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、Performance Routing（PfR; パフォーマンス ルーティング）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、「Cisco IOS Optimized Edge Routing Overview」モジュールを参照してください。

機能情報の検索

このモジュールに記載されている機能の一部が、ご使用のソフトウェア リリースでサポートされていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「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」（P.32）を参照してください。

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

マニュアルの内容

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

- 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、あるいは 12.2SR または 12.2SX のイメージを実行している場合は、『*Cisco IOS Optimized Edge Routing Configuration Guide*』を参照してください。
- 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 Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）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、Policy-Based Routing（PBR; ポリシーベース ルーティング）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

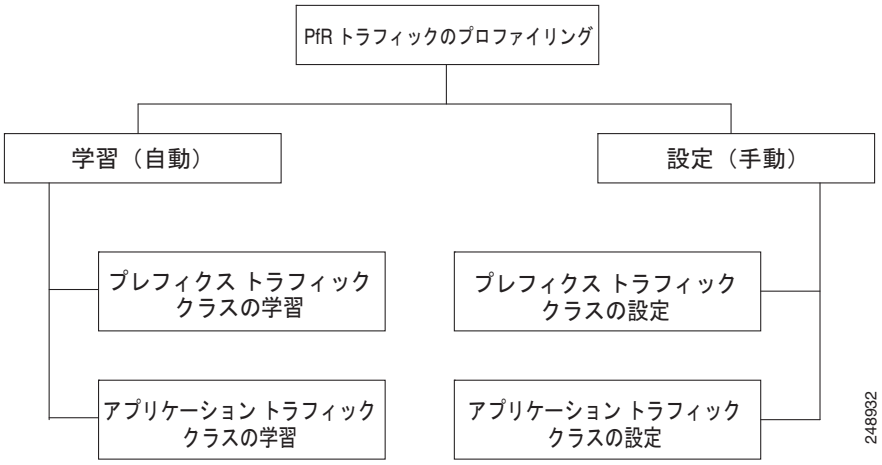
プロファイル フェーズの概念

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 はボーダー 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、Monitored Traffic Class（MTC; 監視対象トラフィック クラス）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 プロセスとそのコンポーネントの全体的な構造については、図 1 を参照してください。

図 1　　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。

図 1 の各部分の詳細については、次の項で説明します。

- 「自動トラフィック クラス学習」（P.3）
- 「トラフィック クラスの手動設定」（P.6）

自動トラフィック クラス学習

PfR は、ボーダー 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クス トラフィック クラスの学習」（P.4）
- 「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」（P.4）
- 「学習リスト コンフィギュレーション モード」（P.5）

PfR を使用したプレフィクス 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クスを判定します。スループット プレフィクスは高い順にソートされます。遅延学習では、Round-Trip Response Time（RTT; ラウンドトリップ応答時間）が最大のプレフィクスを判定し、これらのプレフィクスの RTT を低減するために、最大遅延プレフィクスを最適化します。遅延プレフィクスは、遅延時間の長い順にソートされます。

PfR は、次の 2 種類のプレフィクスを自動的に学習できます。

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

BGP インバウンド最適化機能に、内部プレフィ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 は内部プレフィクスを選択し、自律システム外のプレフィクスから自律システム内のプレフィ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クスの詳細については、「BGP Inbound Optimization Using Performance Routing」モジュールを参照してください。

自動プレフィクス学習は、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。自動プレフィクス学習がイネーブルの場合、ボーダー ルータ上でプレフィ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、ボーダー ルータ上でプレフィ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。プレフィクスは、プレフィ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、Differentiated Services Code Point（DSCP; DiffServ コード ポイント）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。自動学習の対象として、次の 4 種類のトラフィック クラスをプロファイルできます。

- 宛先プレフィ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
- 宛先プレフィクスを定義するオプションのプレフィクス 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
- 宛先プレフィクスを定義するオプションのプレフィクス リスト付きの Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）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（Cisco IOS Release 12.4(20)T で導入）

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、「Static Application Mapping Using Performance Routing」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。Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）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、「Performance Routing with NBAR/CCE Application Recognition」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クス トラフィック クラスの設定」（P.6）
- 「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」（P.7）

PfR を使用したプレフィクス 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クスまたはプレフィクス範囲を選択するには、IP プレフィクス 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。プレフィクス リストを使用して、正確なプレフィ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クスを監視し、制御できます。完全に一致するプレフィ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クスおよびより限定されたプレフィクス（たとえば、10.0.0.0/8 le 32 プレフィクスを設定すると、10.1.0.0/16 プレフィクスおよび 10.1.1.0/24 プレフィクスを含みます）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 クラスのプレフィクスまたはプレフィ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ボーダー 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 種類のプレフィクスを使用して、IP プレフィクス 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。

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

BGP インバウンド最適化機能に、内部プレフィ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クスから自律システム内のプレフィ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クスの詳細については、「BGP Inbound Optimization Using Performance Routing」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 Access Control List（ACL; アクセス コントロール リスト）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 クラスの設定でサポートされる DSCP 値、プロトコル、およびポート番号のプロファイリング。MTC リストには、プレフィクスのほか、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。手動設定の対象として、次の 4 種類のトラフィック クラスをプロファイルできます。

- 宛先プレフィ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 マッピング名と宛先プレフィクスを定義するためのプレフィクス 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 マッピング名と宛先プレフィクスを定義するためのプレフィクス 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、「Static Application Mapping Using Performance Routing」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、ダイナミックな TCP/UDP ポートの割り当てを利用する Web ベースおよび分類が困難なアプリケーションやプロトコルなど、幅広いプロトコルおよびアプリケーションを認識し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、「Performance Routing with NBAR/CCE Application Recognition」機能を参照してください。

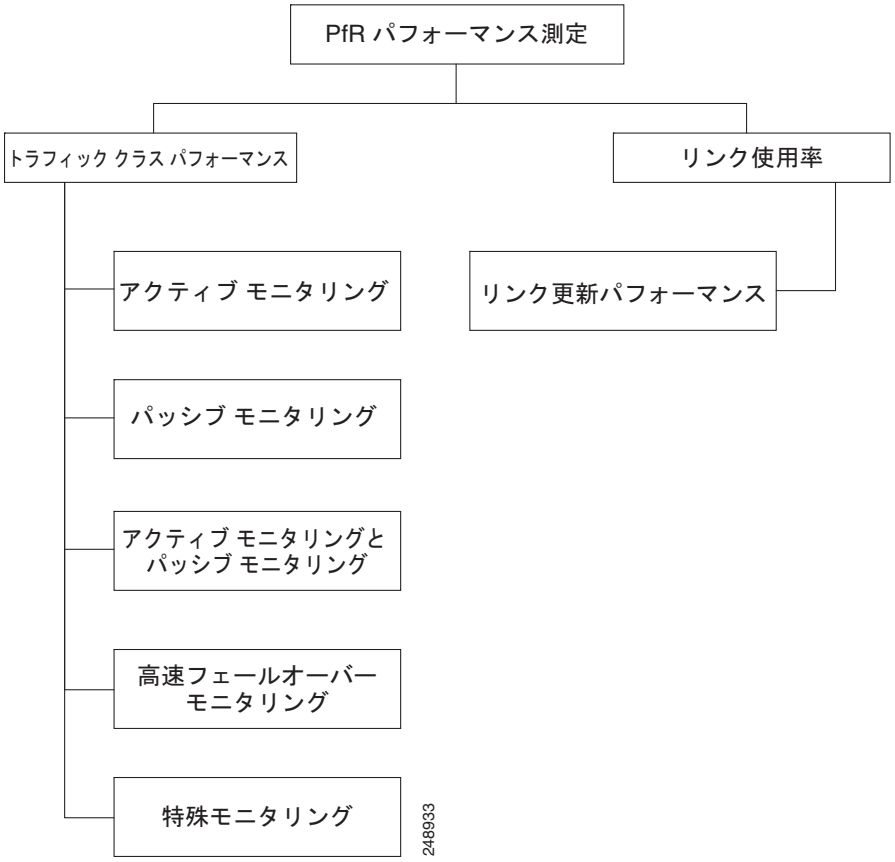
測定フェーズの概念

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。ボーダー 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構成要素を図 2 に示します。

図 2　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 Policy Decision Point（PDP; ポリシー デシジョン ポイント）を使用します。状態遷移図と各種トラフィック クラスの状態の説明については、「PfR ポリシー デシジョン ポイント」（P.18）を参照してください。

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」（P.9）
- 「リンク使用率測定手法」（P.15）

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 Service Level Agreement（SLA; サービス レベル契約）機能が使用されます。

- アクティブおよびパッシブ モニタリング：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て、ネットワークのトラフィック フローをより正確に把握します。

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を表 1 に示します。

表 1　　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	結合モード	高速フェールオーバー モード
導入されたリリース	12.3(14)T	12.3(14)T	12.3(14)T	12.4(15)T
アクティブ /IP SLA	あり	なし	あり	あり
パッシブ /NetFlow	なし	あり	あり	あり
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	あり	あり	あり	あり
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	あり	TCP トラフィック限定	TCP トラフィック限定	あり
ジッターのサポート	あり	なし	なし	あり
MOS のサポート	あり	なし	なし	あり

Cisco IOS Release 12.2(33)SXH では、Cisco Catalyst 6500 シリーズ スイッチを PfR ボーダー ルータとして使用するサポートが導入されました。Cisco IOS Release 12.2(33)SRB では、Cisco 7600 シリーズ ルータを PfR ボーダー ルータとして使用するサポートが導入されました。ボーダー ルータとして使用されている Cisco Catalyst 6500 スイッチまたは Cisco 7600 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 12.4(6)T 以降が稼動しているルータである必要があります。なぜなら Catalyst 6500 では、パッシブな統計情報を収集する制限付き機能をサポートするために、特殊モニタリング モードが導入されたからです。特殊モードはグローバルに設定されるため、Command-Line Interface（CLI; コマンド ライン インターフェイス）を使用して設定することはできません。詳細につ

いては、「特殊モニタリング」（P.15）を参照してください。

各モニタリング手法の詳細については、次の項を参照してください。

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、デフォルトによりボーダー 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。ボーダー 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。トラフィックがボーダー 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し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。

プレフィクスに加えて DSCP 値、ポート番号、プロトコルもボーダー 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 Out-of-Policy（OOP; ポリシー違反）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。良好および最良の出口の選択については、「出口選択モード」（P.24）を参照してください。

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：ジッターとは、パケット間遅延の分散です。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。
- Mean Opinion Score（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 4.0 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 コントローラはボーダー 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。ボーダー 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。

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 では、ネットワーク パフォーマンスの測定にアクティブ トラフィック モニタリングを使用します。つまり、継続的で信頼性が高く予測可能な方法でトラフィックを生成します。Cisco ルータで使用できる IP SLAs 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。

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 Intrusion Detection System（IDS; 侵入検知システム）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 リスト内で一致箇所が最も長いプレフィ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 プローブはボーダー 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）に、PfR が任意の IP Routing Information Base（RIB; ルーティング情報ベース）で親ルート（正確に一致するルートまたはあいまいなルート）を検索できる機能が追加されました。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、すべてのボーダー 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、ボーダー 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、Mean Opinion Score（MOS; 平均オピニオン評点）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、「PfR Voice Traffic Optimization Using Active Probes」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。

特殊モニタリング

PfR ボーダー ルータ専用機能に、マスター コントローラ機能をサポートしていないハードウェア プラットフォーム上で PfR を実行できる機能が追加されました。ただしこれらのプラットフォームは、機能が制限されたボーダー ルータとして動作することができます。ボーダー ルータとして使用されている Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 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 12.4(6)T 以降が稼動しているルータである必要があります。

特殊モニタリング モードの mode monitor special 構文が導入されました。マスター コントローラ機能をサポートしないハードウェア プラットフォームに対し、mode monitor both の代わりに使用できます。特殊モードはグローバルに設定されるため、Command-Line Interface（CLI; コマンド ライン インターフェイス）を使用して設定することはできません。マスター コントローラ機能をサポートしていないハードウェア プラットフォームでは、PfR は TCP フローのパッシブ モニタリングから遅延、損失、到達可能性などのパフォーマンス特性を確認できません。PfR が測定できるのは、パッシブ スループットのみとなります。スループットベースのロード バランシングは引き続きサポートされます。また、パッシブ モニタリングの制限事項に対応してアクティブ プローブがイネーブルにされ、アクティブ IP SLA 測定ができるようになっています。マスター コントローラでは、自動的に Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの制限付き機能が検出され、他のボーダー ルータがダウングレードされて、トラフィック クラスのスループット統計だけが取得されます。その他の統計を無視することによって、マスター コントローラのボーダー ルータ機能の表示が均一になります。

（注） **show oer master prefix** コマンドの出力では、mode monitor special のプレフィクスの隣に "#" が示されます。

リンク使用率測定手法

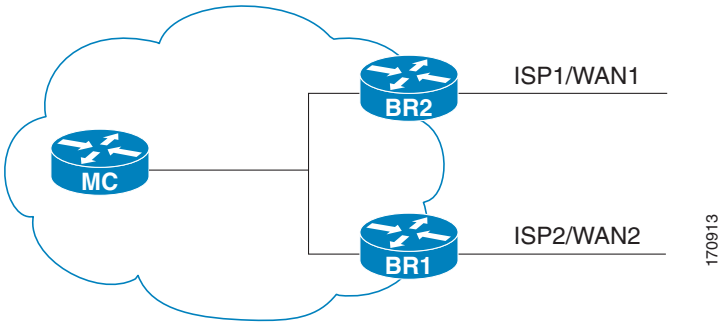
リンク使用率のしきい値

ボーダー 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（外部リンクはボーダー 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、ボーダー 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。図 3 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 つのボーダー ルータを示します。マスター コントローラは、いずれのボーダー ルータのリンク、つまり図 3 の BR1 または BR2 がトラフィック クラスによって使用されているかを判断します。

図 3　　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ボーダー 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 % に指定され、BR1（図 3）の出口リンクの使用率が 70 % のとき、BR2（図 3）の出口リンクの使用率が 40 % に低下すると、2 つの出口リンク間のパーセンテージ範囲は 25 % より大きくなるので、PfR は一部のトラフィック クラスを BR1 の出口リンクの使用にあて、トラフィックの負荷を均一にしようと試みます。BR1（図 3）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。

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。状態遷移の決定の詳細については、「PfR ポリシー デシジョン ポイント」（P.18）を参照してください。

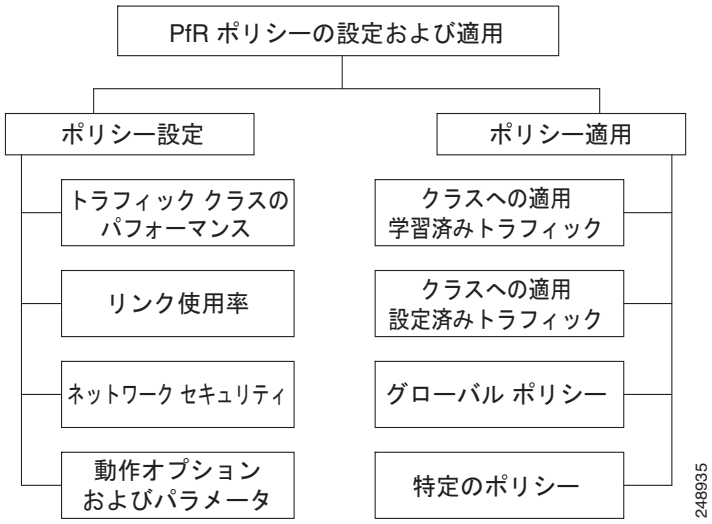
PfR ポリシーは、目的が明示されたルールであり、次の項目が含まれます。

- 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（図 4 を参照）、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 4　PfR ポリシー適用フェーズの構造



3 種類の PfR ポリシーと設定可能な動作オプションおよびパラメータを図 4 に示します。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。

- 「トラフィック クラス パフォーマンス ポリシー」（P.19）
- 「PfR リンク ポリシー」（P.21）
- 「PfR ネットワーク セキュリティ ポリシー」（P.22）
- 「PfR ポリシーの動作オプションおよびパラメータ」（P.22）

PfR ポリシーの設定後は、図 4 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。PfR ポリシーの適用の詳細については、「PfR ポリシーの適用」（P.24）を参照してください。

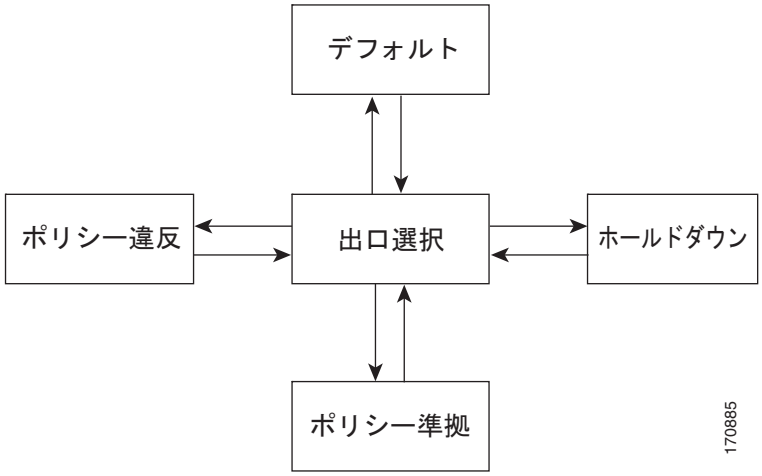
トラフィック クラスに複数のポリシー パラメータを設定する場合、複数のポリシーが重複する可能性があります。実行するポリシーの競合を回避するために、PfR は解決機能を使用します。これは、大半のポリシー タイプにプライオリティを設定できる柔軟なメカニズムです。PfR で複数のポリシーの競合を解決する方法については、「複数の PfR ポリシーに対するプライオリティ解決」（P.25）を参照してください。

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、図 5 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。図 5 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ボーダー 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 5　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、プレフィクスがポリシー準拠状態になるのは、そのプレフィ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。

- 「到達可能性」（P.19）
- 「遅延」（P.20）
- 「パケット損失」（P.20）
- 「ジッター」（P.20）
- 「平均オピニオン評点（MOS）」（P.20）

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 flows per million（fpm; 100 万フローあたりの到達不能数）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。ジッターとは、パケット間遅延の分散です。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 4.0 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 エッジにあるボーダー 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。ボーダー ルータに外部インターフェイスが設定されると、ボーダー 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 コントローラでボーダー 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 モードのボーダー 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。

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。詳細については、「Configuring Performance Routing Cost Policies」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。

PfR リンクのグループ化の詳細については、「Performance Routing Link Groups」のマニュア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」（P.22）
- 「PfR モード オプション」（P.23）

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」（P.23）
- 「ホールドダウン タイマー」（P.23）
- 「周期タイマー」（P.23）

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」（P.23）
- 「ルート モード」（P.23）
- 「出口選択モード」（P.24）

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。

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 トラフィック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-link 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-link 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-link 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-link 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-link 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 プレフィクス リストで permit 文または deny 文を設定し、そのプレフィクス 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。

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 コントローラはボーダー 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、ボーダー 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 タイマーと PfR モード オプションの詳細については、「PfR ポリシーの動作オプションおよびパラメータ」（P.22）を参照してください。

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。

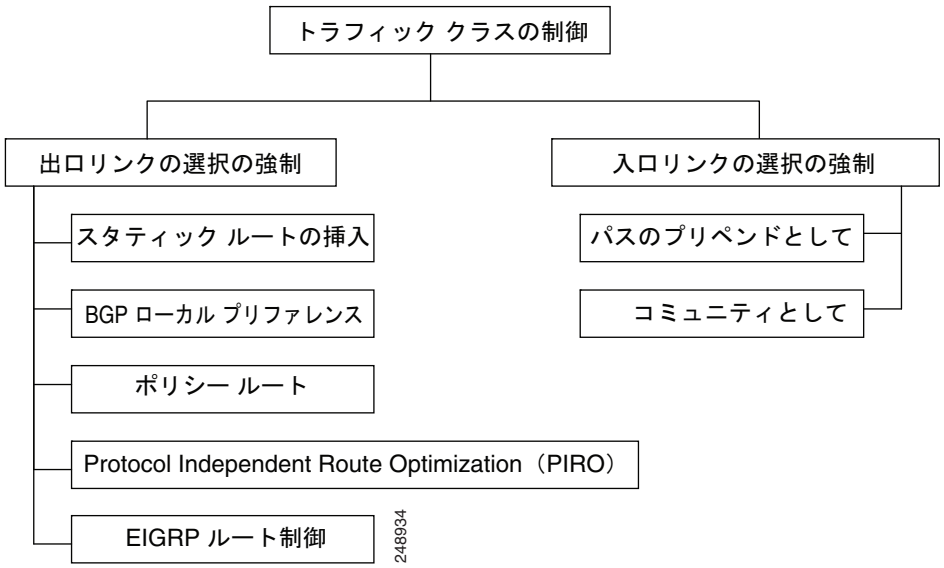
PfR 制御モードがイネーブルになり、設定オプションが検討されたら、次のステップでは PfR で実施されるトラフィック クラス制御の手法を検証します。

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クスは、そのプレフィクスのトラフィックをボーダー 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 ボーダー ルータはシングル ホップの位置にあるか、シングル ホップのように見えるトンネル インターフェイスである必要があります。

出口または入口リンクの選択で分類した各種のトラフィック クラス制御手法を図 6 に示します。

図 6　　トラフィック クラス制御手法



実施可能な各種トラフィック クラス制御手法の詳細については、次の項を参照してください。

- 「PfR 出口リンク選択制御手法」（P.27）
- 「PfR 入口リンク選択の制御テクニック」（P.30）

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負荷を分散する場合の解決法は、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」（P.28）
- 「BGP 制御手法」（P.29）
- 「EIGRP ルート制御」（P.29）
- 「ポリシーベースのルーティング制御」（P.29）
- 「Protocol Independent Route Optimization（PIRO）」（P.30）

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、特定のボーダー 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 コントローラがボーダー 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。ボーダー 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クスとして知られる方法も使用できます。

分割プレフィクスは、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、ボーダー 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 は分割プレフィクスを使用して、既存プレフィ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ボーダー 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。ボーダー 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ボーダー 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クスまたはプレフィクスのセットに Local_Pref 属性を適用するよう指示します。そのあとボーダー 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 5,000 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、「Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support」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 ボーダー 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ボーダー 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、ボーダー 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 の前に、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（正確に一致するルートまたはあいまいなルート）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、「Performance Routing - Protocol Independent Route Optimization (PIRO)」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、「BGP Inbound Optimization Using Performance Routing」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、指定されたボーダー ルータを送信元とするパス情報が含まれます。ボーダー 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。

次の作業

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、「Configuring Advanced Performance Routing」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」（P.31）を参照してください。

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco PfR コマンド（コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例）	『*Cisco IOS Performance Routing Command Reference*』
ベーシック PfR 設定	「Configuring Basic Performance Routing」モジュール
アドバンスド PfR の設定	「Configuring Advanced Performance Routing」モジュール
PfR 機能の位置	「Cisco IOS Performance Routing Features Roadmap」モジュール

シスコのテクニカル サポート

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

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

表 2 に、このモジュールの機能の一覧と、特定の概念情報へのリンクを示します。

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

（注） 表 2 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 2　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
ポートおよびプロトコル ベースのプレフィクス学習	12.3(11)T 12.2(33)SRB	ポートおよびプロトコル ベースのプレフィクス学習では、プロトコル タイプと TCP または UDP ポート番号に基づいてプレフィクス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。 この機能に関する詳細については、次の各項を参照してください。 • 「PfR を使用したプレフィクス トラフィック クラスの学習」（P.4） • 「PfR を使用したプレフィクス トラフィック クラスの設定」（P.6） **protocol**（PfR）コマンドが、この機能によって導入されました。
expire コマンド[1]	12.3(14)T 12.2(33)SRB	**expire after**（PfR）コマンドは、学習済みプレフィ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	12.4(2)T 12.2(33)SRB	OER アクティブ プローブ ソース アドレス機能では、ボーダー 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。 この機能に関する詳細については、次の各項を参照してください。 • 「アクティブ モニタリング」（P.12） **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。

表 2　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（続き）

機能名	リリース	機能の設定情報
OER アプリケーション アウェア ルーティング：PBR	12.4(2)T 12.2(33)SRB	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。 この機能に関する詳細については、次の各項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」（P.7） 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**。
OER DSCP モニタリング	12.4(9)T 12.2(33)SRB	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。レイヤ 3 プレフィクス情報に加えて、プロトコル、ポート番号、および DSCP 情報などのレイヤ 4 情報もマスター 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。 この機能に関する詳細については、次の各項を参照してください。 • 「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」（P.4） • 「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」（P.7） 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 aggregation**（PfR）、**traffic-class filter**（PfR）、および **traffic-class keys**（PfR）。

表 2　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（続き）

機能名	リリース	機能の設定情報
OER ボーダー ルータ専用機能	12.2(33)SXH 12.2(33)SRB	Cisco IOS Release 12.2(33)SXH および Cisco IOS Release 12.2(33)SRB でボーダー ルータ専用機能が導入されました。ハードウェアの制約のため、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータにはボーダー ルータ専用機能を使用でき、マスター コントローラ設定は使用できません。ボーダー ルータとして使用される Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 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 12.4(6)T 以降が稼動しているルータである必要があります。PfR マスター コントローラ ソフトウェアは制限付き機能を処理するように変更されました。ハードウェアの制約のないルータおよびスイッチでは遅延、損失、到達不能、およびスループットの統計が収集されますが、ボーダー ルータではトラフィック クラスのスループット統計だけを取得できます。マスター コントローラでは、自動的に制限付き機能が検出され、他のボーダー ルータがダウングレードされて、トラフィック クラスのスループット統計だけが取得されます。その他の統計を無視することによって、マスター コントローラのボーダー ルータ機能の表示が均一になります。 この機能に関する詳細については、次の各項を参照してください。 • 「トラフィック クラス パフォーマンス測定手法」（P.9） • 「特殊モニタリング」（P.15） 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**。
ポリシー ルール設定に対する OER のサポート	12.3(11)T 12.2(33)SRB	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。 この機能に関する詳細については、次の各項を参照してください。 • 「PfR ポリシーを適用するポリシー ルールの設定」（P.25） 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）。

表 2　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（続き）

機能名	リリース	機能の設定情報
高速フェールオーバー モニタリングのサポート[2]	12.4(15)T	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。 この機能に関する詳細については、次の項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」（P.14） 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、マイナーな機能拡張です。マイナーな機能拡張は、通常、Feature Navigator には表示されません。
2. これは、マイナーな機能拡張です。マイナーな機能拡張は、通常、Feature Navigator には表示されません。