



PfR ターゲット検出 v1.0

パフォーマンス ルーティング ターゲット検出 v1.0 機能により、IP SLA Responder の特定および設定の自動化、パフォーマンスルーティング (PfR) アクティブプローブの使用を最適化して、大企業のブランチ ネットワーク間のビデオおよび音声アプリケーションのパフォーマンスを管理するためのスケーラブルなソリューションが導入されています。音声およびビデオトラフィックを使用してメディアアプリケーションを最適化するために、PfR では、ジッター、損失、および遅延の測定値が使用されます。IP SLA udp ジッター プローブではこれらの測定値が提供されますが、IP SLA Responder が必要です。各送信先プレフィックスの IP SLA Responder アドレスの手動設定は、大企業のブランチ ネットワークに拡張性の問題をもたらします。PfR ターゲット検出 v1.0 機能では、マスター コントローラ (MC) ピアリングを導入し、EIGRP Service Advertisement Framework (SAF) 経由で Service Routing (SR) を使用して、IP SLA Responder および関連付けられた送信先 IP プレフィックスをアドバタイズ、検出、および自動設定します。



(注)

パフォーマンス ルーティング (PfR) ターゲット検出 v1.0 機能では、Cisco ASR1000 プラットフォームのプレフィックスの検出はサポートされていません。

- [機能情報の確認, 1 ページ](#)
- [PfR ターゲット検出の概要, 2 ページ](#)
- [PfR ターゲット検出の設定方法, 7 ページ](#)
- [PfR ターゲット検出の設定例, 15 ページ](#)
- [その他の関連資料, 22 ページ](#)
- [PfR ターゲット検出の機能情報, 23 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載さ

れている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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

PfR ターゲット検出の概要

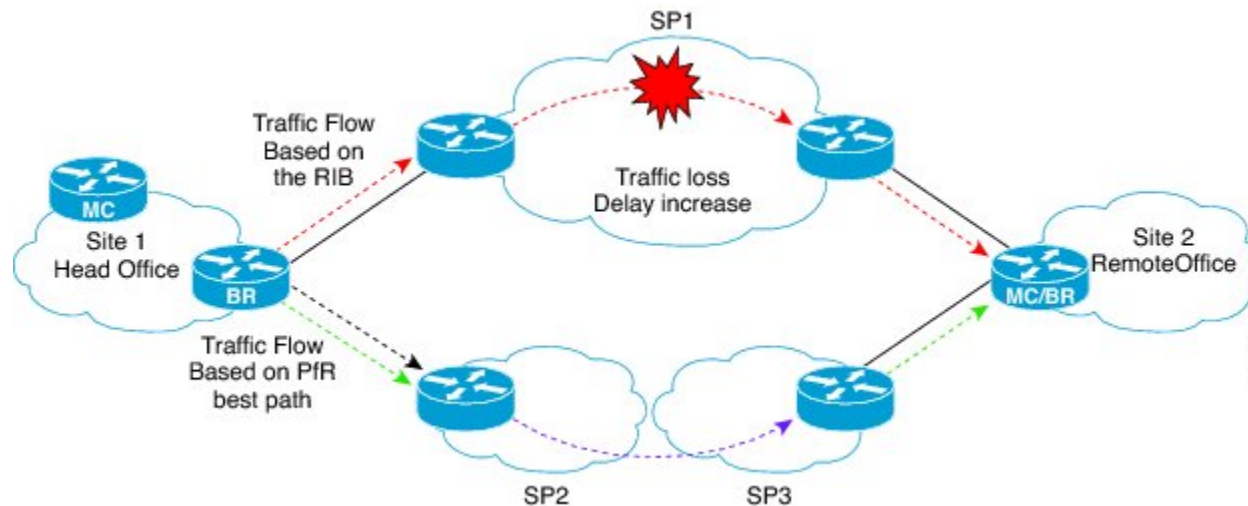
PfR ターゲット検出

Cisco Performance Routing (PfR) は、アプリケーション パフォーマンスの要件を満たす最適なパスを選択する機能を追加することで、従来の IP ルーティングテクノロジーを補完します。次の図は、PfR と従来の IP ルーティングテクノロジーの違いを示しています。次の図では、トラフィックはサイト 1 の本社からサイト 2 のリモート オフィスに向かっています。従来のルーティングテクノロジーは、ルーティングテーブル情報を使用して、パスが短いサービスプロバイダー 1 を経由してトラフィックをルーティングします。ただし、大きな輻輳があるとトラフィックの損失につながり、SP1 経由での遅延が増加します。従来のルーティングテクノロジーでは、パフォーマンスの低下を認識できず、引き続き SP1 経由でトラフィックがルーティングされます。PfR は、到達可能性、遅延、損失、ジッター、MOS、スループット、および負荷などのデータ測定値、および金銭的成本とユーザ定義のポリシーを考慮する能力によって決定される最良のパスを使用して、ネットワーク間でトラフィックをルーティングします。従来の IP ルーティングテクノロジーとは異なり、PfR はリアルタイムのパフォーマンス メトリックに基づく適応型ルーティングの調整を提供します。たとえば、次の図では、PfR は SP1 を経由するトラフィックのパフォーマンス測定値が悪いため、最良のパスである SP2 および SP3 経由でトラフィックを再ルーティングします。



(注) 次のネットワーク図は、小規模な企業ネットワーク向けの MPLS VPN ネットワークとインターネット サービス プロバイダー (ISP) 内の両方の SP に関連しています。

図 1: PfR と従来のルーティング テクノロジー



音声およびビデオ アプリケーションを最適化するために、PfR では、ジッター、損失、および遅延の測定値を使用して、最適なメディア パスを決定します。IP SLA udp ジッター プロブではこれらの測定値が提供されますが、IP SLA Responder が必要です。PfR は、音声およびビデオトラフィック クラスの送信先プレフィックスに最も近い IP SLA Responder の IP アドレスを認識している必要があります。各 PfR アプリケーション ポリシー内の送信先 IP プレフィックスの範囲ごとに IP SLA Responder を手動で設定するのは、WAN を介した何百または何千ものブランチ サイトがある企業ネットワークではスケーラブルなソリューションとは見なされません。

このような手動設定の問題に対応するために、PfR ターゲット検出では、マスター コントローラのピアリングを導入し、IP SLA Responder の IP アドレスをアドバタイズするために EIGRP Service Advertisement Framework (SAF) を使用して、レスポンドと関連付けられた送信先 IP プレフィックスの範囲の自動検出と設定を可能にします。

ターゲット検出データの配信

PfR ターゲット検出は、次の 2 つの利点をもたらすデータ配信メカニズムを使用します。

- 送信先とポリシーごとの IP SLA ターゲット コンフィギュレーションの削減。
- 複数ポリシー間でプローブ データを共有することによる、IP SLA プロブ効率の向上。

ターゲット検出を実行する各 PfR マスター コントローラ (MC) は、他の MC が WAN 経由で検出または学習するために、既知のローカル IP プレフィックスの範囲およびローカル IP SLA Responder をアドバタイズします。ターゲット検出を実行する各 MC は、他の MC からアドバタイズされた

IP SLA Responder および関連付けられた送信先 IP プレフィックスの範囲も学習し、IP SLA Responder からのプローブ データを必要とするポリシーを動的に設定します。PfR は、Cisco Service Routing (SR) および Service Advertisement Framework (SAF) を使用して、IP SLA ターゲット情報を配信 および検出します。

SAF の詳細については、『*Service Advertisement Framework Configuration Guide*』を参照してください。

SAF を使用したマスター コントローラのピアリング

PfR マスター コントローラのピアリングは、Service Advertisement Framework (SAF) 上で実行されます。異なるサイトにある MC 間のピアリングを確立するために、各マスター コントローラで Service Routing (SR) フォワーダを使用します。MC のピアリングにより、PfR ターゲット検出 データのアドバタイズメントと検出が可能になります。

ハブ サイト（ヘッドエンドとして知られる）およびブランチ オフィスのターゲット検出対応 MC は、SR 内部クライアントおよび SR フォワーダの両方として機能します。いずれかのターゲット 検出サービスをアドバタイズする前に、MC は SR フォワーダとして、SR ピアリング用に設定する 必要があります。MC のピアリングが確立されると、MC はローカル情報をアドバタイズして、 他の MC がターゲット検出および自動設定を実行できるようにします。

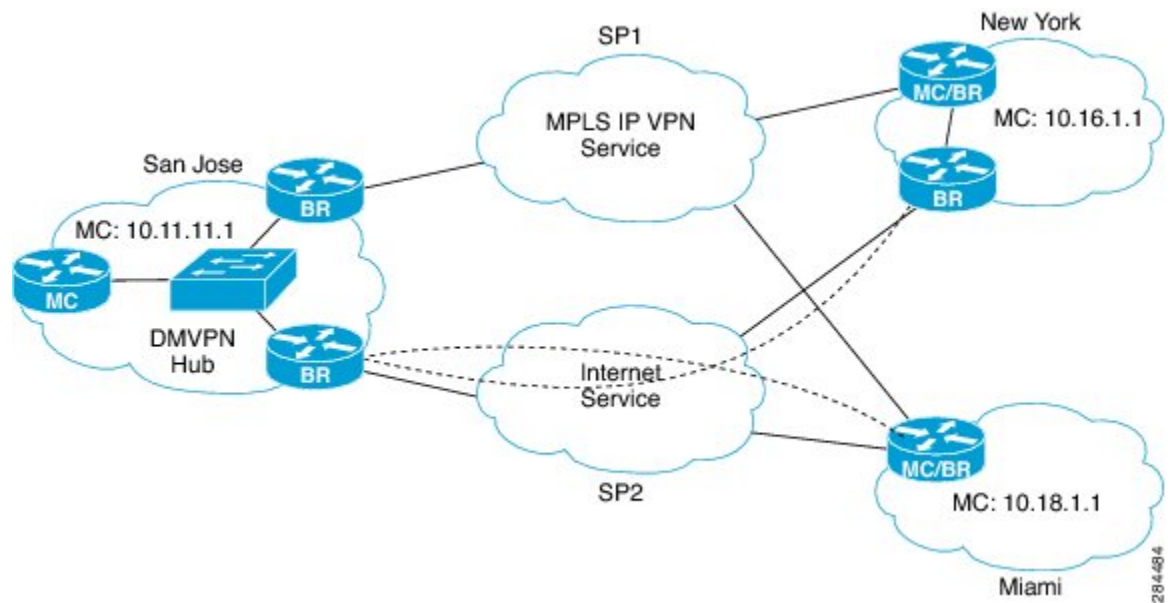
ネットワークの導入はカスタマーごとに異なり、導入ごとに、SR トポロジコンフィギュレーションを設定するさまざまな方法があります。カスタマーがネットワークに使用している導入モデル により、SR フォワーダの設定方法が決まります。ターゲットの検出機能の MC-MC ピアリング アスペクトは、2 つの異なるカスタマー ネットワークの導入をサポートしています。

- マルチホップ：カスタマー ヘッドエンドおよびブランチ オフィスがカスタマーの管理下に ない、または SAF 対応でない 1 台以上のルータで分離されているネットワーク。例として は、MPLS VPN WAN サービスです。
- SAF-Everywhere：ヘッドエンド MC からブランチ オフィス MC への隣接パスにある EIGRP SAF に対してすべてのルータがイネーブルになっているネットワーク。例としては、DMVPN WAN です。

次の図のトポロジは、マルチホップ タイプのネットワークでの MC のピアリングの導入例を示し ています。ハブ サイト（サンノゼ）MC システムとブランチ オフィス サイト（ニュー YORK と マイアミ）MC システムは、論理的なユニキャスト トポロジ間でピアリングします。このモデル

では、ハブ サイトとブランチ サイトは、EIGRP SR フォワーダが設定されていないネットワーク（通常はサービス プロバイダー（SP））によって分離されています。

図 2: **MPLS IP VPN** および **DMVPN** を使用したマルチホップ ネットワーク トポロジ

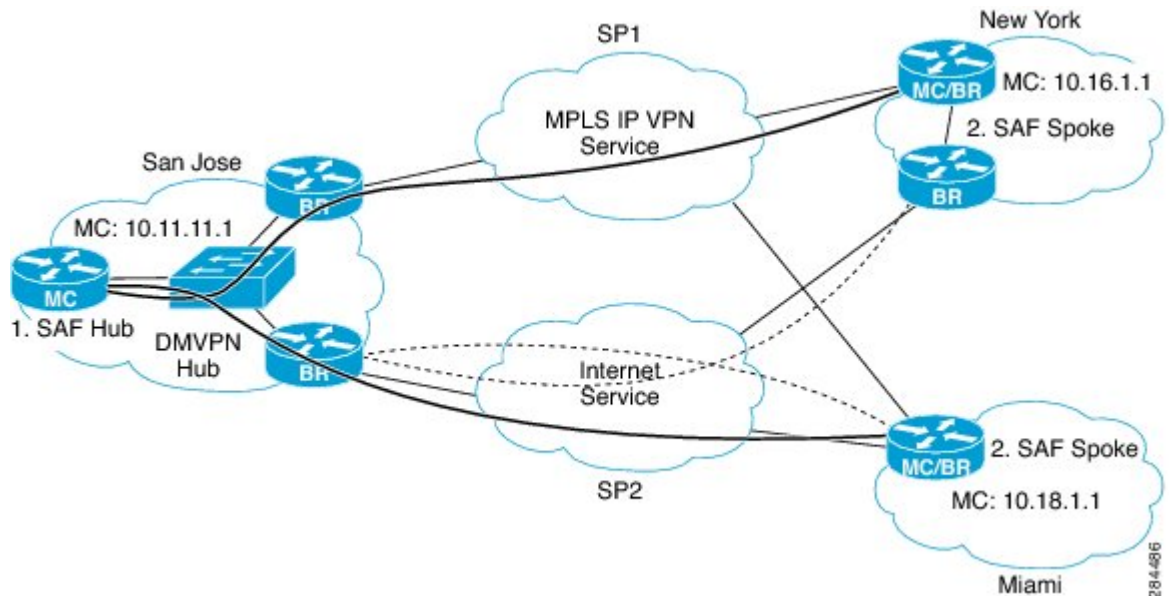


次の図は、前述の図の MPLS IP VPN および DMVPN を実行している同じ企業 WAN ネットワークに実装されている PfR ターゲット検出を示しています。MC のピアリングをイネーブルにすると、サンノゼのマスターコントローラは SAF ハブ フォワーダになり、ニューヨークとマイアミの MC はサンノゼの MC とピアリングされます。ターゲット検出では、各 MC が SAF を使用してローカル IP プレフィックスおよび IP SLA Responder をアドバタイズできます。各 MC は SAF からリモート IP プレフィックスおよび IP SLA Responder を学習します。PfR は、ネットワーク パフォーマンスを測定するためにリモート サイトの IP SLA Responder をプローブします。

マルチホップ ネットワーク経由の MC のピアリングは、BGP ルート リフレクタに似たオーバーレイ モデルです。MC のピアリング システムは、ネットワーク経由で到達可能（ルーティング可

能) である IP アドレスを指定して、送信元ループバックインターフェイスを設定する必要があります。

図 3: マルチホップ エンタープライズ WAN ネットワーク内でイネールになっている MC のピアリングとターゲット検出



マスターコントローラのピアリングの設定オプション

ターゲット検出を実行する各 Pir マスターコントローラ (MC) は、他の MC が WAN 経由で検出または学習するために、既知のローカル IP プレフィックスの範囲およびローカル IP SLA Responder をアドバタイズします。ターゲット検出を実行する各 MC は、他の MC からアドバタイズされた IP SLA Responder および関連付けられた送信先 IP プレフィックスの範囲も学習し、プローブデータを必要とするポリシーを動的に設定します。

ネットワーク構造およびプローブターゲットと IP SLA Responder の設定に必要な制御の程度に応じて、**mc-peer** コマンドを使用して MC のピアリングを設定する際に使用できる主なオプションが 3 つあります。

- ヘッドエンド (ハブサイト) またはピア IP アドレス (ブランチサイト) を設定する。このオプションを使用する場合、SAF EIGRP 隣接関係のソースとしてループバックインターフェイスを設定することを推奨します。この設定オプションは、マルチホップタイプのネットワークで使用されます。
- SAF ドメイン ID を設定する、またはデフォルトの SAF ドメイン ID の 59501 を使用する。このオプションでは、ハブサイトとブランチサイトの両方のマスターコントローラルータに EIGRP SAF を設定する必要があります。また、SAF-Everywhere タイプのネットワークで使用できます。

- SAF EIGRP の自動設定がない EIGRP オプションを設定する。このオプションは、SAF-Everywhere タイプのネットワークで使用されます。SAF がネットワーク内のルータにすでに設定されている場合、同じネットワークとオーバーレイ PfR ターゲット検出を使用できます。PfR ターゲット検出とは別に SAF を設定する方法については、SAF のコンフィギュレーション ガイドを参照してください。



(注) CSCud06237 では、PfR ターゲット検出で **mc-peer eigrp** コマンドを使用する場合、PfR がローカル ID を選択できるように、ループバック インターフェイスを指定する必要があります。

PfR ターゲット検出の設定方法

マルチホップネットワークのハブサイト用 PfR ターゲット検出および MC のピアリングの設定

ネットワークのヘッドエンドにあるマスター コントローラ（通常はハブ サイトのマスター コントローラ）で、PfR マスターコントローラ（MC）のピアリングを設定するには、このタスクを実行します。マスターコントローラは、ルーティング機能を持つデバイスである必要があります。このタスクでは、ハブ サイトとブランチ サイト間のネットワーク クラウドがカスタマーの管理下でない、または SAF 対応でないマルチホップ タイプのネットワークを想定しています。この設計では、ハブ サイトの MC は、ブランチの MC SAF フォワーダがアドバタイズメントを交換するためにピアリングする Service Advertisement Facility (SAF) フォワーダ ハブになります。ハブ サイトの MC は、同じ SAF ドメイン ID と MD5 認証を持つブランチの MC からのピアリング要求を受け入れます。



(注) このタスクでは、ダイナミックな PfR ターゲット検出がイネーブルになります。この方法は、SAF がネットワーク内で他のアプリケーションに対してすでにイネーブルになっている、または MC と SAF 間に既存の隣接関係がある場合に適しています。たとえば、DMVPN WAN で、複数の PfR MC が DMVPN トンネル デバイスに共存している場合、それらには SAF 隣接関係もあり、スタティック ピアリングは必要ありません。



(注) PfR は、スポークツースポーク トンネリングをサポートしていません。Next Hop Resolution Protocol (NHRP) 設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **target-discovery**
5. **mc-peer** [*head-end* | *peer-address*] [*loopback interface-number*] [*description text*] [*domain domain-id*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	pfr master 例 : Device(config)# pfr master	PfR マスター コントローラ コンフィギュレーション モードを開始して、マスター コントローラ としてシスコ デバイスを設定します。
ステップ 4	target-discovery 例 : Device(config-pfr-mc) # target-discovery	PfR ターゲット検出を設定します。 • この例では、ダイナミックな PfR ターゲット検出が設定されます。
ステップ 5	mc-peer [<i>head-end</i> <i>peer-address</i>] [loopback interface-number] [description text] [domain domain-id] 例 : Device(config-pfr-mc) # mc-peer head-end loopback1 description SJ-hub	この例では、このデバイスがハブ（ヘッドエンド）デバイスであることを示すために、PfR マスター コントローラのピアリングが設定されます。 • MC のピアリングに使用される SAF ドメイン ID を指定するには、 domain キーワードを使用します。 <i>domain-id</i> 引数は、1 から 65535 の範囲で指定します。 SAF ドメイン ID を指定しない場合、デフォルト値の 59501 が使用されます。

	コマンドまたはアクション	目的
ステップ 6	end 例 : Device(config-pfr-mc) # end	(任意) PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

マルチホップネットワークのブランチ オフィス用 PfR ターゲット検出および MC のピアリングの設定

スポーク ルータとして機能するブランチ オフィスで PfR ターゲット検出のスタティック モードを使用して PfR MC のピアリングを設定するには、このタスクを実行します。この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、MC のピアリングを可能にするためにループバック インターフェイスとして設定されます。このタスクでは、ハブ サイトとブランチ オフィス間のネットワーク クラウドがカスタマーの管理下でないマルチホップ タイプのネットワークを想定しています。



(注) PfR は、スポークツースポーク トンネリングをサポートしていません。Next Hop Resolution Protocol (NHRP) 設定の一環として、インターフェイス コンフィギュレーション モードで **ip nhrp server-only** コマンドを設定して、スポークツースポーク ダイナミック トンネルをディセーブルにします。

はじめる前に

PfR マスター コントローラ (MC) ピアリングは、ネットワークのハブ サイト（ヘッドエンド）にあるルーティング機能を備えたデバイスに設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mc-peer** [*peer-address loopback interface-number*] [**description text**] [**domain domain-id**]
5. **target-discovery**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	pfr master 例 : Device(config)# pfr master	PfR マスター コントローラ コンフィギュレーション モードを開始して、マスター コントローラ としてシスコ デバイスを設定します。
ステップ 4	mc-peer [<i>peer-address</i> loopback <i>interface-number</i>] [description <i>text</i>] [domain <i>domain-id</i>] 例 : Device(config-pfr-mc)# mc-peer 10.11.11.1 loopback1	この例では、ネットワークの本社（ヘッドエンド）にある PfR マスター コントローラ ハブ デバイスの IP アドレスは、ピア アドレスとして設定されます。
ステップ 5	target-discovery 例 : Device(config-pfr-mc)# target-discovery	ダイナミックな PfR ターゲット検出を設定します。
ステップ 6	end 例 : Device(config-pfr-mc)# end	（任意）PfR マスター コントローラ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PfR ターゲット検出を使用したターゲットおよび IP プレフィックスの範囲のスタティック定義のイネーブル化

PfR ターゲット検出は、ルーティング機能を備えた境界デバイスで IP SLA Responder を動的にイネーブルにし、サイト固有の IP プレフィックスの範囲を学習できます。この情報は、ローカル PfR マスター コントローラ (MC) から他の MC にアドバタイズされます。SAF によってアドバタイズされる IP SLA Responder および IP プレフィックスの範囲をスタティックに設定するには、このタスクを実行します。このタスクは、ハブサイトのマスターコントローラで実行されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list list-name [seq seq-value] {deny network/length | permit network/length}**
4. 必要に応じてステップ 3 を繰り返して、プレフィックス リストを作成します。
5. **pfr master**
6. **target-discovery responder-list prefix-list-name [inside-prefixes prefix-list-name]**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	ip prefix-list list-name [seq seq-value] {deny network/length permit network/length} 例 : Device(config)# ip prefix-list ipfx permit 10.101.1.0/24	アクティブ プローブのターゲットプレフィックスの IP プレフィックス リストを作成します。 • IP プレフィックス リストを学習リスト コンフィギュレーションモードで使用すると、学習される IP アドレスをフィルタリングすることができます。 • この例では、PfR にプレフィックス 10.101.1.0/24 をプロファイリングさせるために ipfx という名前の IP プレフィックス リストを作成します。

	コマンドまたはアクション	目的
ステップ 4	必要に応じてステップ 3 を繰り返して、プレフィックス リストを作成します。	—
ステップ 5	pfr master 例： Device(config)# pfr master	PfR マスター コントローラ コンフィギュレーションモードを開始して、マスター コントローラとしてルーティング機能を備えたシスコ デバイスを設定します。
ステップ 6	target-discovery responder-list prefix-list-name [inside-prefixes prefix-list-name] 例： Device(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx	PfR ターゲット検出を設定します。 • この例では、PfR ターゲット検出は、IP SLA Responder と内部プレフィックスの IP アドレスのスタティック設定を使用して設定されます。
ステップ 7	end 例： Device(config-pfr-mc)# end	(任意) PfR マスター コントローラ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

この例では、ハブ デバイスは、プロンプトに示されているように、ハブ サイトのマスター コントローラです。スポーク（ブランチオフィス）デバイスの設定例については、「設定例」を参照してください。

```
Device-hub> enable
Device-hub# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Device-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Device-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Device-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Device-hub(config)# pfr master
Device-hub(config-pfr-mc)# mc-peer head-end loopback1
Device-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Device-hub(config-pfr-mc)# end
```

PfR ターゲット検出情報の表示

PfR ターゲット検出機能を設定したら、このタスクのコマンドを入力して、ローカルおよびリモートのマスター コントローラ ピア、レスポンド リスト、内部プレフィックス、および SAF ドメイン ID に関する情報を表示します。

手順の概要

1. **enable**
2. **show pfr master target-discovery**
3. **show pfr master active-probes target-discovery**
4. **debug pfr master target-discovery**

手順の詳細

ステップ 1 enable

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

例：

```
Device> enable
```

ステップ 2 show pfr master target-discovery

このコマンドは、PfR マスター コントローラにより監視および制御されるトラフィック クラスに関する情報を表示するときに使用されます。この例では、コマンドはハブ（本社）マスター コントローラで入力され、ローカルおよびリモート ネットワーク、SAF 設定用のドメイン ID、およびマスター コントローラ ピアに関する情報が表示されます。（local）のラベルが付いた出力セクションの情報は、他の MC にアドバタイズされます。（remote）のラベルが付いた出力セクションの情報は、SAF 経由で他の MC から学習されます。

例：

```
Device# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Static Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.11.11.1 Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

MC-peer: 10.18.1.1 Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24

MC-peer: 10.16.1.1 Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

ステップ 3 show pfr master active-probes target-discovery

このコマンドは、ターゲット検出を使用して学習されるすべてのアクティブプローブおよびプローブターゲットのステータスを表示するために使用します。この例では、コマンドはハブ（本社）マスター コン

トローラで入力され、2つのMCピアに関する情報が表示され、プローブのタイプおよびターゲットIPアドレスが一覧表示されます。

例：

```
Device# show pfr master active-probes target-discovery
```

```
PfR Master Controller active-probes (TD)
Border = Border Router running this probe
MC-Peer = Remote MC associated with this target
Type = Probe Type
Target = Target Address
TPort = Target Port
N - Not applicable
```

```
Destination Site Peer Addresses:
```

```
MC-Peer      Targets
10.16.1.1     10.111.1.2, 10.111.1.1
10.18.1.1     10.121.1.1
```

```
The following Probes are running:
```

Border	Idx	State	MC-Peer	Type	Target	TPort
10.16.1.3	27	TD-Actv	10.16.1.1	jitter	10.111.1.2	5000
10.16.1.2	14	TD-Actv	10.16.1.1	jitter	10.111.1.2	5000
10.16.1.3	27	TD-Actv	10.16.1.1	jitter	10.111.1.1	5000
10.16.1.2	14	TD-Actv	10.16.1.1	jitter	10.111.1.1	5000
10.18.1.1	14	TD-Actv	10.18.1.1	jitter	10.121.1.1	5000
10.18.1.1	27	TD-Actv	10.18.1.1	jitter	10.121.1.1	5000

ステップ 4 debug pfr master target-discovery

このコマンドは、問題のトラブルシューティングに役立つデバッグメッセージを表示するために使用します。次の例では、マスター コントローラのピアリング コマンド、**mc-peer** を発行後の PfR メッセージが示されています。MC のピアリングの宛先が変更され、PfR ターゲット検出がシャットダウンされ、再起動されています。

例：

```
Device# debug pfr master target-discovery
```

```
PfR Master Target-Discovery debugging is on
```

```
Device# configure terminal
```

```
Device(config)# pfr master
```

```
Device(config-pfr-mc)# mc-peer description branch office
```

```
*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli chg, op:0/1 idb:0/115967296 ip:0.0.0.0/0.0.0.0
  dom:59501/45000
*Oct 26 20:00:34.084: PFR_MC_TD: mc-peer cli transition, shutting down TD
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown start, mode:4
*Oct 26 20:00:34.084: PFR_MC_TD: SvcUnreg: handle:5
*Oct 26 20:00:34.084: PFR_MC_TD: TD teardown fin, mode:4
*Oct 26 20:00:35.089: PFR_MC_TD: mc-peer cli enabled, starting TD, domain:59501
*Oct 26 20:00:35.089: PFR_MC_TD: TD startup, origin:192.168.3.1 handle:0 dyn_pid:4294967295
*Oct 26 20:00:35.089: PFR_MC_TD: Static mode start <-----
*Oct 26 20:00:35.090: PFR_MC_TD: Static Target list: 10.101.1.2, 10.101.1.1
*Oct 26 20:00:35.090: PFR_MC_TD: Static Prefix list: 10.101.2.0/24, 10.101.1.0/24
*Oct 26 20:00:35.090: PFR_MC_TD: SvcReg: handle:7
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: success 102:1:FFFFFFFF.FFFFFFFFFF.FFFFFFFFFF.FFFFFFFFFF
*Oct 26 20:00:35.093: PFR_MC_TD: SvcSub: handle:7 subscription handle:6
*Oct 26 20:00:35.093: PFR_MC_TD: local data encode, pre-publish
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: success 102:1:0.0.0.C0A80301
```

```
*Oct 26 20:00:35.094: PFR_MC_TD: SvcPub: handle:7 size:336 seq:3 reach via 192.168.3.1
*Oct 26 20:00:35.094: PFR_MC_TD: prereqs met, origin:192.168.3.1 handle:7 sub:6 pub(s:1/r:0)
```

PfR ターゲット検出の設定例

例：ダイナミック モードでのマルチホップ ネットワークの PfR ターゲット検出の設定

次の設定は、本社とブランチ オフィスまたはリモート サイト間のネットワーク クラウドがカスタマーの管理下でない、または SAF 対応でないマルチホップ ネットワークで使用できます。設定例では、3 台のマスター コントローラ（1 台は本社、2 台はブランチ オフィス）が示されています。マスター コントローラのピアリングは 3 台のマスター コントローラ ルータ間に確立されていて、PfR ターゲット検出はダイナミック モードを使用して設定されています。3 つすべてのサイトの **show pfr master target-discovery** コマンドの出力が表示されています。



(注) 次の例では、ハブおよびスポーク デバイスのホスト名は「Router-hub」、「Router-spoke1」、または「Router-spoke2」として設定されていますが、デバイスには PfR をサポートするルーティング機能を備えた任意のデバイスを指定できます。

ハブの MC のピアリングおよびターゲット検出の設定

ハブデバイスにはルーティング機能があり、本社に設置されています。この例では、このデバイスがハブデバイスであることを示すために、マスター コントローラのピアリングが **head-end** キーワードを使用して設定されています。ループバック インターフェイスを指定する必要があります。これは、EIGRP SAF 隣接関係のソースとして使用されます。

```
Router-hub> enable
Router-hub# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end Loopback1
Router-hub(config-pfr-mc)# target-discovery
Router-hub(config-pfr-mc)# end
```

Spoke1 MC のピアリングおよびターゲット検出の設定

spoke1 デバイスにはルーティング機能があり、ニューヨークのブランチ オフィスに設置されています。この例では、マスター コントローラのピアリングがハブ デバイスの IP アドレス（10.11.11.1）とピアリングするように設定されています。

```
Router-spoke1> enable
Router-spoke1# configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke1(config-pfr-mc)# target-discovery
Router-spoke1(config-pfr-mc)# end

```

Spoke2 MC のピアリングおよびターゲット検出の設定

spoke2 デバイスにはルーティング機能があり、マイアミのブランチ オフィスに設置されています。この例では、マスターコントローラのピアリングがハブデバイスのIPアドレス (10.11.11.1) とピアリングするように設定されています。

```

Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.11.11.1 Loopback1
Router-spoke2(config-pfr-mc)# target-discovery
Router-spoke2(config-pfr-mc)# end

```

スタティックモードを使用したPfRターゲット検出の出力例

次の出力は、ダイナミックモードでPfRターゲット検出が設定された後のハブデバイスのものです。

```

Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Dynamic Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.11.11.1 Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

MC-peer: 10.18.1.1 Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24

MC-peer: 10.16.1.1 Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

```

次の出力は、ダイナミックモードでPfRターゲット検出が設定された後のspoke1デバイスのものです。

```

Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Dynamic Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.16.1.1 Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)

```

```
MC-peer: 10.11.11.1          Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24
```

```
MC-peer: 10.18.1.1          Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

次の出力は、ダイナミック モードで PfR ターゲット検出が設定された後の spoke2 デバイスのものです。

```
Router-spoke2# show pfr master target-discovery
```

```
PfR Target-Discovery Services
Mode: Dynamic   Domain: 59501
Responder list: tgt   Inside-prefixes list: ipfx
SvcRtg: client-handle: 3  sub-handle: 2  pub-seq: 1
```

```
PfR Target-Discovery Database (local)
```

```
Local-ID: 10.18.1.1          Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

```
PfR Target-Discovery Database (remote)
```

```
MC-peer: 11.11.11.1          Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24
```

```
MC-peer: 10.16.1.1          Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

例：ダイナミック モードを使用した SAF-Everywhere ネットワークでの PfR ターゲット検出の設定

次の設定例は、PfR MC 間のルーティング可能なデバイスがすべて SAF をサポートするように設定されているネットワークで使用できます。このモデルでは、ハブサイトとブランチサイトは、EIGRP SR フォワーダが設定されておらず、すべてのデバイスが SAF 対応である、ネットワーク（通常はサービスプロバイダー（SP）ネットワーク）によって分離されています。SAF-Everywhere タイプのネットワークを介した MC のピアリングは、隣接ネイバー間の EIGRP ピアリングと同様です。

設定例では、2 台のマスター コントローラ（1 台は本社、1 台はブランチ オフィス）が示されています。マスター コントローラのピアリングは 2 台のマスター コントローラ ルータ間に確立されていて、PfR ターゲット検出は本社とブランチ オフィスでダイナミック モードでイネーブルになっています。



(注) わかりやすくするために、表示されている設定には、コマンドプロンプトはありません。

本社のマスター コントローラの設定

本社（ヘッドエンド）ルータでは、マスター コントローラのピアリングがイネーブルになっており、PfR ターゲット検出はダイナミック モードで設定されています。SAF の設定は **service-family**

コマンドセクションの下に表示されています。この設定は、PfR MC のピアリングおよびターゲット検出オーバーレイの設定が追加される前に存在していると想定されています。

```
key chain metals
  key 1
    key-string gold
!
pfr master
mc-peer
target-discovery
no keepalive
!
border 10.1.1.2 key-chain metals
  interface Ethernet0/2 external
  interface Ethernet0/3 external
  interface Ethernet0/0 internal
  interface Ethernet0/1 internal
!
learn
throughput
periodic-interval 0
monitor-period 1
delay threshold 100
mode route control
mode select-exit best

interface Loopback1
ip address 10.100.100.101 255.255.255.255
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
!
router eigrp
!
  service-family ipv4 autonomous-system 59501
!
  remote-neighbors source Loopback1 unicast-listen
exit-service-family
```

ブランチ オフィスのマスター コントローラの設定

ブランチ オフィス ルータでは、マスター コントローラのピアリングがイネーブルになっており、PfR ターゲット検出はダイナミック モードで設定されています。

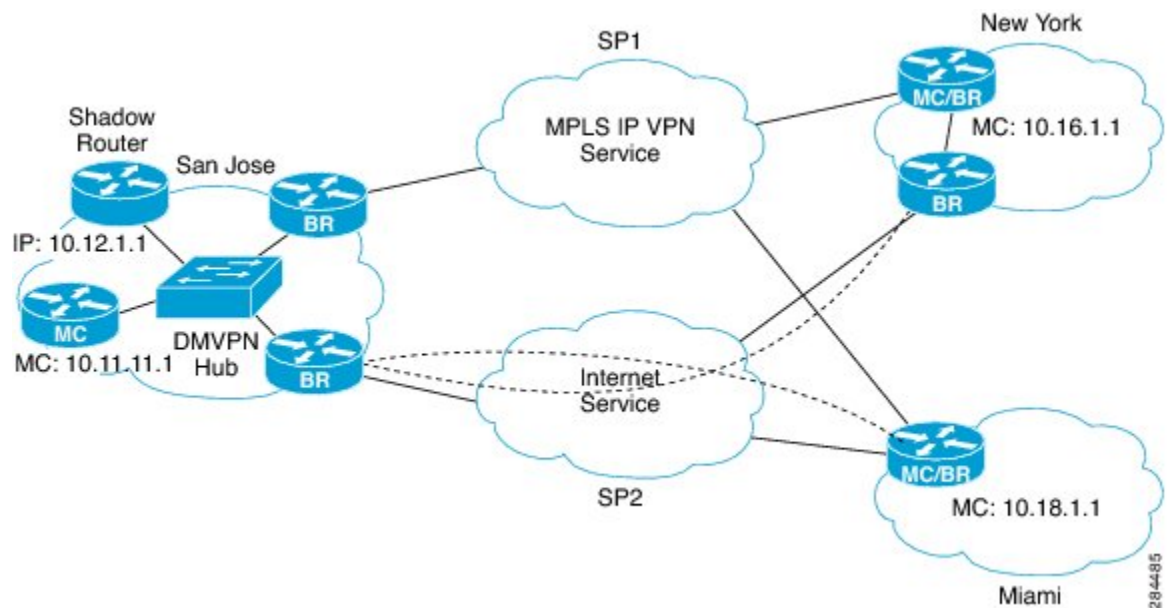
```
key chain metals
  key 1
    key-string gold
!
pfr master
mc-peer
target-discovery
!
border 172.16.1.3 key-chain metals
  interface Ethernet0/0 external
  interface Ethernet0/1 external
  interface Ethernet0/2 internal
  interface Ethernet0/3 internal
!
learn
throughput
periodic-interval 0
monitor-period 1
!
interface Loopback1
ip address 172.16.100.121 255.255.255.255
!
interface Ethernet0/2
ip address 172.16.1.4 255.255.255.0
!
```

```
router eigrp
!
service-family ipv4 autonomous-system 59501
!
neighbor 10.100.100.101 Loopback1 remote 10
exit-service-family
```

例：ターゲットのスタティック定義およびIPプレフィックスの範囲を使用した **PfR** ターゲット検出の設定

次の設定例は、IP SLA Responder および IP プレフィックスの範囲が SAF によってアドバタイズされるように指定する場合に使用できます。この設定は、本社とブランチオフィスまたはリモートサイト間のネットワーククラウドが SAF 対応でないマルチホップネットワークで実行できます。次の図では、シャドウルータはハブサイトとして設定されています。シャドウルータは IP SLA Responder (IP SLA 測定のソース) として使用される専用ルータです。設定例では、3 台のマスターコントローラ (1 台は本社、2 台はブランチオフィス) が示されています。マスターコントローラのピアリングは 3 台のマスターコントローラルータ間に確立されていて、プレフィックスリストが各サイトのローカルレスポンドと内部プレフィックスを特定するために設定されています。3 つすべてのサイトの **show pfr master target-discovery** コマンドの出力が表示されています。

図 4: MPLS IP VPN および DMVPN を使用したシャドウ ルータ ネットワーク トポロジを備えたマルチホップ



ハブの MC のピアリングおよびターゲット検出の設定

ハブ ルータは本社に設置されています。この例では、このルータがハブ ルータであることを示すために、マスターコントローラのピアリングが **head-end** キーワードを使用して設定されています。ループバック インターフェイスを指定する必要があります。これは、EIGRP SAF 隣接関係のソースとして使用されます。

例：ターゲットのスタティック定義および IP プレフィックスの範囲を使用した PfR ターゲット検出の設定



- (注) 次の例では、ハブおよびスポーク デバイスのホスト名は「Router-hub」、「Router-spoke1」、または「Router-spoke2」として設定されていますが、デバイスには PfR をサポートするルーティング機能を備えた任意のデバイスを指定できます。

```
Router-hub> enable
Router-hub# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-hub(config)# ip prefix-list ipfx permit 10.101.1.0/24
Router-hub(config)# ip prefix-list ipfx permit 10.101.2.0/24
Router-hub(config)# ip prefix-list tgt permit 10.101.1.1/32
Router-hub(config)# ip prefix-list tgt permit 10.101.1.2/32
Router-hub(config)# pfr master
Router-hub(config-pfr-mc)# mc-peer head-end loopback1
Router-hub(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-hub(config-pfr-mc)# end
```

Spoke1 MC のピアリングおよびターゲット検出の設定

spoke1 ルータはニューヨークのブランチ オフィスに設置されています。この例では、マスター コントローラのピアリングがシャドウ (ハブ) ルータの IP アドレス (10.12.1.1) とピアリングするように設定されています。

```
Router-spoke1> enable
Router-spoke1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.1.0/24
Router-spoke1(config)# ip prefix-list ipfx permit 10.111.2.0/26
Router-spoke1(config)# ip prefix-list tgt permit 10.111.3.1/32
Router-spoke1(config)# !
Router-spoke1(config)# pfr master
Router-spoke1(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke1(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke1(config-pfr-mc)# end
```

Spoke2 MC のピアリングおよびターゲット検出の設定

spoke2 ルータはマイアミのブランチ オフィスに設置されています。この例では、マスター コントローラのピアリングがシャドウ (ハブ) ルータの IP アドレス (10.12.1.1) とピアリングするように設定されています。

```
Router-spoke2> enable
Router-spoke2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.1.0/24
Router-spoke2(config)# ip prefix-list ipfx permit 10.121.2.0/26
Router-spoke2(config)# ip prefix-list tgt permit 10.121.1.1/32
Router-spoke2(config)# ip prefix-list tgt permit 10.121.2.1/32
Router-spoke2(config)# pfr master
Router-spoke2(config-pfr-mc)# mc-peer 10.12.1.1 loopback1
Router-spoke2(config-pfr-mc)# target-discovery responder-list tgt inside-prefixes ipfx
Router-spoke2(config-pfr-mc)# end
```

スタティック モードを使用した PfR ターゲット検出の出力例

次の出力は、スタティック モードで PfR ターゲット検出が設定された後のハブ ルータのもので

```
Router-hub# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Static Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.12.1.1 Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24

PfR Target-Discovery Database (remote)

MC-peer: 10.18.1.1 Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24

MC-peer: 10.16.1.1 Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

次の出力は、スタティック モードで PfR ターゲット検出が設定された後の spoke1 ルータのもので

```
Router-spoke1# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Static Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.16.1.1 Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24

PfR Target-Discovery Database (remote)

MC-peer: 10.12.1.1 Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24

MC-peer: 10.18.1.1 Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

次の出力は、スタティック モードで PfR ターゲット検出が設定された後の spoke2 ルータのもので

```
Router-spoke2# show pfr master target-discovery

PfR Target-Discovery Services
Mode: Static Domain: 59501
Responder list: tgt Inside-prefixes list: ipfx
SvcRtg: client-handle: 3 sub-handle: 2 pub-seq: 1

PfR Target-Discovery Database (local)

Local-ID: 10.18.1.1 Desc: Router-spoke2
Target-list: 10.121.1.2, 10.121.1.1
Prefix-list: 10.121.2.0/26, 10.121.1.0/24
```

PfR Target-Discovery Database (remote)

```
MC-peer: 10.12.1.1          Desc: Router-hub
Target-list: 10.101.1.2, 10.101.1.1
Prefix-list: 10.101.2.0/24, 10.101.1.0/24

MC-peer: 10.16.1.1          Desc: Router-spoke1
Target-list: 10.111.1.3, 10.111.1.2, 10.111.1.1
Prefix-list: 10.111.3.1/32, 10.111.2.0/26, 10.111.1.0/24
```

その他の関連資料

関連資料

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

MIB

MIB	MIB のリンク
• CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PfR ターゲット検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 1 : PfR ターゲット検出の機能情報

機能名	リリース	機能情報
PfR ターゲット検出 v1.0	Cisco IOS XE Release 3.5S	PfR ターゲット検出機能では、IP SLA Responder の特定および設定を自動化することにより、大企業のブランチ ネットワーク間のビデオおよび音声アプリケーションのパフォーマンスを管理するためのスケーラブルなソリューションが導入されています。 次のコマンドが導入または変更されました。debug pfr master target-discovery、mc-peer、show pfr master active-probes、show pfr master target-discovery、および target-discovery。