基本的なパフォーマンス ルーティングの設定

Performance Routing（PfR; パフォーマンス ルーティング）は標準的なルーティング テクノロジーの機能を高めるテクノロジーであり、アプリケーション トラフィック用に最適な出力パスまたは入力パスを判断するため、ワイド エリア ネットワーク（WAN）インフラストラクチャ上の 2 つのデバイス間のパスのパフォーマンスの追跡または品質の確認を行います。

シスコ パフォーマンス ルーティングは、アプリケーションのパフォーマンス要件を満たす最適パスを選択する機能を付加することで、標準的な 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 テクノロジーの最初のフェーズでは、企業内 WAN 上およびインターネットを介するアプリケーション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。このテクノロジーを使用すると、エンドツーエンドのパフォーマンス重視のネットワークによって、企業ネットワーク全体におけるアプリケーション パフォーマンスの最適化の実現に役立ちます。

このマニュアルでは、Cisco ASR 1000 シリーズの集約サービス ルータ上で Cisco IOS XE ソフトウェアを使用し、パフォーマンス ルーティングを実装するために必要な基本概念と作業の概要について説明します。

（注） Cisco IOS XE Release 2.6.1 では、境界ルータ専用機能がサポートされます。

機能情報の確認

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「基本的なパフォーマンス ルーティングの機能情報」（P.21）を参照してください。

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

この章の構成

制約事項

Cisco IOS XE Release 2.6.1 では、Cisco ASR 1000 シリーズ集約サービス ルータの PfR 境界ルータとしての使用のサポートが導入されました。境界ルータ専用機能は Cisco IOS XE Release 2.6.1 イメージに含まれており、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。

パフォーマンス ルーティングについて

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

Performance Routing（PfR; パフォーマンス ルーティング）は、最適な出力パスまたは入力パスを選択するための追加のサービサビリティ パラメータよって、ビジネスにおける標準的なルーティング テクノロジーを補完するシスコの先進テクノロジーです。標準的なルーティング テクノロジーは、この追加機能によって強化されます。PfR では到達可能性、遅延、コスト、ジッタ、MOS スコアなどのパラメータに基づいて入出力 WAN インターフェイスを選択する、または負荷、スループット、および金銭的な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ができます。EIGRP、OSPF、RIPv2、BGP などの標準的なルーティングでは、一般に最短または最低のコスト パスに基づいてループがないトポロジーを作成することに重点を置いています。

PfR では、測定値の計測による追加機能が実現します。インターフェイスの統計情報、アクティブ モニタリング用の Cisco IP SLA、およびパッシブ モニタリング用の NetFlow が使用されます。PfR には IP SLA または NetFlow に関する知識や経験は必要なく、手動で設定せずにこれらの機能が自動的にイネーブルになります。

シスコ パフォーマンス ルーティングでは、到達可能性、遅延、コスト、ジッタ、Mean Opinion Score（MOS; 平均オピニオン評点）などのアプリケーション パフォーマンスに影響を及ぼすパラメータに基づいて、WAN の出力パスまたは入力パスが選択されます。このテクノロジーによってロード バランシングの効率性が高まり、WAN をアップグレードせずにアプリケーション パフォーマンスが向上するため、ネットワーク コストを削減できます。

PfR は統合された Cisco IOS ソリューションであり、これによって IP トラフィック フローを監視でき、トラフィック クラス パフォーマンス、リンク負荷分散、リンク帯域幅の金銭的なコスト、およびトラフィックの種類に基づいてポリシーとルールを定義できます。PfR にはアクティブおよびパッシブのモニタリング システム、ダイナミック障害検出、および自動パス修正機能が用意されています。PfR を導入することで、高性能な負荷分散と最適なルート選択が企業ネットワークで実現します。

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

シスコ 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膨大な機能を活用し、ネットワークおよびアプリケーションのポリシーに基づく最適なパスを決定します。シスコ パフォーマンス ルーティングは Cisco IOS Optimized Edge Routing（OER）を大幅に拡張したテクノロジーです。OER は元来送信先プレフィクス単位でのルート コントロールを提供するために設計されたものでしたが、パフォーマンス ルーティングはアプリケーション単位でインテリジェントなルート コントロールを行うように機能が拡張されています。この拡張機能によって、OER よりも柔軟性が増し、アプリケーションの最適化の精度が高まります。

パフォーマンス ルーティング対標準的なルーティング テクノロジー

PfR は、従来の IP ルーティング テクノロジーが対処できないネットワーク パフォーマンスの問題を特定して制御するように開発されました。従来の IP ルーティングでは、各ピア デバイスは、メトリックに達するためのコスト関連のなんらかの概念により、到達可能性のビューをプレフィクス送信先に対して伝達します。プレフィクス送信先への最適なパスは、通常最低コスト メトリックを使用して決定され、そのデバイスの Routing Information Base（RIB）にこのルートが組み込まれます。その結果、RIB に組み込まれた任意のルートは、そのプレフィクス送信先に宛てたトラフィックを制御するための最適パスとして扱われます。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して設定されます。たとえば、コスト メトリックはパスに対するユーザ プリファレンス、または高帯域幅インターフェイス（インターフェイスの種類から推論される）に対するプリファレンスのいずれかを反映したものになります。このコスト メトリックには、ネットワークの状態またはその時点でそのネットワーク上を伝送されるトラフィックのパフォーマンスの状態は考慮されていません。そのため、従来の IP ルーティングによるネットワークは、ネットワークでの物理的な状態の変化（インターフェイスがダウンしかかっているなど）には適応しますが、ネットワーク内でのパフォーマンスの変化（低下または向上）には適応しません。場合によっては、トラフィックの低下はルーティング デバイスのパフォーマンスの低下、またはセッション接続が失われたことが原因である可能性がありますが、こうしたトラフィックの低下現象はトラフィック パフォーマンスを測る直接的な基準でなく、最適なパスによるルーティングに関する決定材料として使用できません。

ネットワーク内のトラフィックに関するパフォーマンスの問題に対処するため、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、あるサブセットが、アプリケーションと関連付けられたトラフィックを表す場合があります。各トラフィック クラスのパフォーマンスは計測され、PfR ポリシーに定義された設定、またはデフォルトのメトリックと比較されます。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 クラスに対する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 パフォーマンスがそのポリシーに適合しない場合、PfR はトラフィック クラスに対して別の入口または出口を選択します。

パフォーマンス ルーティングの基本導入

PfR は Cisco IOS Command-line Interface（CLI; コマンドライン インターフェイス）設定を使用して Cisco ルータ上に設定します。パフォーマンス ルーティングは Master Controller（MC; マスター コントローラ）および Border Router（BR; 境界ルータ）の 2 つのコンポーネントから構成されます。PfR の導入には、1 つの MC と 1 つ以上の BR が必要です。MC と BR との間の通信は、キー チェーン認証によって保護されます。

PfR 管理対象ネットワークには、発信トラフィックを運ぶことができて外部インターフェイスとして設定できる出力インターフェイスが 2 つ以上ある必要があります。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、ルータにもパッシブ モニタリングのための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）がある必要があります。PfR の導入には、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 またはその他の参加ネットワークに対する 1 つ以上の出口リンクが備わっているエッジ ルータのデータ プレーン内にあります。BR はスループットおよび TCP パフォーマンス情報をパッシブに収集するために NetFlow を使用します。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 Service-Level Agreement（SLA; サービス レベル契約）プローブを参照します。ネットワーク内でのすべてのポリシー決定およびルーティングの変更は、BR で強制されます。BR は、マスター コントローラへのプレフィクスおよび出口リンクの測定のレポートを作成し、その後のマスター コントローラからのマスターポリシーの変更を強制することで、プレフィクス モニタリングおよびルートの最適化に関与します。BR は優先されるルートをネットワークの変更ルーティングに注入することで、ポリシーの変更を強制します。BR の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上でイネーブルにできます。

Cisco IOS XE Release 2.6.1 の境界ルータ専用機能については、『Performance Routing Border Router Only Functionality』モジュールを参照してください。

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 システムの中央のプロセッサ兼データベースとして機能する単一のルータです。MC コンポーネントはフォワーディング プレーン内になく、スタンドアロンの方法で導入される場合、BR 内に格納されるルーティング情報のビューはありません。マスター コントローラは BR とのセッションでの通信と認証を管理します。MC のロールは、トラフィック クラスがポリシーの範囲に適合しているかどうかを判断し、ルート注入またはダイナミック PBR 注入を使用してトラフィック クラスがポリシーの範囲内であることを保障する方法を BR に指示するための情報を BR または複数の BR から収集することです。

Cisco IOS XE Release 2.6.1 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 15.0(1)M イメージを実行している必要があります。

PfR コンポーネントのバージョン

MC と BR との間の API を変更する新しい PfR 機能が導入される際、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上がります。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の番号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どちらの番号も **show oer master** コマンドを使用して表示します。次の部分的な出力には、最初の節に MC バージョン、境界ルータに関する情報の最後の列に BR のバージョンが表示されています。

```
Router# show oer 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、一連のリリースの各 Cisco IOS ソフトウェア リリースごとに更新されませんが、Cisco IOS ソフトウェア イメージがマスター コントローラおよびすべての境界ルータとして設定されたデバイス上の同じリリースである場合、そのバージョンは互換性のあるバージョンになります。

（注） Cisco IOS XE Release 2.6.1 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、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。

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との間の通信は、キー チェーン認証によって保護されます。認証キーは、通信が確立できる前に、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。Cisco IOS ソフトウェアでのキー管理の詳細については、『*Cisco IOS IP Routing: Protocol Independent Configuration Guide*』の「Configuring IP Routing Protocol-Independent Features」の章の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 管理対象ネットワークには、発信トラフィックを運ぶことができ、外部インターフェイスとして設定できる出力インターフェイスが 2 つ以上ある必要があります。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、ルータにもパッシブ モニタリングのための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）がある必要があります。PfR を導入するには、次の 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*：トラフィックを転送するための PfR 管理対象出口リンクとして設定します。物理的な外部インターフェイスは、境界ルータ上でイネーブルに設定します。外部インターフェイスは、マスター コントローラ上で PfR 外部インターフェイスとして設定します。マスター コントローラは、これらのインターフェイス上のプレフィクスおよび出口リンク パフォーマンスをアクティブに監視します。各境界ルータに 1 つ以上の外部インターフェイスと、PfR 管理対象ネットワーク内に最低 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*：NetFlow とのパッシブ パフォーマンス モニタリングのためだけに使用されます。明示的な NetFlow 設定は必要ありません。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。この内部インターフェイスは、マスター コントローラ上の PfR 内部インターフェイスとして設定します。各境界ルータ上に 1 つ以上の内部インターフェイスが設定されている必要があります。
- *ローカル インターフェイス*：マスター コントローラおよび境界ルータの通信のためだけに使用されます。単一のインターフェイスを各境界ルータ上のローカル 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。

次の種類のインターフェイス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定義できます。

- 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
- トンネル（Cisco IOS XE Release 2.6.1 の NAT ではサポートされていない）
- VLAN（QinQ はサポートされていない）

次の種類の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
- トンネル（Cisco IOS XE Release 2.6.1 の NAT ではサポートされていない）
- VLAN（QinQ はサポートされていない）

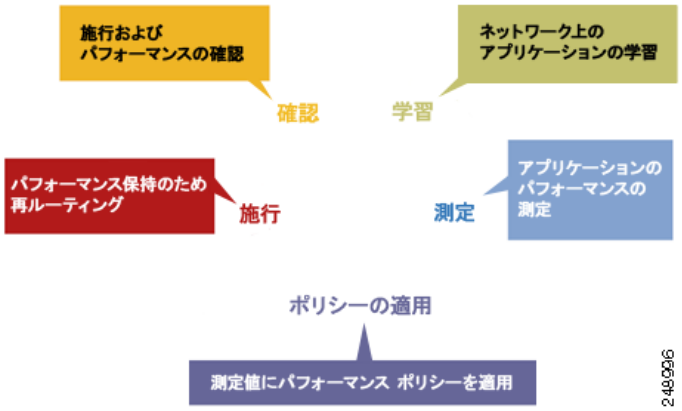
パフォーマンス ルーティング DMVPN mGre のサポート

- PfR はスプリット トンネリングをサポートしていません。
- PfR はハブからスポークへのリンクだけをサポートしています。スポーク間のリンクはサポートされません。
- PfR は DMVPN Multipoint GRE（mGRE; マルチポイント GRE）導入でサポートされます。同じ宛先 IP アドレスに対する複数のネクスト ホップがある任意のマルチポイント インターフェイスの導入はサポートされません（たとえばイーサネット）。

PfR ネットワーク パフォーマンス ループ

従来のすべてのルーティング プロトコルでは、ルーティング トポロジの作成のために、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 が使用するこのルーティング 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重視のデバイスとの間で実装されます。このパフォーマンス ルーティング プロトコルは、ネットワークが最適化すべきトラフィック クラスをプロファイリングするネットワーク パフォーマンス ループを作成し、特定されたトラフィック クラスのパフォーマンス メトリックを測定および監視し、ポリシーをそのトラフィック クラスに適用し、特定されたトラフィック クラスを最適なパフォーマンス パスに基づいてルーティングします。図 1 に、プロファイル フェーズ、測定フェーズ、ポリシー適用フェーズ、強制フェーズ、および確認フェーズの各 PfR フェーズを示します。

図 1　PfR ネットワーク パフォーマンス ループ



PfR がネットワーク内でどのように動作するかを理解するには、次の 5 段階の PfR フェーズを理解および実装する必要があります。

- 「プロファイル フェーズ」（P.7）
- 「測定フェーズ」（P.7）
- 「ポリシー適用フェーズ」（P.8）
- 「強制フェーズ」（P.8）
- 「確認フェーズ」（P.9）

PfR パフォーマンス ループはプロファイル フェーズで始まり、測定フェーズ、ポリシー適用フェーズ、制御フェーズ、および確認フェーズへと続きます。確認フェーズの後、このフローはトラフィック クラスの更新のためプロファイル フェーズへと戻り、このプロセスを繰り返します。

プロファイル フェーズ

中規模から大規模ネットワークには、デバイスがトラフィックをルーティングしようとする RIB 内に数十万のルートがあります。パフォーマンス ルーティングは一部のトラフィックを他のトラフィックよりも優先する手段のため、RIB 内の合計ルートのサブセットは、パフォーマンス ルーティング用に最適化するために選択する必要があります。PfR は、自動ラーニングまたは手動設定のうち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。

- 自動ラーニング：デバイスは、デバイスを通過させるフローを学習し、遅延が最高またはスループットが最高の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）を行う必要があるトラフィックをプロファイリングします。
- 手動設定：ラーニングに加えて、またはラーニングの代わりに、パフォーマンス ルーティングを行うトラフィックのクラスを設定できます。

測定フェーズ

パフォーマンス ルーティングの対象とするトラフィック クラスのプロファイリング後、PfR は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 メトリックを測定するには、パッシブ モニタリングとアクティブ モニタリングの 2 つのメカニズムがあり、この作業を完了するため、これらのいずれか、または両方をネットワーク内に導入できます。モニタリングは定期的な間隔で測定を行う動作です。

パッシブ モニタリングは、フローがデータ パス内のデバイスを通過するときのトラフィック フローのパフォーマンス メトリックを測定する動作です。パッシブ モニタリングは NetFlow 機能を使用し、パッシブ モニタリングをなんらかのトラフィック クラスのパフォーマンス メトリックの測定に使用することはできず、ハードウェアまたはソフトウェアによるいくつかの制限事項があります。

アクティブ モニタリングは、IP Service Level Agreement（SLA; サービス レベル契約）を使用して監視するトラフィック クラスをエミュレートする合成トラフィックの生成で構成されます。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 モニタリングの結果は、合成トラフィックで表されるトラフィック クラスをルーティングするパフォーマンスに適用されます。

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 モードの両方をトラフィック クラスに適用できます。パッシブ モニタリング フェーズでは、PfR ポリシーに準拠しないトラフィック クラス パフォーマンスが検出されることがあり、その際に最適な代替パフォーマンス パスが使用可能であれば検索するために、アクティブ モニタリングをそのトラフィック クラスに適用できます。

NetFlow または IP SLA 設定のサポートは、自動的にイネーブルに設定されます。

ポリシー適用フェーズ

最適化するトラフィック クラスのパフォーマンス メトリックの収集後、PfR はポリシーとして設定された各メトリックに対する下限しきい値および上限しきい値の設定セットとその結果を比較します。メトリックとその結果のポリシーが範囲外の場合、Out-of-Policy（OOP）イベントです。結果は相対的基準（観察された平均値からのずれ）、またはしきい値を基準（値の範囲の下限または上限）として、あるいはその両方の組み合わせで比較されます。

PfR で定義できるポリシーには、トラフィック クラス ポリシーとリンク ポリシーの 2 種類があります。トラフィック クラス ポリシーはプレフィクスまたはアプリケーションに対して定義します。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します。どちらの種類の PfR ポリシーも、OOP イベントを識別するための条件を定義します。これらのポリシーはグローバル単位（すべてのトラフィック クラスに対してポリシー セットが適用される）、または対象を絞った単位（トラフィック クラスの選択、つまりフィルタ処理されたリストに対してポリシー セットが適用される）で適用します。

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を使用し、ポリシーの競合を解決する方法が作成されました。デフォルトの調停方法では、各パフォーマンス メトリック変数および各ポリシーに割り当てら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、すべてのポリシー、または選択されたポリシー セットに対するデフォルトの調停よりも優先するように設定できます。

強制フェーズ

パフォーマンス ループの PfR の強制フェーズ（制御フェーズとも呼ばれる）では、トラフィックはネットワークのパフォーマンスを高めるために制御されます。トラフィックの制御に使用されるテクニックは、トラフィックのクラスに応じて異なります。プレフィクスだけを使用して定義されたトラフィック クラスの場合、従来のルーティングに使用されるプレフィクスの到達可能性情報を操作できます。ルートとそれに対応するコスト メトリックを導入または削除することによってプレフィクスの到達可能性情報を知らせる、または削除するため、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）または RIP などのプロトコルが使用されます。

プレフィクスおよび追加のパケット一致基準が指定されているアプリケーションによって定義されたトラフィック クラスの場合、ルーティング プロトコルはプレフィクスだけの到達可能性を伝達するため、PfR は従来のルーティング プロトコルを使用できません。これらのアプリケーション トラフィック クラスに対し、PfR はデバイス固有、またはネットワーク固有の 2 種類の制御方法を使用します。

デバイス固有の制御方法は、Policy-based Routing（PBR; ポリシーベース ルーティング）とのインタラクションを使用することで実現します。

ネットワーク固有の制御方法は、次の 2 種類の方法で実現します。

- オーバーレイ パフォーマンス ネットワーク：オーバーレイ ネットワークは、ネットワーク エッジにある各デバイスが、ネットワーク エッジのその他すべてのデバイスの存在について認識できる場所で作成されます。このとき、要求されたエッジ デバイスに到達するため、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）、またはマルチポイントの Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）テクノロジーを使用できます。
- コンテキスト拡張プロトコル：既存のルーティング プロトコル（BGP、Open Shortest Path First（OSPF））、Enhanced Interior Gateway Routing Protocol（EIGRP）はプレフィクスに対応付けられたコンテキストに関する情報を通信するために拡張されています。トラフィック クラス フロー内の外部パケット一致基準によって、ルートの更新内のプレフィクスに対応付けるコンテキストが作成されます。

確認フェーズ

トラフィック クラスが OOP の場合、PfR の強制フェーズ中に、OOP であるトラフィック クラスに対するトラフィックのフローに影響を与える（最適化する）ため、PfR はコントロールを導入します。スタティック ルートおよび BGP ルートは、PfR がネットワークに導入するコントロールの例です。コントロールの導入後、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入口リンクを通過することを確認します。トラフィック クラスが OOP のままの場合、PfR は OOP トラフィック クラスに対して最適化するために導入したコントロールを破棄し、ネットワーク パフォーマンス ループを繰り返します。

PfR と企業ネットワーク

企業ネットワークでは、信頼性と負荷分散のためにネットワーク エッジで複数の Internet Service Provider（ISP; インターネット サービス プロバイダー）または WAN 接続を使用します。既存の信頼性メカニズムは、プレフィクスまたはプレフィクス セットの最適な出口リンクを選択するために境界ルータ上でのリンク ステートまたはルートの削除に依存します。複数の接続によって、企業ネットワークは重大な障害から保護されますが、ネットワークは、ネットワークの輻輳が原因で発生する電圧低下または軽度の障害からは保護されません。既存のメカニズムは、問題の最初の兆候時の重大な障害に対応できます。しかし、停電および電圧低下が検出されないことがあり、問題を解決するためにネットワーク オペレータが措置を講じる必要が生じることがしばしばあります。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。企業ネットワーク内で WAN ルート選択を最適化することによって、エンド ユーザのパフォーマンスは、ローカル ネットワーク内での LAN 速度の向上よりも大幅に向上します。

PfR の導入の説明に使用される例の多くに、エッジ デバイスの通信相手のネットワークとして ISP が示されますが、それ以外にも解決策があります。ネットワーク エッジは、ネットワーク内において、WAN 接続および ISP 接続だけでなく、同じ場所内のデータ センター ネットワークなどのネットワークの別の部分である任意の論理的分離として定義できます。元のネットワーク エッジ デバイスに接続されているネットワーク、またはネットワークの部分には、BGP を使用して通信する場合、個別のオートノマス システム番号がある必要があります。

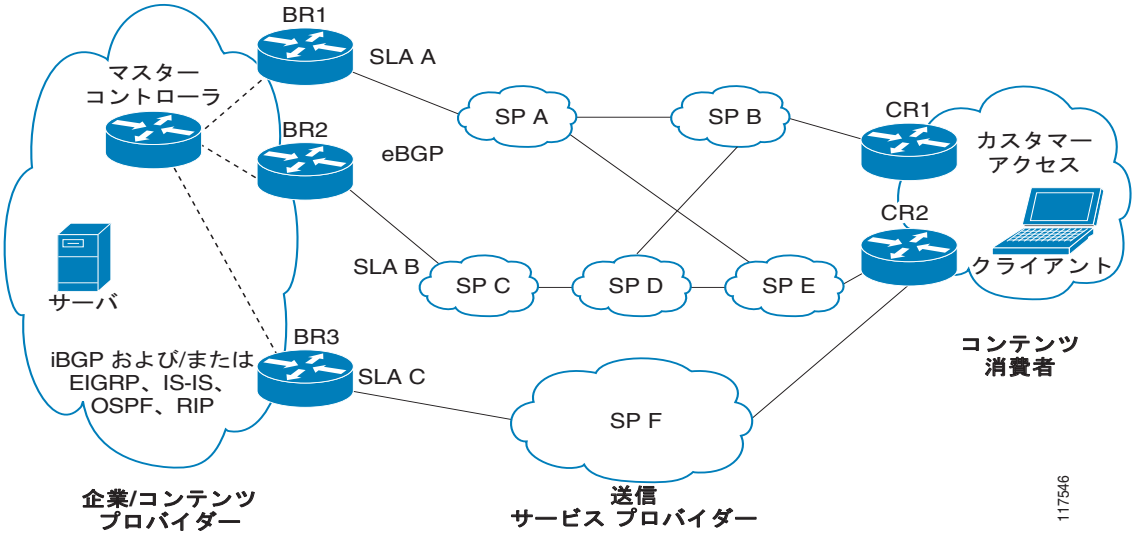
PfR は、シスコ コア ルーティング機能に内蔵された状態でシスコのソフトウェア内に実装されています。PfR を導入することで、ネットワーク エッジでのデータ パスに対するネットワーク トラフィック負荷の分散とダイナミック障害検出が可能になります。他のルーティング メカニズムで負荷分散と障害軽減の両方を提供できる場合がありますが、PfR だけが、応答時間、パケット損失、パスの可用性、

トラフィック負荷分散など、スタティック 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えます。PfR を導入することで、帯域幅コストを最小化して運用コストを抑えながら、ネットワーク パフォーマンスおよびリンク負荷使用率を最適化できます。

PfR を導入する一般的なトポロジ

図 2 に、コンテンツ プロバイダーの一般的な PfR 管理対象企業ネットワークを示します。企業ネットワークには、コンテンツをカスタマー アクセス ネットワークに提供するために使用される 3 つの出口インターフェイスがあります。コンテンツ プロバイダーには、各出口リンクについての異なる ISP との個別の Service Level Agreement（SLA; サービス レベル契約）があります。カスタマー アクセス ネットワークには、インターネットに接続する 2 つのエッジ ルータがあります。トラフィックは企業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 6 つの Service Provider（SP）ネットワーク上で伝送されます。

図 2　　一般的な PfR の導入



PfR は 3 つの Border Router（BR; 境界ルータ）上の発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 上の出力インターフェイスからのパケット応答時間およびパスの可用性を測定します。境界ルータ上の出口リンクのパフォーマンスの変化は、プレフィクス単位で検出されます。プレフィクスのパフォーマンスがデフォルトまたはユーザ定義のポリシー パラメータよりも低下した場合、パフォーマンスを最適化し、企業ネットワークの外部で発生した障害状態を回避するため、企業ネットワーク内でローカルにルーティングが変更されます。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 オペレータが介入せずにこの種類の問題を予想する、または解決することはできません。PfR では、障害状態を検出し、補正のためにネットワーク内部でルーティングを自動的に変更できます。

（注） Cisco IOS XE Release 2.6.1 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、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。

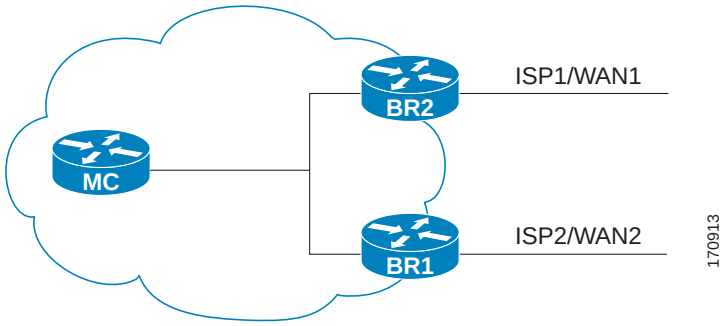
基本的なパフォーマンス ルーティングの設定方法

PfR マスター コントローラの設定

この作業は、PfR マスター コントローラを設定して PfR 管理対象ネットワークを管理するために実行します。この作業は、PfR マスター コントローラとして指定されたルータ上で実行する必要があります。マスター ルータおよび 2 つの境界ルータのネットワーク設定例については、図 3 を参照してください。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。内部および外部の境界ルータ インターフェイスも指定されます。

（注） Cisco IOS XE Release 2.6.1 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。

図 3　マスター コントローラおよび境界ルータの図



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

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 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。**shutdown** コマンドは、イネーブルにすると実行コンフィギュレーション ファイルに表示されます。

前提条件

PfR 管理対象ネットワークを設定する前に、マスター コントローラおよび境界ルータでインターフェイスが定義され到達可能である必要があります。

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 管理対象ネットワークの通信応答時間を最小限にするため、マスター コントローラを境界ルータと物理的に近い場所に配置することを推奨します。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、ホップ数を最小限にするため、それらの境界ルータも物理的に近い場所に配置する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. ステップ 6 を繰り返します。
8. 各境界ルータに対するキー チェーン認証を設定するため、適切な変更を加えてステップ 3 からステップ 7 を繰り返します。
9. **oer 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. 各境界ルータとの通信を確立するため、適切な変更を加えて ステップ 11 からステップ 15 を繰り返します。
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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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。通信を確立するには、キー ID とキー文字列が一致する必要があります。 • この例では、キー チェーンは境界ルータ 1 で使用するために作成されます。
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 は境界ルータ上に設定されたキー ID と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上に設定された認証文字列と一致する必要があります。 • 任意の暗号化レベルを設定できます。 • この例では、キー文字列は境界ルータ 1 で使用するために作成されます。
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、キー チェーン コンフィギュレーション モードに戻ります。
ステップ 7	ステップ 6 を繰り返します。	キー チェーン コンフィギュレーション モードを終了し、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	各境界ルータに対するキー チェーン認証を設定するため、適切な変更を加えてステップ 3 からステップ 7 を繰り返します。	—
ステップ 9	**oer master** **例：** `Router(config)# oer master`	OER マスター コントローラ コンフィギュレーション モードを開始し、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 プロセスは、同じルータ上でイネーブルにできます（たとえば、異なるサービス プロバイダーへの 2 つの出口リンクを持つ単一のルータがあるネットワーク）。
ステップ 10	**logging** **例：** `Router(config-oer-mc)# logging`	マスター コントローラまたは境界ルータ プロセスの Syslog メッセージをイネーブルにします。 • Syslog メッセージの通知レベルは、デフォルトでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 11	**border** *ip-address* [**key-chain** *key-chain-name*] **例：** `Router(config-oer-mc)# border 10.1.1.2 key-chain border1_PFR`	PfR 管理対象境界ルータ コンフィギュレーション モードを開始し、境界ルータとの通信を確立します。 • IP アドレスは境界ルータを特定するために設定されます。 • PfR 管理対象ネットワークを作成するには、1 つ以上の境界ルータを指定する必要があります。単一のマスター コントローラにより最大 10 台の境界ルータを制御できます。 • *key-chain-name* 引数の値は、ステップ 3 で設定したキー チェーン名と一致している必要があります。 （注） **key-chain** キーワードと *key-chain-name* 引数は、境界ルータを最初に設定するときに入力する必要があります。しかし、このキーワードは、既存の境界ルータを再設定する際には省略できます。
ステップ 12	**interface** *type number* **external** **例：** `Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external`	境界ルータ インターフェイスを PfR 管理対象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とアクティブ モニタリングのために使用されます。 • 最低 2 つの外部境界ルータ インターフェイスが PfR 管理対象ネットワーク内に必要です。各境界ルータ上に 1 つ以上の外部インターフェイスが設定されている必要があります。単一のマスター コントローラにより、最大 20 個の外部インターフェイスを制御できます。 ヒント インターフェイスをルータ上の PfR 管理対象外部インターフェイスとして設定することで、OER 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。このモードでは、最大リンク使用率またはコスト ベースの最適化をインターフェイスに対して設定できます。 （注） **interface** コマンドを **external** または **internal** キーワードを指定しないで入力することで、ルータがグローバル コンフィギュレーション モードになり、OER ボーダー出口コンフィギュレーション モードになりません。このコマンドの **no** 形式は、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、注意して適用する必要があります。
ステップ 13	**exit** **例：** `Router(config-oer-mc-br-if)# exit`	OER 管理対象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 管理対象境界ルータ 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-oer-mc-br)# interface GigabitEthernet 1/0/0 internal`	境界ルータ インターフェイスを PfR 制御された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 モニタリング目的でのみ使用されます。内部インターフェイスはトラフィックを転送しません。 • 各境界ルータ上に 1 つ以上の内部インターフェイスが設定されている必要があります。

	コマンドまたはアクション	目的
ステップ 15	**exit** **例：** `Router(config-oer-mc-br)# exit`	OER 管理対象境界ルータ コンフィギュレーション モードを終了し、OER マスター コントローラ コンフィギュレーション モードに戻ります。
ステップ 16	各境界ルータとの通信を確立するため、適切な変更を加えて ステップ 11 からステップ 15 を繰り返します。	—
ステップ 17	**keepalive** *timer* **例：** `Router(config-oer-mc)# keepalive 10`	（任意）キープアライブ パケットを受信しなかったあとに、PfR マスター コントローラが PfR 境界ルータとの接続性を維持する時間の長さを設定します。 • この例では、キープアライブ タイマーは 10 秒に設定されています。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-oer-mc-learn)# end`	OER トップ報告者およびトップ遅延ラーニング 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）実行コンフィギュレーションを表示し、この作業で開始したコンフィギュレーションを確認します。

PfR 境界ルータの設定

この作業は、PfR 境界ルータを設定するために実行します。この作業は、PfR 管理対象ネットワーク内の各境界ルータで実行する必要があります。マスター ルータおよび 2 つの境界ルータのネットワーク設定例については、図 3 を参照してください。まず境界ルータとマスター コントローラとの間で、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。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の送信元として設定し、外部インターフェイスは PfR 管理対象出口リンクとして設定します。

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

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 OER 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。**shutdown** コマンドは、イネーブルにすると実行コンフィギュレーション ファイルに表示されます。

前提条件

- 「PfR マスター コントローラの設定」（P.11）の作業は、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するために実行します。
- 各境界ルータに、ISP との接続に使用する、または外部 WAN リンクとして使用する 1 つ以上の外部インターフェイスがある必要があります。最低 2 つの外部インターフェイスが PfR 管理対象ネットワーク内に必要です。

- 各境界ルータに 1 つ以上の内部インターフェイスがある必要があります。内部インターフェイスは NetFlow とのパッシブ パフォーマンス モニタリングのためだけに使用されます。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は使用されません。
- 各境界ルータに 1 つ以上のローカル インターフェイスがある必要があります。ローカル インターフェイスはマスター コントローラおよび境界ルータの通信のためだけに使用されます。単一のインターフェイスを各境界ルータ上のローカル 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 2.6.1 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 SR 1000 シリーズ ルータ上でイネーブルにできません。

ヒント ホップ数を最小限にするため、境界ルータを互いに物理的に近い場所に配置することを推奨します。PfR 管理対象ネットワークの通信応答時間を最小限にするため、マスター コントローラも境界ルータと物理的に近い場所に配置する必要があります。

制約事項

- 境界ルータが同じ同報通信メディア上でいくつかのサービス 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。
- 2 つ以上の境界ルータが PfR 管理対象ネットワークに導入されている場合、RIB 内に組み込まれた各境界ルータ上の外部ネットワークに対するネクスト ホップは、同じサブネットからの IP アドレスにできません。

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. **oer 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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* **例：** `Router(config)# key chain 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両方の間の通信セッションを保護します。通信を確立するには、キー ID とキー文字列が一致する必要があります。
ステップ 4	**key** *key-id* **例：** `Router(config-keychain)# key 1`	キー チェーン上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 コントローラ上に設定されたキー ID と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 コントローラ上に設定された認証文字列と一致する必要があります。 • 任意の暗号化レベルを設定できます。
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、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、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	**oer border** **例：** `Router(config)# oer border`	OER 境界ルータ コンフィギュレーション モードを開始し、ルータを境界ルータとして設定します。 • 境界ルータはフォワーディング パス内にある必要があり、1 つ以上の外部インターフェイスおよび内部インターフェイスを備えている必要があります。
ステップ 9	**local** *type number* **例：** `Router(config-oer-br)# local GigabitEthernet 0/0/0`	PfR マスター コントローラとの通信の発信元である PfR 境界ルータ上のローカル インターフェイスを特定します。 • ローカル インターフェイスが定義されている必要があります。

	コマンドまたはアクション	目的
ステップ 10	**master** *ip-address* **key-chain** *key-chain-name* **例：** `Router(config-oer-br)# master 10.1.1.1 key-chain border1_PFR`	OER 管理対象境界ルータ コンフィギュレーション モードを開始し、マスター コントローラとの通信を確立します。 • IP アドレスはマスター コントローラを特定するために使用されます。 • *key-chain-name* 引数の値は、ステップ 3 で設定したキー チェーン名と一致している必要があります。
ステップ 11	**end** **例：** `Router(config-oer-br)# end`	OER トップ報告者およびトップ遅延ラーニング 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。

この次の手順

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。境界ルータ上に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 管理対象ネットワークは運用可能です。PfR の詳細設定について参照するには、「関連情報」（P.19）に進みます。

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。ルーティング プロトコル設定の詳細情報について参照するには、「関連情報」（P.19）に進みます。

基本的なパフォーマンス ルーティングの設定例

ここでは、次の例について説明します。

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 モードを開始し、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ために必要な最小限の設定を説明する設定例を示します。PFR というキー 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。

（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 2.6.1 イメージに含まれており、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。

```
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 境界ルータおよび 10.200.2.2 境界ルータと通信するように設定します。キープアライブ間隔を 10 秒に設定します。ルート モード コントロールをイネーブルに設定します。内部および外部の PfR 制御対象境界ルータ インターフェイスを定義します。

```
Router(config)# oer master
Router(config-oer-mc)# keepalive 10
Router(config-oer-mc)# logging
Router(config-oer-mc)# border 10.100.1.1 key-chain PFR
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-oer-mc-br)# exit
Router(config-oer-mc)# border 10.200.2.2 key-chain PFR
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external
Router(config-oer-mc-br)# interface GigabitEthernet 0/0/1 internal
Router(config-oer-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 モードを開始し、境界ルータをイネーブルにするために必要な最小限の設定を説明する設定例を示します。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 を適用します。マスター コントローラに対するインターフェイスが、PfR 通信のためのローカル インターフェイス（発信元）として識別されます。

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

関連情報

マスター コントローラおよび境界ルータの設定後、PfR の最適化機能全体をアクティブにするには、追加の設定が必要な場合があります。詳細については、『Understanding Performance Routing』モジュールおよび『Configuring Advanced Performance Routing』モジュール、または「関連資料」（P.20）のその他の参考資料を参照してください。

概念の詳細については、『Understanding Performance Routing』モジュールを、詳細や設定作業、例については、『Cisco IOS Performance Routing Features Roadmap』の一覧にある個別の機能を参照してください。

その他の参考資料

ここでは、基本的なパフォーマンス ルーティングの設定に関する参考資料について説明します。

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco OER コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS Optimized Edge Routing Command Reference*』
Cisco IOS XE リリースの境界ルータ専用機能に関する情報と設定	『Performance Routing Border Router Only Functionality』モジュール
高度な PfR 設定	『Configuring Advanced Performance Routing』モジュール
パフォーマンス ルーティングの運用フェーズを理解するために必要な概念	『Understanding Performance Routing』モジュール
Cisco IOS XE リリースの PfR 機能の場所	『Cisco IOS XE Performance Routing Features Roadmap』モジュール
IP SLA の概要	『*Cisco IOS IP SLAs Overview*』

シスコのテクニカル サポート

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

基本的なパフォーマンス ルーティングの機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

ここに記載されていないこのテクノロジーの機能情報については、『Cisco IOS XE Performance Routing Features Roadmap』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ソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

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

表 1　基本的なパフォーマンス ルーティングの機能情報

機能名	リリース	機能情報
Optimized Edge Routing	Cisco IOS XE Release 2.6.1	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。 **（注）** 境界ルータ専用機能は Cisco IOS XE Release 2.6.1 イメージに含まれており、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。