



## **Cisco IOS XE 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 Performance Routing Configuration Guide**

リリース 2

**【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/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

*Cisco IOS XE 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*

© 2010 Cisco Systems, Inc.

All rights reserved.

Copyright © 2010, シスコシステムズ合同会社.

All rights reserved.



# Cisco IOS XE パフォーマンス ルーティング 機能ロードマップ

この機能ロードマップは、『Cisco IOS XE 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』に記載された Cisco IOS XE の機能の一覧を挙げ、それらの説明があるドキュメントとの関連付けをまとめたものです。

調べる機能の機能名を検索し、「参照先」列の URL をクリックすると、その機能を記載したドキュメントにアクセスできます。



(注)

---

Performance Routing (PfR; パフォーマンス ルーティング) は Optimized Edge Routing (OER) を拡張したテクノロジーであり、コマンドおよびコマンドモードの多くに、現在も OER の命名規則が使用されています。元の OER の機能はすべてパフォーマンス ルーティング テクノロジーに組み込まれており、元の機能名でここに記載されています。

---

## 機能とリリース サポート

表 1 に、一連の Cisco IOS XE ソフトウェア リリースに対する Cisco IOS パフォーマンス ルーティング機能のサポートを示します。

- 「Cisco IOS XE Release 2」

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 に、最新の XE リリースと、そのリリース内の機能をアルファベット順に示します。



表 1 サポート対象の Cisco IOS XE パフォーマンス ルーティング機能

リリース	機能名	機能の説明	参照先
<b>Cisco IOS XE Release 2</b>			
XE 2.6.1	OER アクティブ プロープ送信元アドレス	この機能では、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 プロープの送信元として設定する機能が導入されました。	<ul style="list-style-type: none"> <li>『<a href="#">Understanding Performance Routing</a>』</li> <li>『<a href="#">Configuring Advanced Performance Routing</a>』</li> </ul>
	OER アプリケーション認識型ルーティング：PBR	これにより、監視対象のプレフィクスで伝送されるアプリケーションの種類に基づいて IP トラフィックを最適化する機能が導入されました。独立したポリシー設定がトラフィックのサブセット（アプリケーション）に適用されます。	<ul style="list-style-type: none"> <li>『<a href="#">Understanding Performance Routing</a>』</li> <li>『<a href="#">Configuring Advanced Performance Routing</a>』</li> </ul>
	スタティック アプリケーション マッピングを使用する OER アプリケーション認識型ルーティング	この機能では、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する機能が導入されます。Cisco IOS Release 12.4(9)T 以前のリリースでは、アプリケーション トラフィックの定義には、いくつかの使用しにくい設定が含まれていました。この機能では、PfR ポリシーを学習リスト内にプロファイリングされたトラフィック クラスに適用できる、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す。各学習リストに別々のポリシーを適用できます。新しい <b>traffic-class</b> コマンドと <b>match traffic-class</b> コマンドが、PfR が自動的に学習できる、または手動で設定できるトラフィック クラス設定を簡略化するために導入されます。	『 <a href="#">Static Application Mapping Using Performance Routing</a> 』
	OER BGP インバウンド最適化	この機能により、オートノマス システム内部のプレフィクスに宛てたオートノマス システム外部のプレフィクスを送信元とするトラフィックに対する最適な入口選択のサポートが導入されました。オートノマス システムから別のオートノマス システム（インターネット サービス プロバイダーなど）への External BGP (eBGP; 外部 BGP) アドバタイズメントは、ネットワークに入るトラフィックの入口パスに影響する場合があります。PfR は eBGP アドバタイズメントを使用し、最適な入口選択を操作します。  (注) Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズの集約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クスの最大数は 30 です。	『 <a href="#">BGP Inbound Optimization Using Performance Routing</a> 』

表 1 サポート対象の Cisco IOS XE パフォーマンス ルーティング機能 (続き)

リリース	機能名	機能の説明	参照先
XE 2.6.1	OER 境界ルータ専用機能	Performance Routing (PfR; パフォーマンス ルーティング) によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズの集約サービス ルータ上での Border Router (BR; 境界ルータ) 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。	『Performance Routing Border Router Only Functionality』
	OER DSCP モニタリング	この機能によって、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 値で構成されるキーと、要求されていないトラフィックを除外する機能、および対象とするトラフィックを集約する機能を組み合わせることで定義できます。プロトコル、ポート番号、および DSCP 情報などの情報は、プレフィ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。この新機能によって、PfR はアクティブおよびパッシブの両方でアプリケーショントラフィックを監視できます。	<ul style="list-style-type: none"> <li>『Understanding Performance Routing』</li> <li>『Configuring Advanced Performance Routing』</li> </ul>
	コスト ベースの最適化および traceroute レポート作成に対する OER サポート	この機能によって、ISP 請求コストに基づいて出口リンク ポリシーを設定する機能が導入されました。この機能では、traceroute プロンプトを設定してホップバイホップベースのプレフィクス特性を判断する機能も導入されます。	<ul style="list-style-type: none"> <li>『Configuring Performance Routing cost Policies』</li> <li>『Performance Routing Traceroute Reporting』</li> </ul>
	ポリシー ルール設定に対する OER サポート	この機能により、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 マップを選択して設定を適用する機能が導入され、定義済みの PfR マップ間で切り替えるための方式が向上します。	<ul style="list-style-type: none"> <li>『Understanding Performance Routing』</li> <li>『Configuring Advanced Performance Routing』</li> </ul>
	OER 音声トラフィックの最適化	この機能によって、音声メトリック、ジッタ、および Mean Opinion Score (MOS; 平均オピニオン評点) に基づく音声トラフィックの発信最適化のサポートが導入されました。ジッタおよび MOS は音声トラフィックのための重要な量的メトリックであり、これらの音声メトリックは、PfR アクティブ プロンプトを使用して測定されます。	『PfR Voice Traffic Optimization Using Active Probes』

表 1 サポート対象の Cisco IOS XE パフォーマンス ルーティング機能 (続き)

リリース	機能名	機能の説明	参照先
XE 2.6.1	Optimized Edge Routing (OER)	<p>PfR では、ネットワーク間の複数の接続に対する自動的なルート最適化と負荷分散が提供されます。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、プレフィクス 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。</p> <p>Cisco IOS XE Release 2.6.1 では、Cisco ASR 1000 シリーズの集約サービス ルータ上での Border Router (BR; 境界ルータ) 専用機能のサポートが導入されました。</p>	<ul style="list-style-type: none"> <li>『<a href="#">Configuring Basic Performance Routing</a>』</li> <li>『<a href="#">Understanding Performance Routing</a>』</li> <li>『<a href="#">Configuring Advanced Performance Routing</a>』</li> </ul>
	パフォーマンス ルーティング - アプリケーション インターフェイス	この機能では、PfR アプリケーション インターフェイスのサポートが導入されます。このアプリケーション インターフェイスでアプリケーション間の通信およびメッセージングのモードと、アプリケーションと関連付けられたトラフィックを最適化する目的でネットワークが定義されます。アプリケーションを PfR とのインターフェイスにする前に、プロバイダーを PfR マスター コントローラに登録する必要があります。また、アプリケーション インターフェイスを使用して PfR と通信するアプリケーションを実行するプロバイダー ネットワーク内のホスト デバイスも、IP アドレスとキー チェーン パスワードを使用して PfR マスター コントローラに設定する必要があります。	『 <a href="#">Performance Routing Application Interface</a> 』
	PfR EIGRP mGRE DMVPN ハブおよびスポークのサポート	PfR EIGRP mGRE DMVPN ハブおよびスポークのサポート機能によって、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 がルートを制御する機能が導入されました。また、ハブおよびスポーク ネットワーク設計に続く、Multicast Generic Routing Encapsulation (mGRE; マルチキャスト総称ルーティング カプセル化) Dynamic Multipoint Virtual Private Network (DMVPN; ダイナミック マルチポイント VPN) 導入のサポートも追加されました。	『 <a href="#">Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support</a> 』
	PfR - Protocol Independent Route Optimization (PIRO)	PIRO によって、PfR が任意の IP Routing Information Base (RIB) 内の親ルート (正確に一致するルート、またはそれよりも具体的でないルート) を検索する機能が導入され、それにより、OSPF および IS-IS などの Interior Gateway Protocol (IGP) を含む IP ルート環境に PfR を導入できます。	『 <a href="#">Performance Routing - Protocol Independent Route Optimization (PIRO)</a> 』

表 1 サポート対象の Cisco IOS XE パフォーマンス ルーティング機能 (続き)

リリース	機能名	機能の説明	参照先
XE 2.6.1	ポートおよびプロトコルベースのプレフィクス学習	この機能によって、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。	<ul style="list-style-type: none"> <li>『<a href="#">Understanding Performance Routing</a>』</li> <li>『<a href="#">Configuring Advanced Performance Routing</a>』</li> </ul>
	VPN IPsec/GRE トンネル最適化	この章では、IP Security (IPsec; IP セキュリティ) /Generic Routing Encapsulation (GRE; 総称ルーティングカプセル化) トンネルインターフェイスを PfR 管理対象出口リンクとして設定する方法を説明する PfR ソリューションを記載しています。ネットワークベースの IPsec VPN だけがサポートされます。	『 <a href="#">Configuring VPN IPsec/GRE Tunnel Interfaces As PfR-Managed Exit Links</a> 』

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLXNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2010 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社.  
All rights reserved.







## 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

- 「パフォーマンス ルーティングについて」 (P.2)
- 「関連情報」 (P.19)

- 「その他の参考資料」 (P.19)
- 「基本的なパフォーマンス ルーティングの機能情報」 (P.21)

## 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」 (P.2)
- 「パフォーマンス ルーティングと Optimized Edge Routing」 (P.3)
- 「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」 (P.3)
- 「パフォーマンス ルーティングの基本導入」 (P.3)
- 「PfR ネットワーク パフォーマンス ループ」 (P.6)
- 「PfR と企業ネットワーク」 (P.9)

## 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スビリティ パラメータによって、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。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)

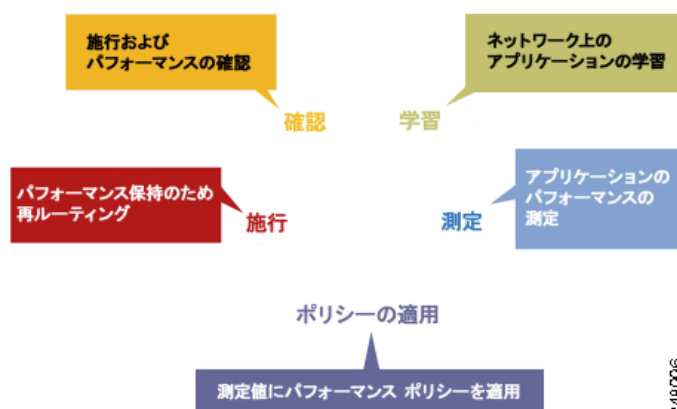
#### パフォーマンス ルーティング DMVPN mGre のサポート

- 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 packets 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。

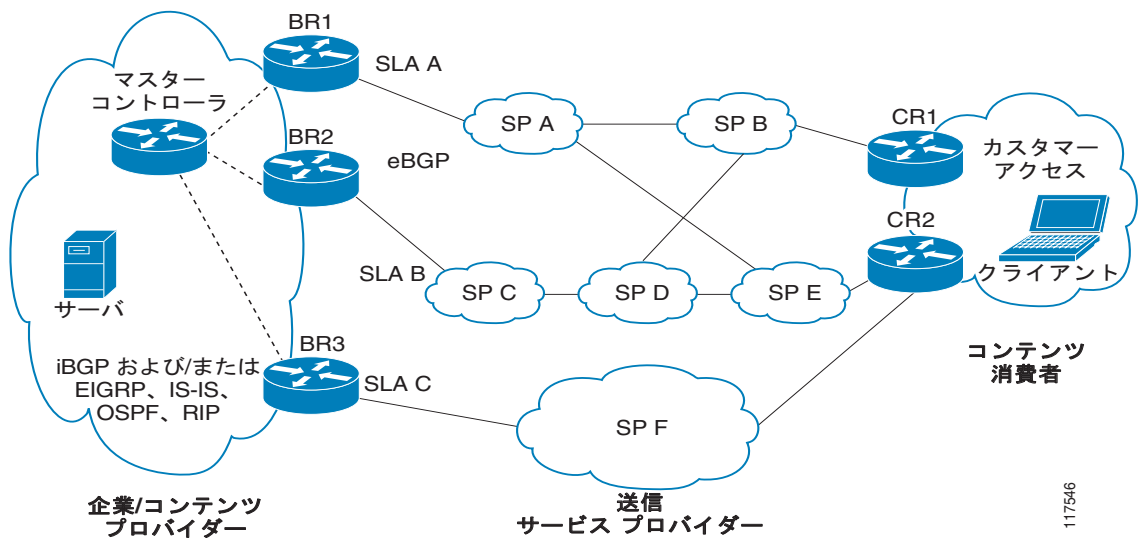
**PfR** は、シスコ コア ルーティング機能に内蔵された状態でシスコのソフトウェア内に実装されています。**PfR** を導入することで、ネットワーク エッジでのデータ パスに対するネットワーク トラフィック 負荷の分散とダイナミック障害検出が可能になります。他のルーティング メカニズムで負荷分散と障害軽減の両方を提供できる場合がありますが、**PfR** だけが、応答時間、パケット損失、パスの可用性、

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」(P.11)
- 「PfR 境界ルータの設定」(P.15)

## PfR マスター コントローラの設定

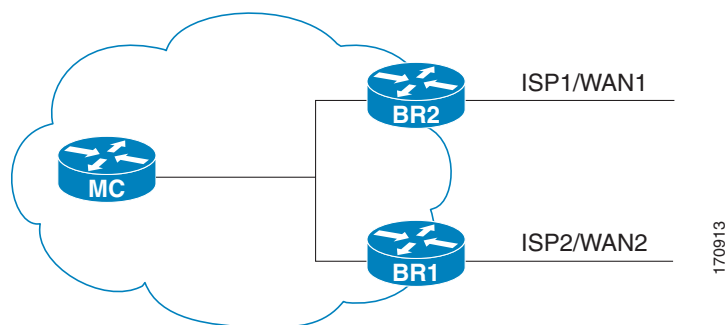
この作業は、PfR マスター コントローラを設定して PfR 管理対象ネットワークを管理するために実行します。この作業は、PfR マスター コントローラとして指定されたルータ上で実行する必要があります。マスター ルータおよび 2 つの境界ルータのネットワーク設定例については、図 3 を参照してください。まずマスター コントローラと境界ルータとの間で、マスター コントローラと境界ルータとの間の通信セッションを保護するために設定されるキー チェーン認証を使用し、通信が確立されます。内部および外部の境界ルータ インターフェイスも指定されます。



(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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>• 必要に応じてパスワードを入力します。</li> </ul>
ステップ 2	<b>configure terminal</b>  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
<p><b>ステップ 3</b> <code>key chain name-of-chain</code></p> <p><b>例 :</b> Router(config)# key chain border1_PFR</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
<p><b>ステップ 4</b> <code>key key-id</code></p> <p><b>例 :</b> Router(config-keychain)# key 1</p>	<p>キー チェーンの認証キーを識別します。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
<p><b>ステップ 5</b> <code>key-string text</code></p> <p><b>例 :</b> Router(config-keychain-key)# key-string bl</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 任意の暗号化レベルを設定できます。</li> <li>• 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。</li> </ul>
<p><b>ステップ 6</b> <code>exit</code></p> <p><b>例 :</b> Router(config-keychain-key)# exit</p>	<p>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。</p>
<p><b>ステップ 7</b> <a href="#">ステップ 6</a> を繰り返します。</p>	<p>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。</p>
<p><b>ステップ 8</b> 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<a href="#">ステップ 3</a> から<a href="#">ステップ 7</a> を繰り返します。</p>	<p>—</p>
<p><b>ステップ 9</b> <code>oer master</code></p> <p><b>例 :</b> Router(config)# oer master</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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)。</li> </ul>
<p><b>ステップ 10</b> <code>logging</code></p> <p><b>例 :</b> Router(config-oer-mc)# logging</p>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>

コマンドまたはアクション	目的
<p><b>ステップ 11</b> <code>border ip-address [key-chain key-chain-name]</code></p> <p><b>例：</b>  <pre>Router(config-oer-mc)# border 10.1.1.2 key-chain border1_PFR</pre></p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li><code>key-chain-name</code> 引数の値は、<a href="#">ステップ 3</a> 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。</li> </ul> <p><b>(注)</b> <code>key-chain</code> キーワードと <code>key-chain-name</code> 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。</p>
<p><b>ステップ 12</b> <code>interface type number external</code></p> <p><b>例：</b>  <pre>Router(config-oer-mc-br)# interface GigabitEthernet 0/0/0 external</pre></p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p><b>ヒント</b> 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。</p> <p><b>(注)</b> <code>interface</code> コマンドを <code>external</code> または <code>internal</code> 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 <code>no</code> 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。</p>
<p><b>ステップ 13</b> <code>exit</code></p> <p><b>例：</b>  <pre>Router(config-oer-mc-br-if)# exit</pre></p>	<p>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。</p>
<p><b>ステップ 14</b> <code>interface type number internal</code></p> <p><b>例：</b>  <pre>Router(config-oer-mc-br)# interface GigabitEthernet 1/0/0 internal</pre></p>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

コマンドまたはアクション	目的
<b>ステップ 15</b> <code>exit</code>  <b>例 :</b> <code>Router(config-oer-mc-br)# exit</code>	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。
<b>ステップ 16</b> 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 <b>ステップ 11</b> から <b>ステップ 15</b> を繰り返します。	—
<b>ステップ 17</b> <code>keepalive timer</code>  <b>例 :</b> <code>Router(config-oer-mc)# keepalive 10</code>	(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。 <ul style="list-style-type: none"> <li>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。</li> </ul>
<b>ステップ 18</b> <code>end</code>  <b>例 :</b> <code>Router(config-oer-mc-learn)# end</code>	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。
<b>ステップ 19</b> <code>show running-config</code>  <b>例 :</b> <code>Router# show running-config</code>	(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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>key chain name-of-chain</b>  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	<b>key key-id</b>  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	<b>key-string text</b>  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	<b>exit</b>  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	<b>oer border</b>  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	<b>local type number</b>  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	<pre>master ip-address key-chain key-chain-name</pre> <p>例:</p> <pre>Router(config-oer-br)# master 10.1.1.1 key-chain border1_PFR</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li><i>key-chain-name</i> 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。</li> </ul>
ステップ 11	<pre>end</pre> <p>例:</p> <pre>Router(config-oer-br)# end</pre>	<p>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。</p>

## 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](#)」(P.18)
- 「[PfR 境界ルータの設定 : 例](#)」(P.19)

## 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
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• テクニカル サポートを受ける</li> <li>• ソフトウェアをダウンロードする</li> <li>• 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</li> <li>• ツールおよびリソースへアクセスする</li> <li>• Product Alert の受信登録</li> <li>• Field Notice の受信登録</li> <li>• Bug Toolkit を使用した既知の問題の検索</li> <li>• 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</li> <li>• トレーニング リソースへアクセスする</li> <li>• 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</li> </ul> <p>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。</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## 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、フィードバック、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。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2010 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社.  
All rights reserved.





## パフォーマンス ルーティング境界ルータ専用機能

---

Performance Routing (PfR; パフォーマンス ルーティング) によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズの集約サービス ルータ上での Border Router (BR; 境界ルータ) 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なければなりません。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。

### 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、「PfR 境界ルータ専用機能の機能情報」(P.12) 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

- 「PfR 境界ルータ専用機能の前提条件」(P.2)
- 「PfR 境界ルータ専用機能の制約事項」(P.2)
- 「PfR 境界ルータ専用機能に関する情報」(P.2)
- 「PfR 境界ルータ専用機能の設定方法」(P.5)
- 「PfR 境界ルータ専用機能の設定例」(P.9)
- 「関連情報」(P.10)
- 「その他の参考資料」(P.10)

- ・ [「PfR 境界ルータ専用機能の機能情報」 \(P.12\)](#)

## 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 シリーズ集約サービス ルータは、Cisco IOS XE Release 2.6.1 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

Cisco IOS XE Release 2.6.1 では、Cisco ASR 1000 シリーズ 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 Release 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。

## PfR 境界ルータ専用機能に関する情報

境界ルータ専用機能を設定するには、次の概念を理解する必要があります。

- ・ [「ASR 1000 シリーズ ルータ上での PfR 境界ルータ専用機能」 \(P.2\)](#)
- ・ [「PfR 境界ルータの運用」 \(P.4\)](#)

## 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 シリーズの集約サービス ルータ上での Border Router (BR; 境界ルータ) 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 は、次の 3 種類のトラフィック クラス パフォーマンス測定方式を使用します。

- ・ **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ときのトラフィック クラス エントリのパフォーマンス メトリックを測定します。学習および設定されたプレフィクスに基づき、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**：可能な限り詳細にトラフィック クラスをレプリケートする合成トラフィック ストリームを生成し、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 Service Level Agreement (IP SLA; IP サービス レベル契約) 機能を使用します。
- ・ **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**：ネットワーク内のトラフィック フローにより近い全体像を生成するため、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、**Command-line Interface (CLI; コマンドライン インターフェイス)** 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 **Border Router (BR; 境界ルータ)** 専用機能は次の機能をサポートします。

- **OER アクティブ プロープ送信元アドレス** : OER アクティブ プロープ送信元アドレス機能では、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 プロープの送信元として設定できます。OER アクティブ プロープ送信元アドレスの設定の詳細については、『[Configuring Advanced Performance Routing](#)』モジュールを参照してください。
- **スタティック アプリケーション マッピングを使用する OER アプリケーション認識型ルーティング** : スタティック アプリケーション マッピングを使用する OER アプリケーション認識型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する機能が導入されます。この機能では、**Performance Routing (PfR; パフォーマンス ルーティング)** ポリシーを学習リスト内にプロファイリングされたトラフィック クラスに適用できる、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す。各学習リストに別々のポリシーを適用できます。新しい **traffic-class** コマンドと **match traffic-class** コマンドが、PfR が自動的に学習できる、または手動で設定できるトラフィック クラス設定を簡略化するために導入されます。OER アクティブ プロープ送信元アドレスの設定の詳細については、『[Static Application Mapping Using Performance Routing](#)』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 ベースのプレフィクス学習を設定する方法の詳細については、『[Configuring Advanced Performance Routing](#)』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 ベースのプレフィクス学習** : OER ポートおよびプロトコル ベースのプレフィ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 ベースのプレフィクス学習を設定する方法の詳細については、『[Configuring Advanced Performance Routing](#)』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 レポート作成に対する 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** プロープを設定してホップバイホップ ベースのプレフィクス特性を判断する機能が導入されました。**traceroute** レポート作成に対するパフォーマンス ルーティング サポートでは、ホップバイホップ ベースでプレフィ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は、プローブ発信元 (境界ルータ) からターゲット プレフィクスに対する各ホップについて収集されます。詳細については、『[Configuring Performance Routing Cost Policies](#)』または『[Performance Routing Traceroute Reporting](#)』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、オートノマス システム内部のプレフィクスに宛てたオートノマス システム外部のプレフィ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。オートノマス システムから **Internet Service Provider (ISP; インターネット サービス プロバイダー)** への **External BGP (eBGP; 外部 BGP)** アドバタイズメントは、ネットワークに入るトラフィックの入口パスに影響する場合があります。PfR は eBGP アドバタイズメントを使用し、最適な入口選択を操作します。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、『[BGP Inbound Optimization Using Performance Routing](#)』モジュールを参照してください。



(注) Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズの集約サービス 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 値で構成されるキーと、要求されていないトラフィックを除外する機能、および対象とするトラフィックを集約する機能を組み合わせることで定義できます。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。この新機能によって、OER はアクティブおよびパッシブの両方でアプリケーション トラフィックを監視できます。ポリシー ルールおよびポート ベースのプレフィクス学習を設定する方法の詳細については、『[Configuring Advanced Performance Routing](#)』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 によって、PfR が IP Routing Information Base (RIB) 内の親ルート (正確に一致するルート、またはそれよりも具体的でないルート) を検索する機能が導入され、それにより、OSPF および IS-IS などの Interior Gateway Protocol (IGP) を含む IP ルート環境に PfR を導入できます。PIRO の構成の詳細については、『[Performance Routing - 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 モニタリングによって、高速モニタリング モードを設定す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、すべての出口はアクティブ モニタリングおよびパッシブ モニタリングを使用して継続的にプローブされます。このプローブ頻度は、高速フェールオーバー モニタリング モードで他のモニタリング モードよりも低い頻度に設定でき、高速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種類のアクティブ プローブ (ICMP エコー、ジッタ、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、『[Configuring Advanced Performance Routing](#)』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、この機能では、ハブおよびスポーク ネットワーク設計に続く mGRE Dynamic Multipoint VPN (DMVPN; ダイナミック マルチポイント VPN) 導入のサポートが追加されます。EIGRP ルート制御および mGRE DMVPN サポートの詳細については、『[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。
- **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、音声メトリック、ジッタ、および Mean Opinion Score (MOS; 平均オピニオン評点) に基づく音声トラフィックの発信最適化のサポートが提供されます。ジッタおよび MOS は音声トラフィックのための重要な量的メトリックであり、これらの音声メトリックは、PfR アクティブ プローブを使用して測定されます。ポリシー ルールおよびポート ベースのプレフィクス学習を設定する方法の詳細については、『[PfR Voice Traffic Optimization Using Active Probes](#)』モジュールを参照してください。
- **VPN IPsec/GRE トンネル最適化** : PfR は、IP Security (IPsec; IP セキュリティ) /Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) トンネル インターフェイスを PfR 管理対象 出口リンクとしてサポートしています。ネットワーク ベースの IPsec VPN だけがサポートされます。IPsec/GRE トンネル インターフェイスを PfR 管理対象出口リンクとして設定する方法の詳細については、『[Configuring VPN IPsec/GRE Tunnel Interfaces As PfR-Managed Exit Links](#)』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 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。

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。

## PfR 境界ルータ専用機能の設定方法

ここでは、次の作業について説明します。

- 「PfR 境界ルータの設定」(P.5)
- 「PfR 境界ルータ情報の表示」(P.7)

## 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。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 : 例」(P.9) 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。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。
- 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。

## 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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>必要に応じてパスワードを入力します。</li> </ul>
ステップ 2	<b>configure terminal</b>  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	<b>key chain name-of-chain</b>  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。 <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 4	<b>key key-id</b>  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。 <ul style="list-style-type: none"> <li>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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 5	<code>key-string text</code>  例： Router(config-keychain-key)# key-string bl	キーの認証文字列を指定します。 <ul style="list-style-type: none"><li>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。</li><li>任意の暗号化レベルを設定できます。</li></ul>
ステップ 6	<code>exit</code>  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	<code>oer border</code>  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。 <ul style="list-style-type: none"><li>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。</li></ul>
ステップ 9	<code>local type number</code>  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。 <ul style="list-style-type: none"><li>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。</li></ul>
ステップ 10	<code>master ip-address key-chain key-chain-name</code>  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。 <ul style="list-style-type: none"><li>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。</li><li><code>key-chain-name</code> 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。</li></ul>
ステップ 11	<code>end</code>  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は、「[関連情報](#)」(P.10) に進みます。

## 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序で入力できます。

## 手順の概要

1. **enable**
2. **show oer border**
3. **show oer border active-probes**
4. **show oer border passive prefixes**
5. **show oer 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。必要に応じてパスワードを入力します。

```
Router> enable
```

**ステップ 2 show oer 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。

```
Router# show oer 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 oer 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。

```
Router# show oer 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 oer border passive prefixes**

このコマンドは、PfR で監視されたプレフィクスおよびトラフィック フローについて NetFlow が収集するパッシブ測定情報を表示するために使用します。次の出力は、**show oer border passive prefixes** コマンドが実行された境界ルータに対して NetFlow がパッシブに監視中のプレフィクスを示しています。

```
Router# show oer border passive prefixes
```

```
OER Passive monitored prefixes:
```

```
Prefix      Mask  Match Type
10.1.5.0    /24   exact
```

### ステップ 5 show oer 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。この例では、プレフィクス 10.1.2.0/24 が PfR に制御される出力を示します。このコマンドは、親ルート照合および親ルートが EIGRP ルーティング テーブルから識別される際の既存の親ルートへのルートの変更を表示するために使用します。

```
Router# show oer 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

ここで説明する次の例では、次のサンプル PfR リンク グループを示します。

- [「PfR マスター コントローラの設定 : 例」 \(P.9\)](#)
- [「PfR 境界ルータの設定 : 例」 \(P.10\)](#)

## 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、「[ASR 1000 シリーズ ルータ上での PfR 境界ルータ専用機能](#)」(P.2) に説明されている Cisco IOS XE のサポート対象機能、および『[Configuring Basic Performance Routing](#)』モジュール、または「[関連資料](#)」(P.10) のその他の参考資料を参照してください。

## その他の参考資料

ここでは、NAT 機能を使用するパフォーマンス ルーティングに関連した関連資料を示します。

### 関連資料

内容	参照先
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
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	『 <a href="#">Cisco IOS Optimized Edge Routing Command Reference</a> 』
Cisco IOS XE リリースでの基本的な PfR 設定	『 <a href="#">Configuring Basic Performance Routing</a> 』モジュール
高度な PfR 設定	『 <a href="#">Configuring Advanced Performance Routing</a> 』モジュール



内容	参照先
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

## シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• テクニカル サポートを受ける</li> <li>• ソフトウェアをダウンロードする</li> <li>• 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</li> <li>• ツールおよびリソースへアクセスする</li> <li>• Product Alert の受信登録</li> <li>• Field Notice の受信登録</li> <li>• Bug Toolkit を使用した既知の問題の検索</li> <li>• 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</li> <li>• トレーニング リソースへアクセスする</li> <li>• 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</li> </ul> <p>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。</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

## PfR 境界ルータ専用機能の機能情報

表 1 に、この機能のリリース履歴を示します。

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 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	Performance Routing (PfR; パフォーマンス ルーティング) によって、Cisco IOS XE Release 2.6.1 内の Cisco ASR 1000 シリーズの集約サービス ルータ上での Border Router (BR; 境界ルータ) 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。  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。 <b>show oer border passive cache</b> 、 <b>show oer master prefix</b>

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2010 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社 .  
All rights reserved.





## NAT を使用するパフォーマンス ルーティング

Performance Routing (PfR; パフォーマンス ルーティング) によって、NAT を使用するネットワークでのスタティック ルーティングによるトラフィック クラスの制御のサポートが導入され、これに伴って既存の 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 機能を同じルータ上で設定し、PfR がスタティック ルーティングを使用するトラフィック クラスのルーティングを制御する場合、一部のアプリケーションはパケットの廃棄のために動作に失敗する可能性があります。このパケットの廃棄動作は、同じルータから複数の ISP に接続するためにスタティック ルーティングが使用される場合に見られ、PfR はトラフィック クラス ルーティングを制御するためにスタティック ルーティングを使用し、セキュリティ上の理由によって 1 つまたは複数の ISP が **Unicast Reverse Path Forwarding (Unicast RPF; ユニキャスト Reverse Path Forwarding)** フィルタリングを使用します。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。

この新しい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。

### 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、「[NAT を使用するパフォーマンス ルーティングの機能情報](#)」(P.11) 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

- 「[NAT を使用するパフォーマンス ルーティングの前提条件](#)」(P.2)
- 「[NAT を使用するパフォーマンス ルーティングの制約事項](#)」(P.2)
- 「[NAT を使用するパフォーマンス ルーティングについて](#)」(P.2)
- 「[NAT を使用するパフォーマンス ルーティングの設定方法](#)」(P.4)

- 「[NAT を使用するパフォーマンス ルーティングの設定例](#)」 (P.7)
- 「[関連情報](#)」 (P.8)
- 「[その他の参考資料](#)」 (P.9)
- 「[NAT を使用するパフォーマンス ルーティングの機能情報](#)」 (P.11)

## 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 シリーズ集約サービス ルータは、Cisco IOS XE Release 2.6.1 以降のリリースを実行している必要があります。

## NAT を使用するパフォーマンス ルーティングの制約事項

- Cisco IOS XE Release 2.6.1 以降のリリースを実行する Cisco ASR 1000 シリーズの集約サービス 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。
- Cisco IOS XE Release 2.6.1 では、Cisco ASR 1000 シリーズ 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 Release 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。

## NAT を使用するパフォーマンス ルーティングについて

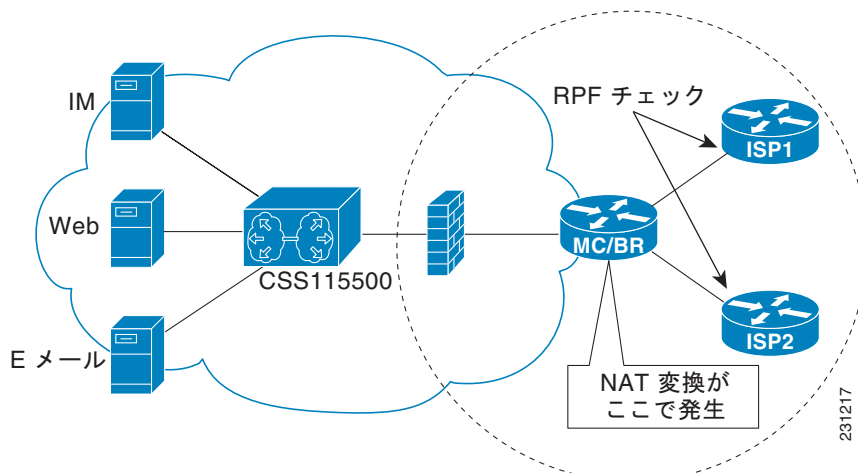
NAT を使用する PfR を設定するには、次の概念を理解する必要があります。

- 「[PfR および NAT](#)」 (P.2)
- 「[ネットワーク アドレス変換 \(NAT\)](#)」 (P.4)
- 「[内部グローバルアドレスのオーバーロード](#)」 (P.4)

## PfR および NAT

PfR および NAT 機能を同じルータ上で設定し、PfR がスタティック ルーティングを使用するトラフィック クラスのルーティングを制御する場合、一部のアプリケーションはパケットの廃棄のために動作に失敗する可能性があります。このパケットの廃棄動作は、同じルータから複数の ISP に接続するためにスタティック ルーティングが使用される場合に見られ、PfR はトラフィック クラス ルーティングを制御するためにスタティック ルーティングを使用し、セキュリティ上の理由によって 1 つまたは複数の ISP が Unicast Reverse Path Forwarding (Unicast RPF; ユニキャスト Reverse Path Forwarding) フィルタリングを使用します。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 変換の実行後、PfR がトラフィック クラスに対して発信パケットのルートのある出口から別の出口インターフェイスに変更するため、ユニキャスト RPF を実行中の受信側ルータでパケットが破棄されます。パケットの送信時、受信側ルータでのユニキャスト RPF フィルタリングで、NAT が割り当てた発信元アドレス プールと異なる発信元 IP アドレスが示され、パケットが破棄されます。例として、NAT を使用する PfR の動作方法を [図 1](#) に示します。

図 1 NAT を使用する PfR



NAT 変換が内部ネットワークに接続されたルータで発生し、このルータとして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ためにルートを変更した場合、ISP1 へのインターフェイスを介してルーティングされた図 1 の境界ルータからのトラフィックは、トラフィック パフォーマンスの測定とポリシーしきい値の適用後に ISP2 へのインターフェイスを介してルーティングされる可能性があります。RPF チェックが ISP ルータで実行されますが、現在 ISP2 を介してルーティングされているすべてのパケットは、発信元インターフェイスの IP アドレスが変更されているため、ISP2 の受信側ルータでの RPF チェックに失敗します。



(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。図 1 ではルータは境界ルータであり、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 は図 1 のインターフェイス A から ISP1、およびインターフェイス B から ISP2 の 2 つのインターフェイスを使用する境界ルータ上でトラフィックを管理するように設定されます。まず、PfR は 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、このトラフィックに対する NAT 変換は、インターフェイス A に設定されたパケット内の発信元 IP アドレスですでに存在します。PfR はトラフィック パフォーマンスを測定し、インターフェイス B が現在トラフィック フローに対する最適な出口であると判断しますが、PfR は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 クラスを学習して測定するように設定され、その E メールトラフィックが開始された場合、NAT 変換はインターフェイス B に対して行われます。PfR スタティック ルーティング NAT ソリューションは、1 つにパッケージ化されたソリューションであり、NAT を使用する複数のルータ上のインターフェイスを使用し、PfR によって管理される設定はサポートされません。NAT を使用するネットワーク設定および Cisco IOS XE ソフトウェアが実行されていない PIX ファイアウォールなどのデバイスはサポートされません。

PfR スタティック ルーティング NAT ソリューションの設定方法の詳細については、「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」(P.4) を参照してください。

## ネットワーク アドレス変換 (NAT)

NAT によって、登録されていない IP アドレスを使用してインターネットに接続する、プライベート IP インターネットワークが可能になります。NAT は、通常ルータ上で動作して 2 つのネットワークを結びつけ、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 (グローバルに固有ではない) アドレスを合法的なアドレスに変換します。NAT はネットワーク全体に対して 1 つのアドレスだけを外部向けにアドバタイズするように設定できます。この機能によって、セキュリティが強化され、内部ネットワーク全体を 1 つのアドレスの背後に効果的に隠すことができます。

また、NAT は企業エッジで使用してインターネットへの内部ユーザ アクセスを許可し、メール サーバなどの内部デバイスへのインターネット アクセスを許可することもできます。

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

多くのローカルアドレスに対しルータで 1 つのグローバルアドレスを使用することで、内部グローバルアドレス プールのアドレスを保護できます。このオーバーロードを設定すると、ルータは上位レベルのプロトコル (TCP または UDP ポート番号など) からの十分な情報を使用して、グローバルアドレスを元通りのローカルアドレスに変換します。複数のローカルアドレスを 1 つのグローバルアドレスにマップする場合、ローカルアドレスの識別は各内部ホストの TCP または UDP ポート番号で行います。

## NAT を使用するパフォーマンス ルーティングの設定方法

ここでは、次の作業について説明します。

- 「[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](#)」(P.4)

## 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

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できるように PfR を設定するには、この作業を実行します。この作業では、インターネットへの内部ユーザ アクセスを許可しながら、PfR がトラフィック クラスを最適化できるようにします。

Cisco IOS PfR および NAT 機能を同じルータ上で設定し、PfR がスタティック ルーティングを使用するトラフィック クラスのルーティングを制御する場合、一部のアプリケーションはパケットの廃棄のために動作に失敗する可能性があります。このパケットの廃棄動作は、同じルータから複数の ISP に接続するためにスタティック ルーティングが使用される場合に見られ、PfR はトラフィック クラスルーティングを制御するためにスタティック ルーティングを使用し、セキュリティ上の理由によって 1 つまたは複数の ISP が Unicast Reverse Path Forwarding (Unicast RPF; ユニキャスト Reverse Path Forwarding) フィルタリングを使用します。

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。この作業では、単一の IP アドレスを使用しますが、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 プールを使用する設定例については、「[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](#)」(P.4) 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 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。



(注) PfR スタティック ルーティング NAT ソリューションは、1 つにパッケージ化されたソリューションであり、NAT を使用する複数のルータ上のインターフェイスを使用し、PfR によって管理される設定はサポートされません。

NAT の設定方法の詳細については、『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。

## 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-number* | **prefix-list** *prefix-list-name*}
6. **match interface** *interface-type interface-number* [...*interface-type interface-number*]
7. **exit**
8. ルート マップ設定を続けるには、必要に応じて**ステップ 4**から**ステップ 7**を繰り返します。
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	<code>enable</code>  例: Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>必要に応じてパスワードを入力します。</li></ul>
ステップ 2	<code>configure terminal</code>  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	<code>access-list access-list-number {permit   deny} ip-address mask</code>  例: Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255	変換される IP アドレスを許可する標準アクセス リストを定義します。 <ul style="list-style-type: none"><li>アクセス リストでは、変換するこれらのアドレスだけを許可する必要があります (各アクセス リストの末尾に暗黙の「deny all」設定があることに注意してください)。許容度が高すぎるアクセス リストを使用すると、予期しない結果になる場合があります。</li></ul>
ステップ 4	<code>route-map map-tag [permit   deny] [sequence-number]</code>  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、ルート マップを設定します。 <ul style="list-style-type: none"><li>この例では、BGP という名前のルート マップを作成します。</li></ul>
ステップ 5	<code>match ip address {access-list access-list-name   prefix-list prefix-list-name}</code>  例: Router(config-route-map)# match ip address access-list 1	アクセス リストまたはプレフィクス リストの <code>match</code> 句エントリをルート マップに作成し、NAT で変換するトラフィックを識別します。 <ul style="list-style-type: none"><li>この例では、<code>match</code> 条件として 10.1.0.0 0.0.255.255 を指定する、<a href="#">ステップ 3</a> で作成したアクセス リストを参照します。</li></ul>
ステップ 6	<code>match interface interface-type interface-number [...interface-type interface-number]</code>  例: Router(config-route-map)# match interface serial 1/0	指定したインターフェイスの 1 つと一致する任意のルートを配布するため、ルート マップ内に <code>match</code> 句を作成します。 <ul style="list-style-type: none"><li>この例では、シリアル インターフェイス 1/0 を介して <a href="#">ステップ 5</a> の <code>match</code> 句に合格するルートを配布する <code>match</code> 句を作成します。</li></ul>
ステップ 7	<code>exit</code>  例: Router(config-route-map)# exit	ルート 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 8	ルート マップ設定を続けるには、必要に応じて <a href="#">ステップ 4</a> から <a href="#">ステップ 7</a> を繰り返します。	—
ステップ 9	<code>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]</code>  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、オーバーロードによるダイナミック発信元変換を確立します。 <ul style="list-style-type: none"><li><code>interface</code> キーワードと、種類および番号の引数を使用してインターフェイスを指定します。</li><li><code>oer</code> 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。</li></ul>

	コマンドまたはアクション	目的
ステップ 10	<code>interface type number</code>  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	<code>ip address ip-address mask</code>  例： Router(config-if)# ip address 10.114.11.8 255.255.255.0	インターフェイスに対するプライマリ IP アドレスを設定します。
ステップ 12	<code>ip nat inside</code>  例： Router(config-if)# ip nat inside	インターフェイスを内部に接続するものとしてマークします。
ステップ 13	<code>exit</code>  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、コンフィギュレーション モードに戻ります。
ステップ 14	<code>interface type number</code>  例： Router(config)# interface GigabitEthernet 1/1/0	別の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 モードに戻ります。
ステップ 15	<code>ip address ip-address mask</code>  例： Router(config-if)# ip address 172.17.233.208 255.255.255.0	インターフェイスに対するプライマリ IP アドレスを設定します。
ステップ 16	<code>ip nat outside</code>  例： Router(config-if)# ip nat outside	インターフェイスを外部に接続するものとしてマークします。
ステップ 17	<code>end</code>  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 を使用するパフォーマンス ルーティングの設定例

ここで説明する次の例では、次のサンプル PfR リンク グループを示します。

- 「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」(P.8)

## 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、PfR がネットワーク内で 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できるようにマスター コントローラを設定する設定例を示します。次の例は、NAT 変換のために IP アドレス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 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。

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、インターネットへの内部ユーザ アクセスを許可しながら、PfR がトラフィック クラスを最適化できるようにします。この例では、NAT を使用して変換されるトラフィック クラスがアクセス リストおよびルート マップを使用して指定します。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 PfR がパケットに対して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、1 つにパッケージ化されたソリューションであり、NAT を使用する複数のルータ上のインターフェイスを使用し、PfR によって管理される設定はサポートされません。

```
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 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 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
```

## 関連情報

その他のパフォーマンス ルーティング機能または概念に関する一般的な資料については、「[関連資料](#)」(P.9) の参考資料を参照してください。

## その他の参考資料

ここでは、NAT 機能を使用するパフォーマンス ルーティングに関連した関連資料を示します。

### 関連資料

内容	参照先
Cisco IOS コマンド	<a href="#">『Cisco IOS Master Commands List, All Releases』</a>
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	<a href="#">『Cisco IOS Optimized Edge Routing Command Reference』</a>
Cisco IOS XE リリースでの基本的な PfR 設定	<a href="#">『Configuring Basic Performance Routing』</a> モジュール
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	<a href="#">『Performance Routing Border Router Only Functionality』</a> モジュール
高度な PfR 設定	<a href="#">『Configuring Advanced Performance Routing』</a> 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	<a href="#">『Understanding Performance Routing』</a> モジュール
Cisco IOS XE リリースの PfR 機能の場所	<a href="#">『Cisco IOS XE Performance Routing Features Roadmap』</a> モジュール
NAT に関する一般情報	<a href="#">『Configuring NAT for IP Address Conservation』</a> モジュール

## シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"><li>• テクニカル サポートを受ける</li><li>• ソフトウェアをダウンロードする</li><li>• 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</li><li>• ツールおよびリソースへアクセスする</li><li>• Product Alert の受信登録</li><li>• Field Notice の受信登録</li><li>• Bug Toolkit を使用した既知の問題の検索</li><li>• 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</li><li>• トレーニング リソースへアクセスする</li><li>• 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</li></ul> <p>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。</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

# NAT を使用するパフォーマンス ルーティングの機能情報

表 1 に、この機能のリリース履歴を示します。

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、フィアチャセット、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 NAT を使用するパフォーマンス 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 <sup>1</sup>	Cisco IOS XE Release 2.6.1	PfR がネットワーク内で 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 クラスを制御できるようにするためにサポートされます。  この機能は、Cisco ASR 1000 シリーズの集約サービス ルータで導入されました。  この機能によりコマンド <b>ip nat inside source</b> が変更されました。

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。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2010 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社.  
All rights reserved.

