ エンタープライズ *WAN* ネットワーク内でイネーブルになっている *MC* のピアリングとターゲット検出



マスター コントローラのピアリングの設定オプション

ターゲット検出を実行する各 PfR マスター コントローラ（MC）は、他の MC が WAN 経由で検出または学習するために、既知のローカルIPプレフィックスの範囲およびローカルIP SLA Responderをアドバタイズします。 ターゲット検出を実行する各 MC は、他の MC からアドバタイズされた IP SLA Responder および関連付けられた送信先 IP プレフィックスの範囲も学習し、プローブ データを必要とするポリシーを動的に設定します。

ネットワーク構造およびプローブ ターゲットと IP SLA Responder の設定に必要な制御の程度に応じて、**mc-peer** コマンドを使用して MC のピアリングを設定する際に使用できる主なオプションが 3 つあります。

- ヘッドエンド（ハブ サイト）またはピア IP アドレス（ブランチ サイト）を設定する。 このオプションを使用する場合、SAF EIGRP 隣接関係のソースとしてループバック インターフェイスを設定することを推奨します。 この設定オプションは、マルチホップ タイプのネットワークで使用されます。
- SAF ドメイン ID を設定する、またはデフォルトの SAF ドメイン ID の 59501 を使用する。 このオプションでは、ハブ サイトとブランチ サイトの両方のマスター コントローラ ルータに EIGRP SAF を設定する必要があります。また、SAF-Everywhere タイプのネットワークで使用できます。

- SAF EIGRP の自動設定がない EIGRP オプションを設定する。 このオプションは、SAF-Everywhere タイプのネットワークで使用されます。 SAF がネットワーク内のルータにすでに設定されている場合、同じネットワークとオーバーレイ PfR ターゲット検出を使用できます。 PfR ターゲット検出とは別に SAF を設定する方法については、SAF のコンフィギュレーション ガイドを参照してください。

（注） CSCud06237 では、PfR ターゲット検出で **mc-peer eigrp** コマンドを使用する場合、PfR がローカル ID を選択できるように、ループバック インターフェイスを指定する必要があります。

PfR ターゲット検出の設定方法

マルチホップ ネットワークのハブ サイト用 PfR ターゲット検出および MC のピアリングの設定

ネットワークのヘッドエンドにあるマスター コントローラ（通常はハブ サイトのマスター コントローラ）で、PfR マスター コントローラ（MC）のピアリングを設定するには、このタスクを実行します。マスターコントローラは、ルーティング機能を持つデバイスである必要があります。このタスクでは、ハブ サイトとブランチ サイト間のネットワーク クラウドがカスタマーの管理下にない、または SAF 対応でないマルチホップ タイプのネットワークを想定しています。 この設計では、ハブ サイトの MC は、ブランチの MC SAF フォワーダがアドバタイズメントを交換するためにピアリングする Service Advertisement Facility（SAF）フォワーダ ハブになります。 ハブ サイトの MC は、同じ SAF ドメイン ID と MD5 認証を持つブランチの MC からのピアリング要求を受け入れます。

（注） このタスクでは、ダイナミックな PfR ターゲット検出がイネーブルになります。 この方法は、SAF がネットワーク内で他のアプリケーションに対してすでにイネーブルになっている、または MC と SAF 間に既存の隣接関係がある場合に適しています。 たとえば、DMVPN WAN で、複数の PfR MC が DMVPN トンネル デバイスに共存している場合、それらには SAF 隣接関係もあり、スタティック ピアリングは必要ありません。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **target-discovery**
5. **mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
6. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスターコントローラとしてシスコデバイスを設定します。
ステップ 4	**target-discovery** 例： `Device(config-pfr-mc)# target-discovery`	PfR ターゲット検出を設定します。 • この例では、ダイナミックな PfR ターゲット検出が設定されます。
ステップ 5	**mc-peer** [**head-end**	*peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] 例： `Device(config-pfr-mc)# mc-peer head-end loopback1 description SJ-hub`	この例では、このデバイスがハブ（ヘッドエンド）デバイスであることを示すために、PfR マスター コントローラのピアリングが設定されます。 • MC のピアリングに使用される SAF ドメイン ID を指定するには、**domain** キーワードを使用します。 *domain-id* 引数は、1 から 65535 の範囲で指定します。 SAF ドメイン ID を指定しない場合、デフォルト値の 59501 が使用されます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-pfr-mc)# end`	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

マルチホップ ネットワークのブランチ オフィス用 PfR ターゲット検出および MC のピアリングの設定

スポーク ルータとして機能するブランチ オフィスで PfR ターゲット検出のスタティック モードを使用して PfR MC のピアリングを設定するには、このタスクを実行します。 この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、MC のピアリングを可能にするためにループバック インターフェイスとして設定されます。このタスクでは、ハブ サイトとブランチ オフィス間のネットワーク クラウドがカスタマーの管理下にないマルチホップ タイプのネットワークを想定しています。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

はじめる前に

PfR マスター コントローラ（MC）ピアリングは、ネットワークのハブ サイト（ヘッドエンド）にあるルーティング機能を備えたデバイスに設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
5. **target-discovery**
6. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスター コントローラとしてシスコデバイスを設定します。
ステップ 4	**mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] 例： `Device(config-pfr-mc)# mc-peer 10.11.11.1 loopback1`	この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、ピア アドレスとして設定されます。
ステップ 5	**target-discovery** 例： `Device(config-pfr-mc)# target-discovery`	ダイナミックな PfR ターゲット検出を設定します。
ステップ 6	**end** 例： `Device(config-pfr-mc)# end`	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PfR ターゲット検出を使用したターゲットおよび IP プレフィックスの範囲のスタティック定義のイネーブル化

PfR ターゲット検出は、ルーティング機能を備えた境界デバイスで IP SLA Responder を動的にイネーブルにし、サイト固有の IP プレフィックスの範囲を学習できます。 この情報は、ローカル PfR マスター コントローラ（MC）から他の MC にアドバタイズされます。 SAF によってアドバタイズされる IP SLA Responder および IP プレフィックスの範囲をスタティックに設定するには、このタスクを実行します。 このタスクは、ハブ サイトのマスター コントローラで実行されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. 必要に応じてステップ 3 を繰り返して、プレフィックス リストを作成します。
5. **pfr master**
6. **target-discovery responder-list** *prefix-list-name* [**inside-prefixes** *prefix-list-name*]
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} 例： `Device(config)# ip prefix-list ipfx permit 10.101.1.0/24`	アクティブ プローブのターゲット プレフィックスの IP プレフィックス リストを作成します。 • IP プレフィックス リストを学習リスト コンフィギュレーション モードで使用すると、学習される IP アドレスをフィルタリングすることができます。 • この例では、PfR にプレフィックス 10.101.1.0/24 をプロファイリングさせるために ipfx という名前の IP プレフィックス リストを作成します。

	コマンドまたはアクション	目的
ステップ 4	必要に応じてステップ 3 を繰り返して、プレフィックス リストを作成します。	—
ステップ 5	**pfr master** 例： `Device(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、マスター コントローラとしてルーティング機能を備えたシスコ デバイスを設定します。
ステップ 6	**target-discovery responder-list** *prefix-list-name* [**inside-prefixes** *prefix-list-name*] 例： `Device(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx`	PfR ターゲット検出を設定します。 • この例では、PfR ターゲット検出は、IP SLA Responder と内部プレフィックスの IP アドレスのスタティック設定を使用して設定されます。
ステップ 7	**end** 例： `Device(config-pfr-mc)# end`	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

この例では、ハブ デバイスは、プロンプトに示されているように、ハブ サイトのマスター コントローラです。スポーク（ブランチ オフィス）デバイスの設定例については、「設定例」を参照してください。

```
Device-hub> enable
Device-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Device-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Device-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Device-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Device-hub(config)# pfr master
Device-hub(config-pfr-mc)# mc-peer head-end loopback1
Device-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Device-hub(config-pfr-mc)# end
```

PfR ターゲット検出情報の表示

PfR ターゲット検出機能を設定したら、このタスクのコマンドを入力して、ローカルおよびリモートのマスター コントローラ ピア、レスポンダ リスト、内部プレフィックス、および SAF ドメイン ID に関する情報を表示します。

手順の概要

1. **enable**
2. **show pfr master target-discovery**
3. **show pfr master active-probes target-discovery**
4. **debug pfr master target-discovery**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show pfr master target-discovery**
このコマンドは、PfR マスター コントローラにより監視および制御されるトラフィック クラスに関する情報を表示するときに使用されます。 この例では、コマンドはハブ（本社）マスター コントローラで入力され、ローカルおよびリモート ネットワーク、SAF 設定用のドメイン ID、およびマスター コントローラ ピアに関する情報が表示されます。 （local）のラベルが付いた出力セクションの情報は、他の MC にアドバタイズされます。（remote）のラベルが付いた出力セクションの情報は、SAF 経由で他の MC から学習されます。

例：

```
Device# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.11.11.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

ステップ 3 **show pfr master active-probes target-discovery**
このコマンドは、ターゲット検出を使用して学習されるすべてのアクティブ プローブおよびプローブ ターゲットのステータスを表示するために使用します。 この例では、コマンドはハブ（本社）マスター コン

トローラで入力され、2 つの MC ピアに関する情報が表示され、プローブのタイプおよびターゲット IP アドレスが一覧表示されます。

例：

```
Device# show pfr master active-probes target-discovery

PfR Master Controller active-probes (TD)
Border = Border Router running this probe
MC-Peer = Remote MC associated with this target
Type = Probe Type
Target = Target Address
TPort = Target Port
N - Not applicable

Destination Site Peer Addresses:

MC-Peer           Targets
10.16.1.1         10.111.1.2, 10.111.1.1
10.18.1.1         10.121.1.1

The following Probes are running:

Border          Idx  State     MC-Peer           Type     Target          TPort
10.16.1.3       27   TD-Actv   10.16.1.1         jitter   10.111.1.2      5000
10.16.1.2       14   TD-Actv   10.16.1.1         jitter   10.111.1.2      5000
10.16.1.3       27   TD-Actv   10.16.1.1         jitter   10.111.1.1      5000
10.16.1.2       14   TD-Actv   10.16.1.1         jitter   10.111.1.1      5000
10.18.1.1       14   TD-Actv   10.18.1.1         jitter   10.121.1.1      5000
10.18.1.1       27   TD-Actv   10.18.1.1         jitter   10.121.1.1      5000
```

ステップ 4 **debug pfr master target-discovery**

このコマンドは、問題のトラブルシューティングに役立つデバッグ メッセージを表示するために使用します。 次の例では、マスター コントローラのピアリング コマンド、**mc-peer** を発行後の PfR メッセージが示されています。MC のピアリングの宛先が変更され、PfR ターゲット検出がシャットダウンされ、再起動されています。

例：

```
Device# debug pfr master target-discovery

PfR Master Target-Discovery debugging is on
Device# configure terminal
Device(config)# pfr master
Device(config-pfr-mc)# mc-peer description branch office

*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli chg, op:0/1 idb:0/115967296 ip:0.0.0.0/0.0.0.0
 dom:59501/45000
*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli transition, shutting down TD
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown start, mode:4
*Oct 26 20:00:34.084: PFR_MC_TD: SvcUnreg: handle:5
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown fin, mode:4
*Oct 26 20:00:35.089: PFR_MC_TD: mc-peer cli enabled, starting TD, domain:59501
*Oct 26 20:00:35.089: PFR_MC_TD: TD startup, origin:192.168.3.1 handle:0 dyn_pid:4294967295
*Oct 26 20:00:35.089: PFR_MC_TD: Static mode start <-------
*Oct 26 20:00:35.090: PFR_MC_TD: Static Target list: 10.101.1.2, 10.101.1.1
*Oct 26 20:00:35.090: PFR_MC_TD: Static Prefix list: 10.101.2.0/24, 10.101.1.0/24
*Oct 26 20:00:35.090: PFR_MC_TD: SvcReg: handle:7
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: success  102:1:FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: handle:7 subscription handle:6
*Oct 26 20:00:35.093: PFR_MC_TD: local data encode, pre-publish
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: success  102:1:0.0.0.C0A80301
```

```
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: handle:7 size:336 seq:3 reach via 192.168.3.1
*Oct 26 20:00:35.094: PFR_MC_TD: prereqs met, origin:192.168.3.1 handle:7 sub:6 pub(s:1/r:0)
```

PfR ターゲット検出の設定例

例：ダイナミック モードでのマルチホップ ネットワークの PfR ターゲット検出の設定

次の設定は、本社とブランチ オフィスまたはリモート サイト間のネットワーク クラウドがカスタマーの管理下にない、または SAF 対応でないマルチホップ ネットワークで使用できます。 設定例では、3 台のマスター コントローラ（1 台は本社、2 台はブランチ オフィス）が示されています。 マスター コントローラのピアリングは 3 台のマスター コントローラ ルータ間に確立されていて、PfR ターゲット検出はダイナミック モードを使用して設定されています。 3 つすべてのサイトの **show pfr master target-discovery** コマンドの出力が表示されています。

（注） 次の例では、ハブおよびスポーク デバイスのホスト名は「Router-hub」、「Router-spoke1」、または「Router-spoke2」として設定されていますが、デバイスには PfR をサポートするルーティング機能を備えた任意のデバイスを指定できます。

ハブの MC のピアリングおよびターゲット検出の設定

ハブデバイスにはルーティング機能があり、本社に設置されています。 この例では、このデバイスがハブ デバイスであることを示すために、マスター コントローラのピアリングが **head-end** キーワードを使用して設定されています。 ループバック インターフェイスを指定する必要があります。これは、EIGRP SAF 隣接関係のソースとして使用されます。

```
Router-hub> enable
Router-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end Loopback1
Router-hub(config-pfr-mc)# target-discovery
Router-hub(config-pfr-mc)# end
```

Spoke1 MC のピアリングおよびターゲット検出の設定

spoke1 デバイスにはルーティング機能があり、ニューヨークのブランチ オフィスに設置されています。 この例では、マスター コントローラのピアリングがハブ デバイスの IP アドレス（10.11.11.1）とピアリングするように設定されています。

```
Router-spoke1> enable
Router-spoke1# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke1(config-pfr-mc)# target-discovery
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC のピアリングおよびターゲット検出の設定

spoke2 デバイスにはルーティング機能があり、マイアミのブランチ オフィスに設置されています。この例では、マスターコントローラのピアリングがハブ デバイスの IP アドレス（10.11.11.1）とピアリングするように設定されています。

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke2(config-pfr-mc)# target-discovery
Router-spoke2(config-pfr-mc)# end
```

スタティック モードを使用した PfR ターゲット検出の出力例

次の出力は、ダイナミック モードで PfR ターゲット検出が設定された後のハブ デバイスのものです。

```
Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.11.11.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

次の出力は、ダイナミック モードで PfR ターゲット検出が設定された後の spoke1 デバイスのものです。

```
Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.16.1.1        Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)
```

```
 MC-peer: 10.11.11.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

次の出力は、ダイナミック モードで PfR ターゲット検出が設定された後の spoke2 デバイスのものです。

```
Router-spoke2# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Dynamic  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.18.1.1        Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 11.11.11.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

例：ダイナミック モードを使用した SAF-Everywhere ネットワークでの PfR ターゲット検出の設定

次の設定例は、PfR MC 間のルーティング可能なデバイスがすべて SAF をサポートするように設定されているネットワークで使用できます。 このモデルでは、ハブ サイトとブランチ サイトは、EIGRP SR フォワーダが設定されておらず、すべてのデバイスが SAF 対応である、ネットワーク（通常はサービス プロバイダー（SP）ネットワーク）によって分離されています。 SAF-Everywhere タイプのネットワークを介した MC のピアリングは、隣接ネイバー間の EIGRP ピアリングと同様です。

設定例では、2 台のマスター コントローラ（1 台は本社、1 台はブランチ オフィス）が示されています。 マスター コントローラのピアリングは 2 台のマスター コントローラ ルータ間に確立されていて、PfR ターゲット検出は本社とブランチ オフィスでダイナミック モードでイネーブルになっています。

（注） わかりやすくするために、表示されている設定には、コマンド プロンプトはありません。

本社のマスター コントローラの設定

本社（ヘッドエンド）ルータでは、マスター コントローラのピアリングがイネーブルになっており、PfR ターゲット検出はダイナミック モードで設定されています。 SAF の設定は **service-family**

コマンドセクションの下に表示されています。この設定は、PfR MC のピアリングおよびターゲット検出オーバーレイの設定が追加される前に存在していると想定されています。

```
key chain metals
 key 1
   key-string gold
!
pfr master
 mc-peer
 target-discovery
 no keepalive
 !
 border 10.1.1.2 key-chain metals
  interface Ethernet0/2 external
  interface Ethernet0/3 external
  interface Ethernet0/0 internal
  interface Ethernet0/1 internal
 !
 learn
 throughput
 periodic-interval 0
 monitor-period 1
 delay threshold 100
 mode route control
 mode select-exit best

interface Loopback1
 ip address 10.100.100.101 255.255.255.255
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
!
router eigrp
 !
 service-family ipv4 autonomous-system 59501
  !
 remote-neighbors source Loopback1 unicast-listen
 exit-service-family
```

ブランチ オフィスのマスター コントローラの設定

ブランチ オフィス ルータでは、マスター コントローラのピアリングがイネーブルになっており、PfR ターゲット検出はダイナミック モードで設定されています。

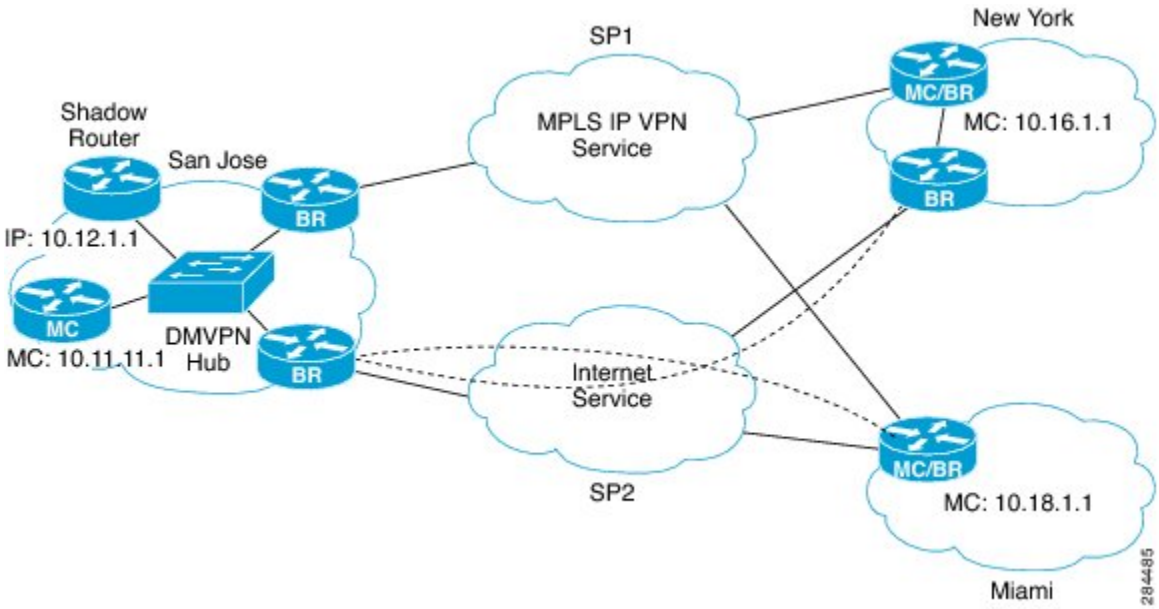
```
key chain metals
 key 1
   key-string gold
pfr master
 mc-peer
 target-discovery
 !
 border 172.16.1.3 key-chain metals
  interface Ethernet0/0 external
  interface Ethernet0/1 external
  interface Ethernet0/2 internal
  interface Ethernet0/3 internal
 !
 learn
 throughput
 periodic-interval 0
 monitor-period 1
!
interface Loopback1
 ip address 172.16.100.121 255.255.255.255
!
interface Ethernet0/2
 ip address 172.16.1.4 255.255.255.0
!
```

```
router eigrp
 !
 service-family ipv4 autonomous-system 59501
  !
 neighbor 10.100.100.101 Loopback1 remote 10
 exit-service-family
```

例：ターゲットのスタティック定義およびIPプレフィックスの範囲を使用したPfRターゲット検出の設定

次の設定例は、IP SLA Responder および IP プレフィックスの範囲が SAF によってアドバタイズされるように指定する場合に使用できます。この設定は、本社とブランチオフィスまたはリモートサイト間のネットワーク クラウドが SAF 対応でないマルチホップ ネットワークで実行できます。次の図では、シャドウ ルータはハブ サイトとして設定されています。シャドウ ルータは IP SLA Responder（IP SLA 測定のソース）として使用される専用ルータです。設定例では、3 台のマスター コントローラ（1 台は本社、2 台はブランチ オフィス）が示されています。マスター コントローラのピアリングは 3 台のマスター コントローラ ルータ間に確立されていて、プレフィックス リストが各サイトのローカル レスポンダと内部プレフィックスを特定するために設定されています。3 つすべてのサイトの **show pfr master target-discovery** コマンドの出力が表示されています。

図 *21*： ***MPLS IP VPN*** および ***DMVPN*** を使用したシャドウ ルータ ネットワーク トポロジを備えたマルチホップ



ハブの MC のピアリングおよびターゲット検出の設定

ハブ ルータは本社に設置されています。この例では、このルータがハブ ルータであることを示すために、マスター コントローラのピアリングが **head-end** キーワードを使用して設定されています。ループバック インターフェイスを指定する必要があります。これは、EIGRP SAF 隣接関係のソースとして使用されます。

（注） 次の例では、ハブおよびスポーク デバイスのホスト名は「Router-hub」、「Router-spoke1」、または「Router-spoke2」として設定されていますが、デバイスには PfR をサポートするルーティング機能を備えた任意のデバイスを指定できます。

```
Router-hub> enable
Router-hub# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Router-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Router-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Router-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end loopback1
Router-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-hub(config-pfr-mc)# end
```

Spoke1 MC のピアリングおよびターゲット検出の設定

spoke1 ルータはニューヨークのブランチ オフィスに設置されています。 この例では、マスター コントローラのピアリングがシャドウ（ハブ）ルータの IP アドレス（10.12.1.1）とピアリングするように設定されています。

```
Router-spoke1> enable
Router-spoke1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.1.0/24
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.2.0/26
Router-spoke1(config)# ip prefix-list tgt permit 10.111.3.1/32
Router-spoke1(config)# !
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke1(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC のピアリングおよびターゲット検出の設定

spoke2 ルータはマイアミのブランチ オフィスに設置されています。 この例では、マスター コントローラのピアリングがシャドウ（ハブ）ルータの IP アドレス（10.12.1.1）とピアリングするように設定されています。

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.1.0/24
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.2.0/26
Router-spoke2(config)# ip prefix-list tgt permit 10.121.1.1/32
Router-spoke2(config)# ip prefix-list tgt permit 10.121.2.1/32
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke2(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke2(config-pfr-mc)# end
```

スタティック モードを使用した PfR ターゲット検出の出力例

次の出力は、スタティック モードで PfR ターゲット検出が設定された後のハブ ルータのものです。

```
Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.12.1.1        Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24

 MC-peer: 10.16.1.1         Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

次の出力は、スタティック モードで PfR ターゲット検出が設定された後の spoke1 ルータのものです。

```
Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.16.1.1        Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)

 MC-peer: 10.12.1.1         Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.18.1.1         Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

次の出力は、スタティック モードで PfR ターゲット検出が設定された後の spoke2 ルータのものです。

```
Router-spoke2# show pfr master target-discovery

PfR Target-Discovery Services
 Mode: Static  Domain: 59501
 Responder list: tgt  Inside-prefixes list: ipfx
 SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1

PfR Target-Discovery Database (local)

 Local-ID: 10.18.1.1        Desc: Router-spoke2
   Target-list: 10.121.1.2, 10.121.1.1
   Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

```
PfR Target-Discovery Database (remote)

 MC-peer: 10.12.1.1          Desc: Router-hub
   Target-list: 10.101.1.2, 10.101.1.1
   Prefix-list: 10.101.2.0/24, 10.101.1.0/24

 MC-peer: 10.16.1.1          Desc: Router-spoke1
   Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
   Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR ターゲット検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *24* : *PfR* ターゲット検出の機能情報

機能名	リリース	機能情報
PfR ターゲット検出 v1.0	Cisco IOS XE Release 3.5S	PfR ターゲット検出機能では、IP SLA Responder の特定および設定を自動化することにより、大企業のブランチ ネットワーク間のビデオおよび音声アプリケーションのパフォーマンスを管理するためのスケーラブルなソリューションが導入されています。 次のコマンドが導入または変更されました。**debug pfr master target-discovery**、**mc-peer**、**show pfr master active-probes**、**show pfr master target-discovery**、および **target-discovery**。

第 20 章

xDSL アクセス用 PfR 帯域幅の可視性の配信

ハブおよびスポーク デバイスがマルチポイント トンネル経由で接続されているネットワークでは、ハブ サイトはスポーク デバイスでの帯域幅の制限を認識していません。 帯域幅の制限に関する更新情報がないと、パフォーマンス ルーティング（PfR）はアプリケーション トラフィックを最適化できません。 通常、インターネット サービス プロバイダー（ISP）へのスポーク デバイスの接続は、定期的に帯域幅が変化する DSL 接続です。 PfR 帯域幅の可視性は、PfR の拡張機能です。正確なポリシーを自動的に適用できるように、ピアリング PfR 要素に正確な最大帯域幅の情報を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

PfR 帯域幅の可視性の制約事項

- PfR 帯域幅解決は、トラフィック クラスのスループット データがないため、PfR アクティブ モードではサポートされていません。
- PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

PfR 帯域幅の可視性の概要

ADSL の定義

デジタル加入者線（DSL）テクノロジーは、マルチメディアやビデオなどの高帯域幅データをサービス加入者に転送するために、既存のツイストペア電話回線を使用するモデム テクノロジーです。 xDSL という用語は、Asymmetric DSL（ADSL/ADSL2）、Symmetric DSL（SDSL）、高速 DSL（HDSL）、Rate Adaptive（RADSL）、および最大 52 Mbps のダウンストリームを配信する Very High Bit Data Rate DSL（VDSL）を含む、類似の多くの DSL の競合形式をカバーします。

Asymmetric DSL の場合、あまり一般的ではない Symmetric DSL とは異なり、帯域幅はデータのアップロードよりダウンロードのほうが広くなります。

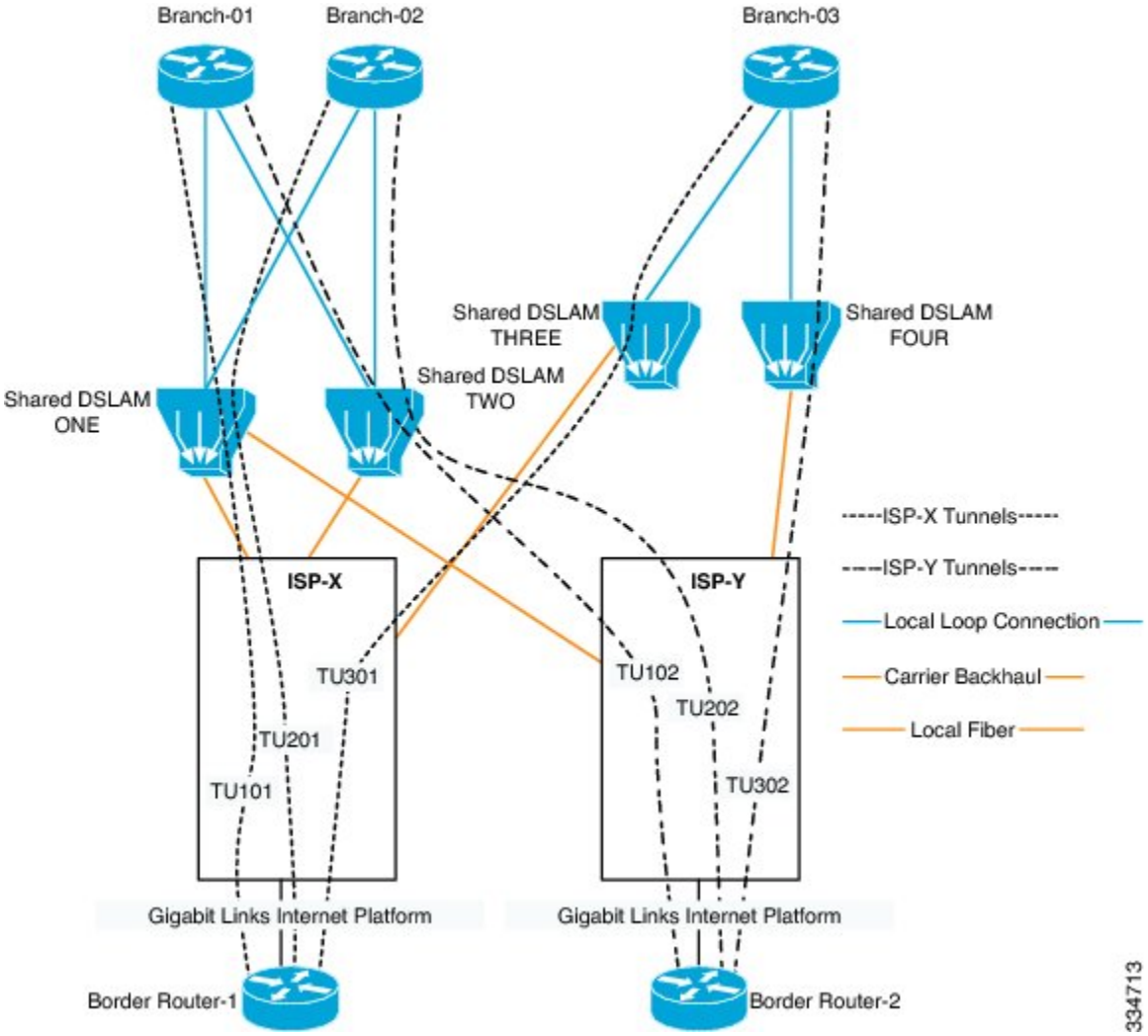
接続の加入者端局では、DSL モデムが、コンピュータで使用されるデジタル信号のデータを、電話回線で使用される適切な周波数帯域の電圧信号に変換します。 交換端局では、デジタル加入者線アクセス マルチプレクサ（DSLAM）は、DSL 回線を終了して集約し、他のネットワーキング転送に渡されます。 ADSL の場合、この手順でさらに DSLAM に内蔵されたフィルタ、または事前に設置された専用のフィルタリング機器を使用して、音声コンポーネントが分離されます。

PfR 帯域幅の可視性の問題

ハブおよびスポーク デバイスがマルチポイント トンネル経由で接続されているネットワークでは、ハブ サイトはスポーク デバイスでの帯域幅の制限を認識していません。 帯域幅の制限に関する更新情報がないと、パフォーマンス ルーティング（PfR）はアプリケーション トラフィックを最適化できません。 通常、インターネット サービス プロバイダー（ISP）へのスポーク デバイ

スの接続は、定期的に帯域幅が変化するDSL接続です。このようなネットワークの例として、次のネットワーク図を参照してください。

図 *22* : ***ADSL*** 接続を使用したハブおよびスポーク デバイス



PfRはハブとスポーク間のリンク使用率が設定されたしきい値を超えた場合、1つのDMVPN/MGREトンネルから別のトンネルにアプリケーション トラフィックをリダイレクトできますが、PfR では特定のスポークがどれだけ輻輳しているか確認することはできません。 スポーク側における更新された受信（Rx）と送信（Tx）の制限を検出し、その制限情報をハブに伝播できるメカニズムが必要です。この場合、PfR で制限情報を使用して、アプリケーション トラフィックを効率的に管理することができます。

ADSL の帯域幅の可視性の問題を生じるシナリオ

PfR 帯域幅の可視性の問題が生じる ADSL の主なシナリオは次の 3 つです。

- ADSL の再トレーニング：自動または手動による介入により、回線の再調整および再トレーニングを DSLAM に強制できます。これにより、回線の帯域幅割り当てが変更されます。 介入は予告なしに発生することがあります。 上方への再トレーニングの場合、ブランチへの影響はわずかです。 下方への再トレーニングの場合、ブランチは帯域幅を失うことがあります（交換の輻輳における一般的な問題）。 別のトンネルを介してトラフィックを移動させるタイミングを監視および評価する機能が、スムーズな再トレーニングを維持するためには重要です。
- ADSL の輻輳：輻輳期間中は、トラフィックが遅延することがあります。 このような状況では、ブランチ トラフィックができる限り最適なパスをとれるようにすること、およびすべてのリンクにわたってそれらのトラフィックを極力分散させることが不可欠です。
- ADSL の断続的なエラー：軽微な停止を引き起こす断続的なエラーが、場合によってはかなり頻繁に発生することがあります。 通常、これらの問題の調査には数営業日かかります（SLA なし）。 このような断続的な大量のエラーは、「割り当てられた」帯域幅の使用率が高い場合に低下となって表れます。 ISP が問題を修復するまで、トラフィック負荷のバランスを取り戻すために、どのトンネルについても使用プロファイルを効率的に変更する機能が存在する必要があります。

PfR 帯域幅の可視性の解決

帯域幅の可視性は、パフォーマンス ルーティング（PfR）の拡張機能です。正確なポリシーを自動的に適用できるように、ピアリング PfR 要素に正確な最大帯域幅の情報を提供します。 帯域幅の可視性が問題になっているネットワークでは通常、マルチポイント トンネルを介して接続されたハブおよびスポーク デバイスがあり、ハブ サイトはスポーク デバイスでの帯域幅の制限を認識していません。 帯域幅の制限に関する更新情報がないと、PfR はアプリケーション トラフィックを最適化できません。 現在、帯域幅の制限は手動で更新されますが、これはスケーラブルなソリューションではありません。

PfR の帯域幅の可視性は、既存の PfR ターゲット検出機能を利用します。 既存の SAF ベースのピアリング インフラストラクチャは、スポーク デバイスからハブ デバイスに帯域幅情報、およびターゲット情報を伝播するために使用することができます。 ハブでは、PfR マスター コントローラは、ピアのデータベースを構築し、それらの送受信の最大帯域幅情報を追跡します。 境界ルータは、特定のピア ネットワークに送信される帯域幅の総量を追跡し、マスターコントローラに報告します。 特定のピアに送信される帯域幅の総量が、そのピアの受信容量の一定の割合を超えると、PfR はそのアプリケーション トラフィックを代替リンクに再ルーティングして、スポーク デバイスでの輻輳を防ぎます。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

PfR 帯域幅解決をイネーブルにするには、PfR 帯域幅解決をイネーブルにするすべてのデバイスで PfR ターゲット検出を設定する必要があります。 その結果、すべてのマスターコントローラ デバ

イスで PfR 帯域幅解決がイネーブルになります。 PfR 帯域幅解決では、ダイナミックおよびスタティック ターゲット検出の両方がサポートされています。 帯域幅解決をイネーブルにすると、送受信の帯域幅制限は、PfR ターゲット検出を使用して自動的に検出されて伝播されます。 このメカニズムにより、動的に検出された制限を上書きできます。

（注） PfR 帯域幅解決は、トラフィック クラスのスループット データがないため、PfR アクティブ モードではサポートされていません。

PfR 帯域幅の可視性の設定方法

マルチホップ ネットワークのハブ サイト用 PfR ターゲット検出および MC のピアリングの設定

ネットワークのヘッドエンドにあるマスター コントローラ（通常はハブ サイトのマスター コントローラ）で、PfR マスター コントローラ（MC）のピアリングを設定するには、このタスクを実行します。マスターコントローラは、ルーティング機能を持つデバイスである必要があります。このタスクでは、ハブ サイトとブランチ サイト間のネットワーク クラウドがカスタマーの管理下にない、または SAF 対応でないマルチホップ タイプのネットワークを想定しています。 この設計では、ハブ サイトの MC は、ブランチの MC SAF フォワーダがアドバタイズメントを交換するためにピアリングする Service Advertisement Facility（SAF）フォワーダ ハブになります。 ハブ サイトの MC は、同じ SAF ドメイン ID と MD5 認証を持つブランチの MC からのピアリング要求を受け入れます。

（注） このタスクでは、ダイナミックな PfR ターゲット検出がイネーブルになります。 この方法は、SAF がネットワーク内で他のアプリケーションに対してすでにイネーブルになっている、または MC と SAF 間に既存の隣接関係がある場合に適しています。 たとえば、DMVPN WAN で、複数の PfR MC が DMVPN トンネル デバイスに共存している場合、それらには SAF 隣接関係もあり、スタティック ピアリングは必要ありません。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **target-discovery**
5. **mc-peer** [**head-end** | *peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
6. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスターコントローラとしてシスコデバイスを設定します。
ステップ 4	**target-discovery** 例： `Device(config-pfr-mc)# target-discovery`	PfR ターゲット検出を設定します。 • この例では、ダイナミックな PfR ターゲット検出が設定されます。
ステップ 5	**mc-peer** [**head-end**	*peer-address*] [**loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] 例： `Device(config-pfr-mc)# mc-peer head-end loopback1 description SJ-hub`	この例では、このデバイスがハブ（ヘッドエンド）デバイスであることを示すために、PfR マスター コントローラのピアリングが設定されます。 • MC のピアリングに使用される SAF ドメイン ID を指定するには、**domain** キーワードを使用します。 *domain-id* 引数は、1 から 65535 の範囲で指定します。 SAF ドメイン ID を指定しない場合、デフォルト値の 59501 が使用されます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-pfr-mc)# end`	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

マルチホップ ネットワークのブランチ オフィス用 PfR ターゲット検出および MC のピアリングの設定

スポーク ルータとして機能するブランチ オフィスで PfR ターゲット検出のスタティック モードを使用して PfR MC のピアリングを設定するには、このタスクを実行します。 この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、MC のピアリングを可能にするためにループバック インターフェイスとして設定されます。このタスクでは、ハブ サイトとブランチ オフィス間のネットワーク クラウドがカスタマーの管理下にないマルチホップ タイプのネットワークを想定しています。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

はじめる前に

PfR マスター コントローラ（MC）ピアリングは、ネットワークのハブ サイト（ヘッドエンド）にあるルーティング機能を備えたデバイスに設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*]
5. **target-discovery**
6. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスター コントローラとしてシスコデバイスを設定します。
ステップ 4	**mc-peer** [*peer-address* **loopback** *interface-number*] [**description** *text*] [**domain** *domain-id*] 例： `Device(config-pfr-mc)# mc-peer 10.11.11.1 loopback1`	この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、ピア アドレスとして設定されます。
ステップ 5	**target-discovery** 例： `Device(config-pfr-mc)# target-discovery`	ダイナミックな PfR ターゲット検出を設定します。
ステップ 6	**end** 例： `Device(config-pfr-mc)# end`	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

帯域幅解決のイネーブル化

このタスクは、関係するサイトのすべてのハブとスポークのすべての PfR マスター コントローラで実行されます。

はじめる前に

（注） PfR ターゲット検出は、帯域幅解決をイネーブルにする前に設定する必要があります。 PfR 帯域幅解決では、ダイナミックおよびスタティック ターゲット検出の両方がサポートされています。 PfR 帯域幅解決は、トラフィック クラスのスループット データがないため、PfR アクティブ モードではサポートされていません。

（注） PfR は、スポークツースポーク トンネリングをサポートしていません。 Next Hop Resolution Protocol（NHRP）設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **bandwidth-resolution**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 4	**bandwidth-resolution** 例： `Device(config-pfr-mc)# bandwidth-resolution`	帯域幅解決をイネーブルにします。

動的に検出された送受信の帯域幅制限の上書き

PfR外部インターフェイスの受信（Rx）および送信（Tx）の制限の最大値を手動で指定するには、PfR マスター コントローラでこのタスクを実行します。 帯域幅解決がイネーブルの場合、送受信の帯域幅制限は、PfR ターゲット検出を使用して動的に検出されて伝播されます。 PfR 帯域幅解決を使用して動的に検出された制限を上書きするには、このタスクを使用します。

境界ルータ用外部インターフェイスが設定されると、PfR は、境界ルータ上の外部リンク使用率を 20 秒ごとに自動的に監視します。 使用率はマスター コントローラに報告されます。使用率が指定された制限値を超えると、PfR はそのリンク上のトラフィック クラス用に別の出口リンクを選択します。 動的に検出された帯域幅制限を上書きするために指定できるのは、絶対値（キロビット毎秒（kbps））だけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive absolute** *kbps*
7. **max-xmit-utilization absolute** *kbps*
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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	**pfr master** 例： `Device(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、マスターコントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] 例： `Device(config-pfr-mc)# border 10.1.1.2`	PfR 管理境界ルータ コンフィギュレーション モードを開始して、境界ルータとの通信を確立します。 • 境界ルータを識別するために、IP アドレスを設定します。 • PfR の管理対象ネットワークを作成するには、少なくとも 1 台の境界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境界ルータは、最大 10 台です。 （注） 境界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、既存の境界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 5	**interface** *type number* **external** 例： `Device(config-pfr-mc-br)# interface GigabitEthernet 0/0/0 external`	PfR 管理の外部インターフェイスとして境界ルータを設定し、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 モードを開始します。 • 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 つの外部境界ルータ インターフェイスが必要です。 各境界ルータでは、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。 （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。

	コマンドまたはアクション	目的
ステップ 6	**maximum utilization receive absolute** *kbps* 例： `Device(config-pfr-mc-br-if)# maximum utilization receive absolute 500000`	PfR 管理の入口リンクのインターフェイスを介して送信できる着信トラフィックの最大使用率のしきい値を設定します。 • PfR 管理の入口リンクでの絶対最大使用率を kbps 単位で指定するには、**absolute** キーワードおよび *kbps* 引数を使用します。
ステップ 7	**max-xmit-utilization absolute** *kbps* 例： `Device(config-pfr-mc-br-if)# max-xmit-utilization absolute 500000`	単一の PfR 管理の出口リンクの最大使用率を設定します。 • PfR 管理の出口リンクでの絶対最大使用率を kbps 単位で指定するには、**absolute** キーワードおよび *kbps* 引数を使用します。
ステップ 8	**end** 例： `Device(config-pfr-mc-br-if)# end`	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 モードを終了し、特権 EXEC モードに戻ります。

PfR 帯域幅の可視性の設定例

例：PfR 帯域幅解決の設定

（注） PfR ターゲット検出は、帯域幅解決がイネーブルになる前に設定する必要があります。 PfR 帯域幅解決では、ダイナミックおよびスタティック ターゲット検出の両方がサポートされています。

次の設定は、本社とブランチ オフィスまたはリモート サイト間のネットワーク クラウドがカスタマーの管理下にない、または SAF 対応でないマルチホップ ネットワークで使用できます。 設定例では、3 台のマスター コントローラ（1 台は本社、2 台はブランチ オフィス）が示されています。 すべての PfR マスター コントローラ（MC）デバイスで PfR 帯域幅解決がイネーブルになっています。 3 つすべてのサイトの **show pfr master bandwidth-resolution** コマンドの出力が表示されています。

（注） 次の例では、ハブおよびスポーク デバイスのホスト名は「Router-hub」、「Router-spoke1」、または「Router-spoke2」として設定されていますが、デバイスには PfR をサポートするルーティング機能を備えた任意のデバイスを指定できます。

ハブの MC 帯域幅解決の設定

ハブ デバイスにはルーティング機能があり、本社に設置されています。 この例では、マスター コントローラで PfR 帯域幅解決がイネーブルになっています。

```
Router-hub> enable
Router-hub# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# bandwidth-resolution
Router-hub(config-pfr-mc)# end
```

Spoke1 MC の帯域幅解決の設定

spoke1 デバイスにはルーティング機能があり、ブランチ（スポーク）オフィスに設置されています。 この例では、ブランチ オフィスのマスター コントローラで PfR 帯域幅解決がイネーブルになっています。

```
Router-spoke1> enable
Router-spoke1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# bandwidth-resolution
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC の帯域幅解決の設定

spoke2 デバイスにはルーティング機能があり、セカンド ブランチ（スポーク）オフィスに設置されています。 この例では、セカンド ブランチ オフィスのマスター コントローラで PfR 帯域幅解決がイネーブルになっています。

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# bandwidth-resolution
Router-spoke2(config-pfr-mc)# end
```

PfR 帯域幅解決の出力例

次の出力は、PfR の帯域幅解決がイネーブルになった後のハブ デバイスのマスター コントローラのものです。

```
Router-hub# show pfr master bandwidth-resolution all

Border Router: 10.20.20.2           External Interface: Tu10
MC-peer address  Overlay address   Rx BW [kbps]   Tx BW [kbps]  Tx Load [kbps]
172.17.51.1      10.110.110.2      1000           900           0
172.20.61.1      10.110.110.3      1000           900           35
```

```
Border Router: 10.20.20.3           External Interface: Tu20
MC-peer address  Overlay address   Rx BW [kbps]   Tx BW [kbps]  Tx Load [kbps]
172.17.51.1      10.90.90.2        1000           900           18
172.20.61.1      10.90.90.3        803            903
```

次の出力は、PfR の帯域幅解決がイネーブルになった後のハブ デバイスのマスター コントローラのもので、IP アドレス 172.20.61.1 のマスター コントローラ ピアの出力が表示されています。

```
Router-hub# show pfr master bandwidth-resolution 172.20.61.1

PfR Bandwidth Resolution Database
MC-peer: 172.20.61.1
Border Router  External Interface  Overlay Address  Rx BW [kbps] Tx BW [kbps] Tx Load [kbps]

10.20.20.2     Tu10                10.110.110.3     1000         900          35

10.20.20.3     Tu20                10.90.90.3       803          903          0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

PfR 帯域幅の可視性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *25*：*PfR* 帯域幅の可視性の機能情報

機能名	リリース	機能情報
xDSL アクセス用 PfR 帯域幅の可視性の配信	15.3(1)T Cisco IOS XE Release 3.8S	PfR 帯域幅の可視性は、PfR の拡張機能です。ポリシーを自動的に適用できるように、ピアリング PfR 要素に正確な最大帯域幅の情報を提供します。 次のコマンドが導入または変更されました。 **bandwidth-resolution**、**debug pfr border bandwidth-resolution**、**debug pfr master bandwidth-resolution**、**show pfr master bandwidth-resolution**。

第 21 章

パフォーマンス ルーティングの traceroute レポート

パフォーマンス ルーティング（PfR）では traceroute レポートをサポートしているので、ホップバイホップ ベースでプレフィックスのパフォーマンスを監視できます。 遅延、損失、および到達可能性の測定が、プローブ ソース（境界ルータ）からターゲット プレフィックスへのホップごとに収集されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

パフォーマンス ルーティングの traceroute レポートの概要

PfR のロギングとレポート

Cisco IOS PfR では、標準の syslog 機能をサポートしています。 デフォルトでは、通知レベルの syslog がイネーブルになります。 システム ロギングの enable と設定は、グローバル コンフィギュレーション モードで行います。 PfR マスター コントローラまたは PfR 境界ルータ コンフィギュレーション モードでは、**logging** (PfR) コマンドは、PfR でシステム ロギングをイネーブルまたはディセーブルにする場合にのみ使用します。 PfR システム ロギングは、次のメッセージ タイプをサポートします。

- エラー メッセージ：これらのメッセージは、通常の PfR 動作に影響する可能性のある PfR の動作障害や通信問題を示します。
- デバッグ メッセージ：これらのメッセージは、動作上の問題やソフトウェアの問題を診断するため、詳細な PfR の動作を監視するときに使用します。
- 通知メッセージ：これらのメッセージは、PfR が通常の動作状態にあることを示します。
- 警告メッセージ：これらのメッセージは、PfR が正しく機能しているものの、PfR の外部のイベントが通常の PfR の動作に影響する可能性があることを示します。

（注） CSCtx06699 では、表示されるメッセージ数を最小限に抑えるために PfR syslog レベルが追加され、トラフィック クラスの 30 % がポリシー違反の場合に表示する syslog 通知が追加されています。

（注） CSCts74631 では、表示されるメッセージ数を最小限に抑えるために PfR syslog レベルが追加され、トラフィック クラスの 30 % がポリシー違反の場合に表示する syslog 通知が追加されています。また、PfR バージョンの不一致、MC-BR 認証エラー、および動作可能な外部インターフェイスが 2 つ未満のために、PfR の最小要件を満たさず、マスター コントローラがディセーブルになっている場合の新しい syslog アラートが追加されています。

システム、端末、宛先、およびその他のシステム グローバル ロギング パラメータを変更するには、グローバル コンフィギュレーション モードで logging コマンドを使用します。 システム ロギングのグローバル コンフィギュレーションの詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Troubleshooting, Logging, and Fault Management」を参照してください。

traceroute レポートを使用した PfR のトラブルシューティング

PfR では、**syslog** および **debug** コマンドライン インターフェイス（CLI）コマンドを使用して問題を診断することができますが、コストベース最適化と traceroute レポートに対する OER のサポート機能により、traceroute レポートもサポートされるようになりました。 traceroute レポートの使用により、PfR では、traceroute プローブを使用してホップバイホップ ベースの遅延が判断され、トラフィック クラスのパフォーマンスが報告されます。

traceroute レポートが導入される前は、出口リンクでトラフィック クラスに予期しないラウンドトリップ遅延値が報告されるような状況でも、ホップ単位の遅延を測定する方法はありませんでした。 PfR では、ユーザ データグラム プロトコル（UDP）の traceroute を使用してホップ単位の遅延統計が収集されます。 traceroute は、所定の IP アドレスまたはホスト名を持つデバイスへのルートをトレースするものとして定義され、デバイスへのパスに存在する問題の場所を検出するのに役立ちます。 デフォルトでは従来の UDP ベースの traceroute が使用されますが、ファイアウォールを通じて許可される TCP SYN パケットを特定のポートに送信するよう、PfR を設定することができます。

traceroute レポートの設定は、マスター コントローラで行います。 traceroute プローブは、境界ルータの出口がソースとなります。この機能を利用することにより、ホップバイホップベースでトラフィック クラスのパフォーマンスを監視できます。 traceroute レポートがイネーブルである場合、自律システム番号、IP アドレス、および遅延測定が、プローブ ソースからターゲット プレフィックスへのホップごとに収集されます。 デフォルトでは、トラフィック クラスがポリシー違反（OOP）になった場合に限り、traceroute プローブが送信されます。 TCP ベースの traceroute は手動で設定でき、traceroute プローブの時間間隔も変更できます。 デフォルトでは、ホップ単位の遅延レポートはディセーブルになります。

traceroute プローブを設定するには、次の方法を使用します。

- 定期：traceroute プローブは、新しいプローブ サイクルごとにトリガーされます。 1 つの出口だけをプローブするオプションが選択されている場合、トラフィック クラスの現在の出口がプローブのソースとなります。すべての出口をプローブするオプションが選択されている場合、使用可能なすべての出口が traceroute プローブのソースとなります。
- ポリシーベース：traceroute プローブは、トラフィック クラスがポリシー違反状態になると自動的にトリガーされます。 PfR マップの match 句に指定されているすべてのトラフィック クラスに対して、traceroute レポートをイネーブルにすることができます。 トラフィック クラスがポリシー準拠状態に戻ると、ポリシーベースの traceroute レポートは停止します。
- オンデマンド：定期的な traceroute レポートも、すべてのパスに関するホップ単位の統計情報も不要である場合には、traceroute プローブをオンデマンドでトリガーできます。 **show pfr master prefix** コマンドのオプションのキーワードと引数を使用して、特定のパスの特定のトラフィック クラス、またはすべてのパスに関する traceroute レポートを開始できます。

パフォーマンス ルーティングの traceroute レポートの設定方法

PfR の traceroute レポートの設定

traceroute レポートを設定するには、マスター コントローラでこのタスクを実行します。 PfR アクティブ プローブを使用した場合に、ホスト アドレスが PfR プローブ メッセージに応答しないことがあります。プローブ メッセージに応答しない理由としては、ファイアウォールまたはその他のネットワークの問題が考えられますが、PfR ではそのホスト アドレスが到達不能と見なされ、プレフィックスの制御が解放されます。 traceroute レポートが導入される前は、出口リンクでトラフィック クラスに予期しないラウンドトリップ遅延値が報告されるような状況でも、ホップ単位の遅延を測定する方法はありませんでした。応答しないターゲットアドレスとホップ単位の遅延情報不足の両方を解決するには、UDP の traceroute と任意で TCP の traceroute を使用します。 traceroute レポートの設定はマスター コントローラで行いますが、traceroute プローブのソースは境界ルータ出口となります。

このタスクでは、3 つの方法を使用して traceroute プローブを設定します。 定期およびポリシーベースの traceroute レポートは、PfR マップを使用して **set traceroute reporting** (PfR) コマンドで設定します。 オンデマンドの traceroute プローブは、特定のパラメータを指定して **show pfr master prefix** コマンドを入力することによってトリガーされます。 また、このタスクでは、**traceroute probe-delay** (PfR) コマンドを使用して traceroute プローブ間の時間間隔を変更する方法も示します。

traceroute レポートがイネーブルの場合、traceroute プローブのデフォルトの時間間隔は 1000 ミリ秒です。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **traceroute probe-delay** *milliseconds*
5. **exit**
6. **pfr-map** *map-name sequence-number*
7. **match pfr learn** {**delay** | **throughput**}
8. **set traceroute reporting** [**policy** {**delay** | **loss** | **unreachable**}]
9. **end**
10. **show pfr master prefix** [**detail** | **learned** [**delay** | **throughput**] | *prefix* [**detail** | **policy** | **traceroute** [*exit-id* | *border-address* | **current**] [**now**]]]

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。 • パスワードを入力します（要求された場合）。
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	**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、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**traceroute probe-delay** *milliseconds* 例： `Router(config-pfr-mc)# traceroute probe-delay 500`	traceroute プローブ サイクルの時間間隔を設定します。 • traceroute プローブ間のデフォルトの時間間隔は 1000 ミリ秒です。 • 例では、プローブの間隔が 500 ミリ秒に設定されます。
ステップ 5	**exit** 例： `Router(config-pfr-mc)# exit`	PfR マスター コントローラ コンフィギュレーション モードを終了し、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	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map TRACEROUTE 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、TRACEROUTE という名前の PfR マップが作成されます。
ステップ 7	**match pfr learn** {**delay** | **throughput**} 例： `Router(config-pfr-map)# match pfr learn delay`	学習済みのプレフィックスに一致させるために、PfR マップ内で match 句エントリを作成します。 • 最高遅延または最高アウトバウンド スループットに基づいてプレフィックスを学習するように設定できます。

	コマンドまたはアクション	目的
		• 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、最高遅延に基づいて学習されたトラフィックを一致させる match 句エントリが作成されます。
ステップ 8	**set traceroute reporting** [**policy** {**delay** | **loss** | **unreachable**}] 例： `Router(config-pfr-map)# set traceroute reporting`	traceroute レポートをイネーブルにします。 • PfR マップには、監視対象プレフィックスが含まれている必要があります。 これらのプレフィックスは学習することも、手動で選択することもできます。 • キーワードを指定せずにこのコマンドを入力すると、継続的なモニタリングがイネーブルになります。 • ポリシー キーワードを指定してこのコマンドを入力すると、ポリシーベースの traceroute レポートがイネーブルになります。
ステップ 9	**end** 例： `Router(config-pfr-map)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show pfr master prefix** [**detail** | **learned** [**delay** | **throughput**] | *prefix* [**detail** | **policy** | **traceroute** [*exit-id* | *border-address* | **current**] [**now**]]] 例： `Router# show pfr master prefix 10.5.5.5 traceroute now`	監視対象プレフィックスのステータスを表示します。 • オンデマンドの traceroute プローブを開始するには、**current** キーワードおよび **now** キーワードを入力します。 • **current** キーワードを指定すると、現在の出口に関する最新の traceroute プローブの結果が表示されます。 • 指定の境界ルータ出口に関する traceroute プローブの結果を表示するには、*exit-id* または *border-address* 引数を入力します。 • 例では、10.5.5.55 プレフィックスに関するオンデマンドの traceroute プローブが開始されます。

パフォーマンス ルーティングの traceroute レポートの設定例

PfR の traceroute レポートの設定例

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、遅延に基づいて学習されたトラフィック クラスの継続的な traceroute レポートを設定する例を示します。

```
Router(config)# pfr master

Router(config-pfr-mc)# traceroute probe-delay 10000

Router(config-pfr-mc)# exit

Router(config)# pfr-map TRACE 10

Router(config-pfr-map)# match pfr learn delay
Router(config-pfr-map)# set traceroute reporting
Router(config-pfr-map)# end
```

次に、特権 EXEC モードで開始し、10.5.5.5 プレフィックスに関するオンデマンドの traceroute プローブを開始する例を示します。

```
Router# show pfr master prefix 10.5.5.55 traceroute current now

Path for Prefix: 10.5.5.0/24         Target: 10.5.5.5
Exit ID: 2, Border: 10.1.1.3         External Interface: Et1/0
Status: DONE, How Recent: 00:00:08 minutes old
Hop  Host            Time(ms) BGP
1    10.1.4.2        8        0
2    10.1.3.2        8        300
3    10.5.5.5        20       50
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール

関連項目	マニュアル タイトル
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

パフォーマンス ルーティングの traceroute レポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *26* : パフォーマンス ルーティングの *traceroute* レポートの機能情報

機能名	リリース	機能情報
コストベースの最適化および traceroute レポートに対する OER のサポート	Cisco IOS XE Release 3.3S	パフォーマンス ルーティングでは traceroute レポートをサポートしているので、ホップバイホップ ベースでプレフィックスのパフォーマンスを監視できます。 遅延、損失、および到達可能性の測定が、プローブ ソース（境界ルータ）からターゲットプレフィックスへのホップごとに収集されます。 この機能により、次のコマンドが導入または変更されました。 **set traceroute reporting (PfR)**、**traceroute probe-delay (PfR)**、および **show pfr master prefix**。

第 22 章

アクティブ プローブを使用した PfR 音声トラフィック最適化

このモジュールでは、音質メトリック、ジッター、平均オピニオン評点（MOS）に基づいた音声トラフィックのアウトバウンド最適化をサポートするパフォーマンス ルーティング（PfR）ソリューションについて説明します。 ジッターおよびMOSは、音声トラフィック向けの重要な定量的品質メトリックであり、これらの音質メトリックはPfRアクティブ プローブを使用して測定します。

PfRは、ネットワーク間の複数の接続に対し、自動ルート最適化と負荷分散を行います。 PfRは、IPトラフィックを監視してから、プレフィック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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表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シスコ 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、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。

アクティブ プローブを使用した PfR 音声トラフィック最適化の前提条件

音声トラフィックの PfR 最適化を実装する前に、PfR の動作原理と PfR ネットワーク コンポーネントのセットアップ方法を理解しておく必要があります。 詳細については、「パフォーマンス ルーティングの理解」、「ベーシック パフォーマンス ルーティングの設定」、および「アドバンスド パフォーマンス ルーティングの設定」のモジュールを参照してください。

アクティブ プローブを使用した PfR 音声トラフィック最適化に関する情報

IP ネットワークの音声品質

IP ネットワークで伝送される音声パケットとデータ パケットに違いはありません。 旧来の公衆電話回線（POTS）では、音声トラフィックは定義済みのパスを使用して回線交換網で伝送され、通話中、各電話コールに専用の接続が割り当てられます。 POTS を使用する音声トラフィックにはリソースの競合に関する問題はありませんが、IP ネットワーク経由の音声トラフィックでは、遅延、ジッター、パケット損失など、通話品質に影響を与える要因に対処する必要があります。

遅延

音声パケットの遅延（レイテンシともいう）は、パケットが送信元デバイスから送信されて宛先デバイスに到着するまでの遅れとして定義されています。 遅延は、一方向遅延またはラウンドトリップ遅延として測定されます。 レイテンシの最大の原因は、ネットワーク伝送遅延です。 ラウンドトリップ遅延は、通話能力に影響し、平均オピニオン評点（MOS）の計算に使用されます。 一方向遅延は、ネットワーク問題の診断に使用されます。 200 ミリ秒の遅延に気づいた発信者は、パケット遅延のため、相手の応答中に話そうとすることがあります。 ITU-T G.114 で規定されている電話業界標準では、一方向遅延の最大値を 150 ミリ秒以下にするよう推奨しています。 一方向遅延が 150 ミリ秒を超えると、音声品質に影響が出ます。 300 ミリ秒以上のラウンドトリップ遅延が発生すると、話者同士が同時に発話してしまうことがあります。

ジッター

ジッターはパケット間の遅延がばらつくことを指します。 複数のパケットが発信元から宛先に連続的に送信された場合、たとえば 10 ms 間隔で送信された場合、ネットワークが理想的に動作していれば、宛先は 10 ms 間隔でパケットを受信します。 しかし、ネットワーク内に遅延（キューイング、代替ルートを介した受信など）が存在する場合、パケット間の到着遅延は、10 ms より大きい場合も、10 ms より小さい場合もあります。 この例を使用すると、正のジッター値は、パケットが 10 ms を超える間隔で到着することを示します。 パケットが 12 ms 間隔で到着する場合、正のジッターは 2 ms です。パケットが 8 ms 間隔で到着する場合、負のジッターは 2 ms です。 Voice over IP（VoIP）など遅延に影響されやすいネットワークでは、正のジッター値は望ましくありません。0 のジッター値が理想的です。

パケット損失

パケット損失は、インターフェイスの障害、パケットのルーティング先の間違い、またはネットワークの輻輳によって発生する可能性があります。 音声トラフィックのパケット損失はサービスの低下を招き、発信者には音声が途切れて聞こえます。 パケット損失の平均値が低くても、音声品質は短期間の連続するパケット損失の影響を受ける場合があります。

平均オピニオン評点（MOS）

すべての要因が音声品質に影響を与えるので、音声品質の測定方法については多くの人々が疑問を持っています。 ITU などの標準化団体によって、P.800（MOS）および P.861（Perceptual Speech Quality Measurement（PSQM））という 2 つの重要な勧告が作成されています。 P.800 は、音声品質の平均オピニオン評点を算出する方法の定義に関するものです。 MOS スコアの範囲は、最低の音声品質を表す 1 から最高を表す 5 までです。 MOS 4 は、「トール品質」音声と見なされます。

PfR で使用されるプローブ

PfR はいくつかの IP SLA プローブを使用して、判断に必要なデータの収集に役立てます。

Cisco IOS IP SLA

Cisco IOS IP SLA は Cisco IOS ソフトウェアの組み込み機能で、これを使用すると IP アプリケーションおよびサービスの IP サービス レベルの分析、生産性の改善、運用コストの削減、ネットワークの輻輳や停止の低減などが可能になります。 IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。 Cisco ルータで使用できる IP SLA Responder を宛先デバイス上でイネーブルにすると、測定データの精度が向上します。 IP SLA の詳細については、『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

PfR で使用されるアクティブ プローブ タイプ

設定可能なアクティブ プローブのタイプは次のとおりです。

ICMP エコー：ターゲット アドレスに ping が送信されます。 アクティブ プローブが自動的に生成されると、PfR はデフォルトにより ICMP エコー プローブを使用します。 ICMP エコー プローブの設定には、ターゲットデバイスからの大きな協力を必要としません。 しかし、プローブを繰

アクティブ プローブを使用した PfR 音声トラフィック最適化

り返し行うと、ターゲット ネットワーク内で侵入検知システム（IDS）アラームが発生することがあります。 自身の管理制御下にないターゲット ネットワークで IDS が設定されている場合には、ターゲット ネットワークの管理者に通知することを推奨します。

ジッター：ジッター プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 設定されるポート番号に関係なく、ターゲット デバイスのリモート レスポンダはイネーブルにする必要があります。

TCP 接続：TCP 接続プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 TCP メッセージの設定で、既知の番号である TCP ポート番号 23 以外のポート番号を使用するように指定されている場合は、リモート レスポンダをイネーブルにする必要があります。

UDP エコー：UDP エコー プローブがターゲット アドレスに送信されます。 ターゲット ポート番号を指定する必要があります。 設定されるポート番号に関係なく、ターゲットデバイスのリモート レスポンダはイネーブルにする必要があります。

プローブの頻度

デフォルトでは、PfR で使用されるプローブの頻度は 60 秒に設定されています。ただし、2 つのプローブ間の時間間隔を短く設定することで、ポリシーごとにこの頻度を増やすことができます。プローブの頻度を増やすと応答時間が短縮され、MOS 低カウント率の近似値をより正確に求めることができます。

アクティブ プローブを使用した PfR 音声トラフィック最適化

アクティブ プローブを使用して音声トラフィックを最適化するように PfR を設定するには、いくつかの決定を行ったあと、派生タスクを実行します。 最初のステップでは、最適化するトラフィックを識別し、プレフィックス リストまたはアクセス リストのいずれを使用するかを決定します。プレフィックス リストは、特定の送信先プレフィックスのセットを持つすべてのトラフィック（音声トラフィックも含む）を識別するために使用します。アクセス リストは、特定の送信先プレフィックスを持ち、特定のプロトコル経由で伝送される音声トラフィックだけを識別するために使用します。

音声トラフィック最適化の 2 番目のステップでは、**active-probe** コマンドまたは **set active-probe** コマンドを使用してアクティブ プローブを設定し、使用するアクティブ プローブのタイプを指定します。 PfR では、アクティブ プローブに強制ターゲット割り当てを設定することもできます。

音声最適化の最後のステップでは、PfR ポリシーを設定し、PfR で識別されたトラフィックに適用するパフォーマンス メトリックを指定します。

PfR 音声パフォーマンス メトリック

PfR 音声トラフィック最適化は、音声パフォーマンス メトリック、遅延、パケット損失、および MOS に基づいた音声トラフィックのアウトバウンド最適化をサポートします。 遅延、パケット損失、ジッター、および MOS は、音声トラフィック用の重要な定量的品質メトリックで、PfR アクティブ プローブを使用してこれらの音質メトリックが測定されます。 IP SLA ジッター プローブ

はPfRと統合されて、遅延およびパケット損失のほか、ジッター（送信元から宛先まで）とMOSスコアを測定します。 ジッター プローブでは、UDP エコー プローブの場合と同様に、リモートサイドの応答が必要です。 PfR に IP SLA ジッター プローブ タイプを統合することで、PfR の音声トラフィック最適化機能が向上します。 PfR ポリシーでは、音声パフォーマンス メトリック（遅延、パケット損失、ジッター、MOS）にしきい値とプライオリティ値を設定できます。

ジッターを測定するように PfR ポリシーを設定する場合は、しきい値だけを指定し、（その他の PfR 機能で使用される）相対的変化は指定しません。これは、音声トラフィックでは、ジッターの相対的変化は意味を持たないからです。 たとえば、ジッターが 5 ミリ秒から 25 ミリ秒に変化するのと、15 ミリ秒から 25 ミリ秒に変化するのとでは、音声品質の低下という観点でいえば違いはありません。 短期間の平均（最後の 5 プローブを測定）ジッターがジッターしきい値よりも高い場合、そのプレフィックスはジッターによるポリシー違反状態であると見なされます。 この場合、PfR はすべての出口をプローブし、ジッターが最も少ない出口が最良出口として選択されます。

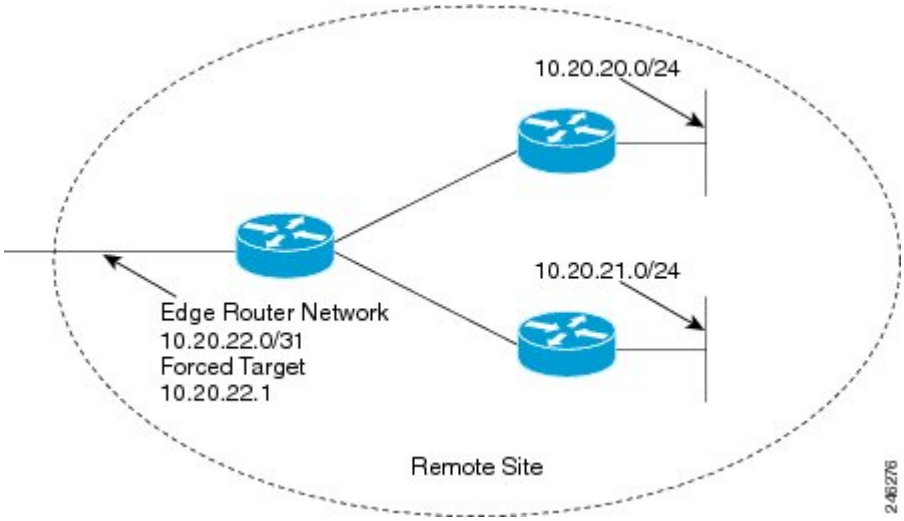
MOSは、さまざまな方法で機能します。 MOSの平均値は重要ではありませんが、MOS値がMOSしきい値を下回る回数は重要な意味を持ちます。 たとえば、MOS しきい値が 3.85 に設定され、10 回のうち 3 回の MOS 測定で測定値が 3.85 の MOS しきい値を下回った場合、MOS 低カウント率は 30 % です。 **show** コマンドの出力では、アクティブに監視された MOS パケットの数が、しきい値を下回った割合と共に ActPMOS フィールドに表示されます。 MOS 測定値がしきい値をわずかに下回っている場合は、この割合が切り捨てられて 0 の ActPMOS 値が表示されることがあります。 MOS 測定が設定されたポリシーを PfR が実行する場合は、MOS しきい値と MOS 低カウント率の両方が考慮されます。 短期間（最後の 5 プローブの平均）の MOS 低カウント率が、設定されたMOS低カウント率よりも高い場合、プレフィックスはポリシー違反状態であると見なされます。 この場合、PfR はすべての出口をプローブし、MOS 値が最も高い出口が最良出口として選択されます。

PfR アクティブ プローブの強制ターゲット割り当て

OER テクノロジーの以前のリリースでは、PfR アクティブ プローブ ターゲットは最長一致プレフィックスに割り当てられます。 しかし、場合によっては送信先プレフィックスと一致しない

ターゲットを使用することもありえます。 次の図の例は、最長一致プレフィックスを使用するよりも、PfR 強制ターゲット割り当てを設定するほうが適切なシナリオを示しています。

図 *23*：*PfR* 強制ターゲット割り当てシナリオ



前述の図では、ネットワーク 10.20.21.0/24 または 10.20.22.0/24 の IP アドレス 10.20.22.1 を（ネットワークのエッジで）プローブします。 ネットワーク内でジッターが発生する可能性は少ないので、ネットワークのエッジをプローブすると、最終的な宛先のプローブとほぼ同等の測定値が得られます。

強制ターゲット割り当てを使用すると、最長一致プレフィックスでなくても、プレフィックスのグループまたはアプリケーションにターゲットを割り当てることができます。 ターゲットの割り当てによって、エンド ホストへの遅延ではなく、ネットワークのエッジへの正確な遅延を判定できます。

アクティブ プローブを使用した PfR 音声トラフィック最適化の設定方法

最適化するトラフィックの識別にプレフィックス リストとアクセス リストのいずれを使用するかに応じて、次に示す 2 つのオプション タスクのいずれかを実行します。 3 つ目のタスクは、アクセス リストを使用して識別されたトラフィックに使用できます。強制ターゲット割り当ての使用方法もここで説明します。プレフィックス リストを使用して特定されるトラフィックで使用できる設定例については、「例：アクティブ プローブを使用したトラフィック（音声トラフィックを含む）の最適化」を参照してください。

プレフィックス リストを使用した PfR のトラフィックの識別

PfR を使用してトラフィックを測定するには、先にトラフィックを識別する必要があります。 プレフィックス リストを使用してこのタスクを実行し、PfR でプローブするトラフィックを識別します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length*| **permit** *network*/*length*}
4. **exit**

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。 • パスワードを入力します（要求された場合）。
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	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length*| **permit** *network*/*length*} 例： `Router(config)# ip prefix-list TRAFFIC_PFX_LIST seq 10 permit 10.20.21.0/24`	IP プレフィックス リストを作成します。 • IP プレフィックス リストは、PfR マスター コントローラでモニタリングするプレフィックスを手動で選択するために使用されます。 • マスター コントローラは、正確なプレフィックス（/32）、所定のプレフィックス長、または所定のプレフィックス長とそれよりも短いプレフィックス（/16 よりも短い /24 など）を監視および制御できます。 • IP プレフィックス リストで指定されたプレフィックスは、**match ip address**（PfR）コマンドを使用して PfR マップにインポートします。 • 例では、10.20.21.0/24 サブネットからのプレフィックスを許可する、TRAFFIC_PFX_LIST という名前の IP プレフィックス リストが作成されます。

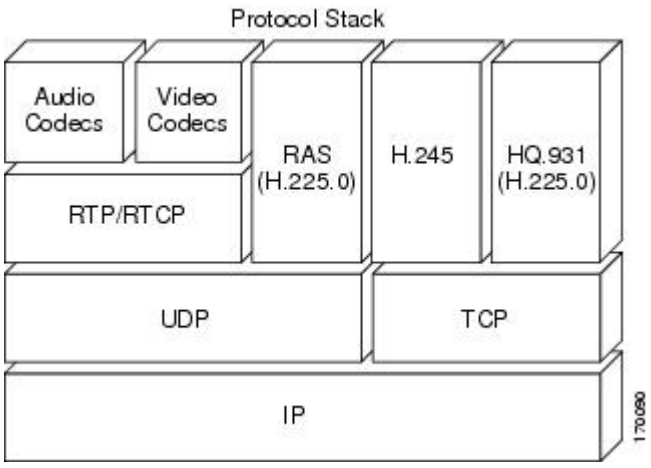
	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

アクセスリストを使用して最適化する音声トラフィックを識別する方法

音声トラフィックを測定するには、先に音声トラフィックを識別する必要があります。 アクセスリストを使用してこのタスクを実行し、音声トラフィックを識別します。

音声トラフィックは、基本となる IP ネットワークでさまざまなプロトコルとストリームを使用します。 次の図は、IP 経由の音声トラフィック伝送に使用できるプロトコル オプションを示しています。 音声用シグナリング トラフィックの大半は TCP 経由で伝送されます。 大半の音声コールは、ユーザ データグラム プロトコル（UDP）および Real-Time Transport Protocol（RTP）経由で伝送されます。 所定の範囲の宛先ポート番号を使用して音声コール トラフィックを UDP 経由で伝送するように音声デバイスを設定できます。

図 *24*：音声トラフィックに使用できるプロトコル スタック オプション



手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} *access-list-name*
4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **exit**

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。 • パスワードを入力します（要求された場合）。
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	**ip access-list** {**standard** | **extended**} *access-list-name* 例： `Router(config)# ip access-list extended VOICE_ACCESS_LIST`	IP アクセス リストを名前で定義します。 • PfR は、名前付きアクセス リストだけをサポートします。 • この例では、VOICE_ACCESS_LIST という名前の拡張 IP アクセス リストが作成されます。
ステップ 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Router(config-ext-nacl)# permit udp any range 16384 32767 10.20.20.0 0.0.0.15 range 16384 32767`	拡張アクセス リストを定義します。 • 任意のプロトコル、ポート、またはその他の IP パケット ヘッダー値を指定できます。 • この例では、任意の送信元から 10.20.20.0/24 の送信先プレフィックスに伝送される、宛先ポート番号 16384 ～ 32767 の UDP トラフィックをすべて識別するように設定されます。この特定の UDP トラフィックが最適化されます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config)# exit`	（任意）グローバル 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。

ターゲット割り当てを使用した PfR 音声プローブの設定

最適化するトラフィックを識別したら（この例では、アクセス リストを使用して音声トラフィックを識別）、このタスクを実行して PfR ジッタープローブを設定し、ジッタープローブの結果を割り当てて、識別されたトラフィックを最適化します。 この例で、PfR アクティブ音声プローブには、通常の最長一致割り当てターゲットではなく、PfR の強制ターゲットが割り当てられます。ソース デバイスで PfR ジッタープローブを設定する前に、ターゲット デバイス（動作のターゲット）で IP SLA Responder をイネーブルにする必要があります。 IP SLA Responder を使用できるのは、Cisco IOS ソフトウェアベースのデバイスだけです。 IP SLA Responder が稼働するネットワーク デバイスで次のタスクを開始します。

（注） IP SLA Responder が稼働するデバイスは、PfR 用に設定されている必要はありません。

（注） PfR マップで適用されたポリシーによって、グローバル ポリシーの設定が上書きされることはありません。

はじめる前に

このタスクを設定する前に、アクセス リストを使用して最適化する音声トラフィックを識別する方法を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. PfR マスター コントローラになっているネットワーク デバイスに移動します。
6. **enable**
7. **configure terminal**
8. **pfr-map** *map-name sequence-number*
9. **match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*}
10. **set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]
11. **set probe frequency** *seconds*
12. **set jitter threshold** *maximum*
13. **set mos** {**threshold** *minimum* **percent** *percent*}
14. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
15. **set resolve mos priority** *value* **variance** *percentage*
16. **set delay** {**relative** *percentage* | **threshold** *maximum*}
17. **exit**
18. **pfr master**
19. **policy-rules** *map-name*
20. **end**
21. **show pfr master active-probes** [**appl**| **forced**]
22. **show pfr master policy** {*sequence-number*|*policy-name* | **default**}

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。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**ip sla monitor responder** 例： `Router(config)# ip sla monitor responder`	IP SLA Responder をイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル 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 5	PfR マスター コントローラになっているネットワーク デバイスに移動します。	--
ステップ 6	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 7	**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 8	**pfr-map** *map-name sequence-number* 例： `Router(config)# pfr-map TARGET_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィックスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは最初に IP プレフィックス リストに定義してから、ステップ 9 で **match ip address** (PfR) コマンドを使用して適用します。 • 例では、TARGET_MAP という名前の PfR マップが作成されます。
ステップ 9	**match ip address** {**access-list** *access-list-name*| **prefix-list** *prefix-list-name*} 例： `Router(config-pfr-map)# match ip address access-list VOICE_ACCESS_LIST`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィックスを参照します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、VOICE_ACCESS_LIST という名前の IP アクセス リストが、PfR マップ内の一致基準として設定されます。 アクセス リストは「アクセス リストを使用して最適化する音声トラフィックを識別する方法」タスクで作成されています。

	コマンドまたはアクション	目的
ステップ 10	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] 例： `Router(config-pfr-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	set 句エントリを作成して、アクティブプローブのターゲットプレフィックスを割り当てます。 • プレフィックスのターゲット IP アドレスを指定し、インターネット制御メッセージ プロトコル（ICMP）エコー（ping）メッセージを使用してアクティブな監視を行うには、**echo** キーワードを使用します。 • プレフィックスのターゲット IP アドレスを指定し、ジッター メッセージを使用してアクティブな監視を行うには、**jitter** キーワードを使用します。 • プレフィックスのターゲット IP アドレスを指定し、インターネット制御メッセージ プロトコル（ICMP）エコー（ping）メッセージを使用してアクティブな監視を行うには、**tcp-conn** キーワードを使用します。 • プレフィックスのターゲット IP アドレスを指定し、インターネット制御メッセージ プロトコル（ICMP）エコー（ping）メッセージを使用してアクティブな監視を行うには、**udp-echo** キーワードを使用します。 • 例では、set 句エントリを作成し、ジッターを使用してアクティブに監視するプレフィックスのターゲット IP アドレスと特定のポート番号を指定しています。
ステップ 11	**set probe frequency** *seconds* 例： `Router(config-pfr-map)# set probe frequency 10`	set 句エントリを作成して、PfR アクティブ プローブの頻度を設定します。 • 指定した IP プレフィックスのアクティブ プローブ モニタリングの間隔を秒単位で設定するには、*seconds* 引数を使用します。 • 例では、アクティブ プローブ頻度を 10 秒に設定する set 句を作成しています。
ステップ 12	**set jitter threshold** *maximum* 例： `Router(config-pfr-map)# set jitter threshold 20`	set 句エントリを作成して、ジッターしきい値を設定します。 • 最大ジッター値をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じPfRマップ シーケンスで一致するトラフィックのジッターしきい値を 20 に設定する set 句を作成しています。

	コマンドまたはアクション	目的
ステップ 13	**set mos** {**threshold** *minimum* **percent** *percent*} 例： `Router(config-pfr-map)# set mos threshold 4.0 percent 30`	set 句エントリを作成して、代替出口を選択するかどうかの判断に使用される MOS しきい値および割合値を設定します。 • 最低 MOS 値を設定するには **threshold** キーワードを使用します。 • MOS しきい値を下回る MOS 値の割合を設定するには **percent** キーワードを使用します。 • PfR は、5 分間隔で記録された MOS しきい値を下回る MOS 値の割合を計算します。 この割合値が、設定した割合値またはデフォルト値を上回る場合、マスター コントローラは代替出口リンクを検索します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックのしきい値 MOS 値を 4.0 に設定し、割合値を 30% に設定する set 句を作成しています。
ステップ 14	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} 例： `Router(config-pfr-map)# set resolve jitter priority 1 variance 10`	set 句エントリを作成し、ポリシー プライオリティを設定するか、ポリシーの競合を解決します。 • このコマンドは、同じプレフィックスに対して複数のポリシーが設定されている場合に、ポリシー タイプのプライオリティを設定するために使用されます。 このコマンドが設定されている場合、最高プライオリティのポリシーが選択されて、ポリシー決定を行います。 • プライオリティ値を指定するには、**priority** キーワードを使用します。1 という番号を設定すると、ポリシーに最高プライオリティが割り当てられます。 10 という番号を設定すると、最低プライオリティが割り当てられます。 • 各ポリシーには、異なるプライオリティ番号を割り当てる必要があります。 • ユーザ定義のポリシーに許容分散を設定するには、**variance** キーワードを使用します。 このキーワードでは、出口リンクまたはプレフィックスがユーザ定義のポリシー値と異なっても、まだ同等であると見なす許容割合が設定されます。 • 分散は、コストまたは範囲ポリシーには設定できません。 • 例では、音声トラフィックのジッター ポリシーのプライオリティを 1 に設定する set 句が作成されます。 プレフィックスがポリシー違反と判定されるまでに、ジッター統計情報で 10 % の差異が許容されるように分散が設定されます。

	コマンドまたはアクション	目的
ステップ 15	**set resolve mos priority** *value* **variance** *percentage* 例： `Router(config-pfr-map)# set resolve mos priority 2 variance 15`	set 句エントリを作成し、ポリシー プライオリティを設定するか、ポリシーの競合を解決します。 • 例では、音声トラフィックの MOS ポリシーのプライオリティを 2 に設定する set 句が作成されます。プレフィックスがポリシー違反と判定されるまでに、MOS 値で 15 % の差異が許容されるように分散が設定されます。 （注） この例では、このタスクに適用可能な構文だけが使用されています。詳細については、ステップ 14 を参照してください。
ステップ 16	**set delay** {**relative** *percentage* | **threshold** *maximum*} 例： `Router(config-pfr-map)# set delay threshold 100`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 100 ミリ秒に設定する set 句を設定しています。
ステップ 17	**exit** 例： `Router(config-pfr-map)# exit`	PfR マップ コンフィギュレーション モードを終了し、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 18	**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境界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 19	**policy-rules** *map-name* 例： `Router(config-pfr-mc)# policy-rules TARGET_MAP`	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、PfR マップからマスター コントローラ コンフィギュレーションに設定を適用します。 • 新しい PfR マップ名でこのコマンドを再入力すると、以前の設定がただちに上書きされます。この動作は、定義済みの PfR 間での迅速な選択および切り替えを可能にするように設計されています。

	コマンドまたはアクション	目的
		• 例では、TARGET_MAP という名前の PfR マップから設定が適用されます。
ステップ 20	**end** 例： `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 21	**show pfr master active-probes** [**appl**| **forced**] 例： `Router# show pfr master active-probes forced`	PfR マスター コントローラ上のアクティブ プローブに関する接続情報およびステータス情報を表示します。 • このコマンドからの出力には、アクティブ プローブのタイプおよび宛先、アクティブプローブのソースである境界ルータ、アクティブプローブに使用されるターゲットプレフィックス、およびプローブが学習済みだったか、または設定済みだったかが表示されます。 • 出力をフィルタリングして、マスター コントローラによって最適化されるアプリケーションに関する情報を表示するには、**appl** キーワードを使用します。 • 割り当てられたすべての強制ターゲットを表示するには、**forced** キーワードを使用します。 • 例では、強制ターゲット割り当てで設定された音声トラフィック用に生成されたアクティブ プローブに関する接続情報およびステータス情報が表示されます。
ステップ 22	**show pfr master policy** {*sequence-number*|*policy-name* | **default**} 例： `Router# show pfr master policy TARGET_MAP`	PfR マスター コントローラ上のポリシー設定を表示します。 • PfR マップを設定して、出口リンクでの送信中に PfR が許可するパケット損失の相対割合または最大数を指定するには、このコマンドを使用します。 パケット損失がユーザ定義またはデフォルトの値を超えると、マスター コントローラはその出口リンクをポリシー違反であると判断します。 • 指定した PfR マップ シーケンスのポリシー設定を表示するには *sequence-number* 引数を使用します。 • 指定した PfR ポリシー マップ名のポリシー設定を表示するには *policy-name* 引数を使用します。 • デフォルトのポリシー設定だけを表示するには、**default** キーワードを使用します。 • 例では、TARGET_MAP ポリシーで指定されたポリシー設定が表示されます。

	コマンドまたはアクション	目的

例

次に、**show pfr master active-probes forced** コマンドからの出力例を示します。 出力はフィルタリングされ、強制ターゲット割り当てで設定された音声トラフィック用に生成されたアクティブ プローブに関する接続情報およびステータス情報だけが表示されます。

```
Router# show pfr master active-probes forced
OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
The following Forced Probes are running:
Border          State    Policy            Type     Target          TPort
10.20.20.2     ACTIVE    40                jitter   10.20.22.1      3050
10.20.21.3     ACTIVE    40                jitter   10.20.22.4      3050
```

アクティブ プローブを使用した PfR 音声トラフィック最適化の設定例

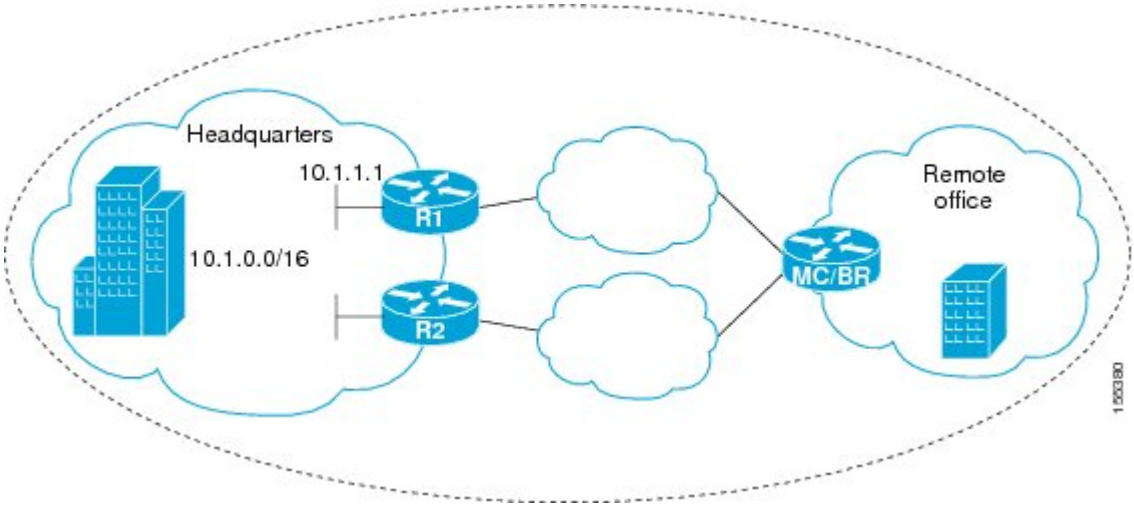
次の例に、アクセス リストを使用して、PfR で最適化する音声トラフィックだけを識別する方法と、プレフィックス リストを使用して、PfR で最適化するトラフィック（音声トラフィックを含む）を識別する方法を示します。

アクティブ プローブを使用した音声トラフィックだけの最適化例

次の図では、リモート オフィス ネットワークからの最良パスを選択するために、リモート オフィスから発信されて本社で終端する音声トラフィックを最適化する必要があります。 ネットワーク

内で音声（トラフィック）品質が低下する可能性は少ないので、ネットワークのエッジをプローブすると、最終的な宛先のプローブとほぼ同等の測定値が得られます。

図 *25*：アクティブ プローブを使用して音声トラフィックを最適化する *PfR* のネットワーク トポロジ



この設定は、最良パフォーマンス パスを使用するために音声トラフィックを最適化します。ただし、同じネットワーク（10.1.0.0/16）を宛先とするその他のすべてのトラフィックは、デバイス上で設定された BGP などの従来型ルーティング プロトコルで指定された最良パスを通過します。この最適化の一部として、PfR はポリシーベース ルーティング（PBR）を使用して、デバイス内の音声トラフィックに最良出口リンクを設定します。

IP SLA Responder をイネーブルにするには、前述の図の本社ネットワークのエッジ ルータ R1 で次のように設定します。

```
enable
configure terminal
 ip sla responder
 exit
```

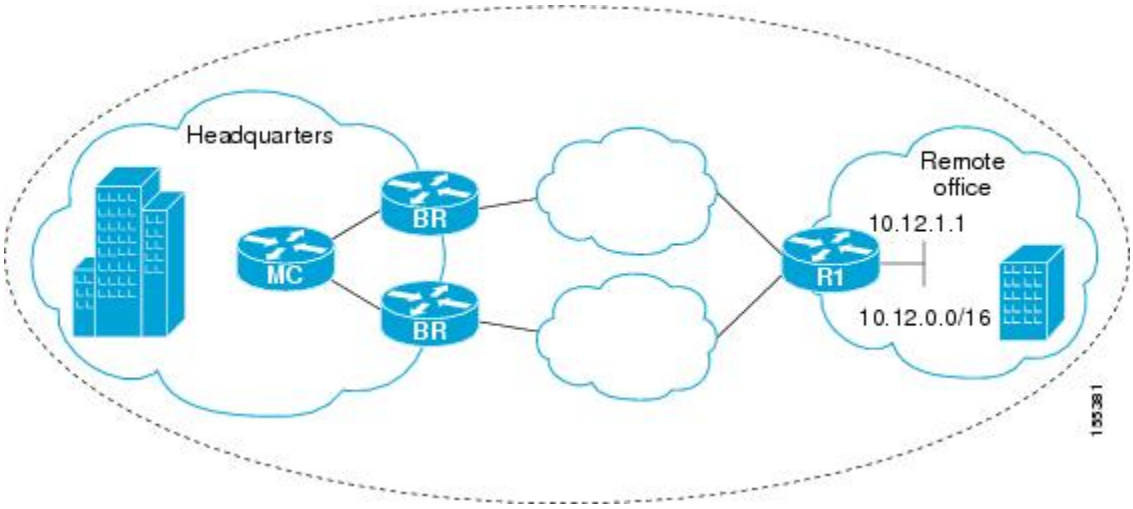
アクティブプローブを使用して音声トラフィックを最適化するには、前述の図のリモートオフィス ネットワークのエッジ ルータ MC/BR（PfR マスター コントローラであり、境界ルータでもある）で次のように設定します。

```
enable
configure terminal
ip access-list extended Voice_Traffic
 10 permit udp any 10.1.0.0 0.0.255.255 range 16384 32767
 exit
pfr-map Voice_MAP 10
 match ip address access-list Voice_Traffic
 set active-probe jitter 10.1.1.1 target-port 1025 codec g711alaw
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

アクティブプローブを使用したトラフィック（音声トラフィックを含む）の最適化例

次の図では、本社ネットワークからリモートオフィスネットワークに向かうトラフィックを音声トラフィックメトリックに基づいて最適化する必要があります。音声トラフィックは、本社からリモート オフィス ネットワークに伝送される最も重要なトラフィック クラスのうちのひとつです。このため、音声トラフィックの最適化を優先する必要があります。 ネットワーク内で音声パケットの品質が低下する可能性は少ないので、ネットワークのエッジをプローブすると、最終的な宛先のプローブとほぼ同等の測定値が得られます。

図 *26*：アクティブ プローブを使用してすべてのトラフィックを最適化する *PfR* のネットワーク トポロジ



この設定では、音声トラフィックも含めて、10.12.0.0/16 ネットワークを宛先とするすべてのトラフィックが最適化されます。 PfR の最適化は、アクティブ プローブを使用した音声パフォーマンス メトリックの測定値としきい値に基づいて行われます。最適化の一部として、PfR は BGP ルートまたはスタティック ルートを本社ネットワークに導入します。 BGP およびスタティック ルートの最適化については、「パフォーマンス ルーティングの理解」モジュールを参照してください。

IP SLA Responder をイネーブルにするには、前述の図のリモート オフィス ネットワークのエッジ ルータ R1 で次のように設定します。

```
enable
configure terminal
 ip sla responder
 exit
```

アクティブ プローブを使用してすべてのトラフィック（音声トラフィックを含む）を最適化するには、前述の図の本社ネットワークにあるいずれかの BR ルータで次のように設定します。

```
enable
configure terminal
 ip prefix-list All_Traffic_Prefix permit 10.12.0.0/16
```

```
 pfr-map Traffic_MAP 10
 match ip address prefix-list All_Traffic_Prefix
 set active-probe jitter 10.12.1.1 target-port 1025 codec g711alaw
! port 1025 for the target probe is an example.
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS PfR のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS Performance Routing Command Reference』
Cisco IOS XE Release での基本的な PfR 設定	「ベーシック パフォーマンス ルーティングの設定」モジュール
Cisco IOS XE Release 3.1 および 3.2 の境界ルータ専用機能の設定に関する情報	「パフォーマンス ルーティング境界ルータ専用機能」モジュール
Cisco IOS XE Release のパフォーマンス 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	「パフォーマンス ルーティングの理解」モジュール
Cisco IOS XE Release でのアドバンスド PfR 設定	「アドバンスド パフォーマンス ルーティングの設定」モジュール
IP SLA の概要	「Cisco IOS IP SLAs Overview」モジュール
シスコの DocWiki コラボレーション環境の PfR 関連のコンテンツへのリンクがある PfR ホームページ	PfR:Home

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 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

アクティブ プローブを使用した PfR 音声トラフィック最適化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 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。

プラットフォームのサポートおよびシスコ 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、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。

表 *27*：アクティブ プローブを使用した *PfR* 音声トラフィック最適化の機能情報

機能名	リリース	機能情報
PfR 音声トラフィック最適化	Cisco IOS XE Release 3.3S	PfR 音声トラフィック最適化機能は、音質メトリック、ジッター、平均オピニオン評点（MOS）に基づいた音声トラフィックのアウトバウンド最適化をサポートします。ジッターおよび MOS は、音声トラフィック向けの重要な定量的品質メトリックであり、これらの音質メトリックは PfR アクティブ プローブを使用して測定します。 この機能により、次のコマンドが導入または変更されました。**active-probe (PfR)**、**jitter (PfR)**、**mos (PfR)**、**resolve (PfR)**、**set active-probe (PfR)**、**set jitter (PfR)**、**set mos (PfR)**、**set probe (PfR)**、**set resolve (PfR)**、**show pfr master active-probes**、**show pfr master policy**、および **show pfr master prefix**。