パフォーマンス ルーティングを使用した BGP インバウンド最適化

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

機能情報の検索

このモジュールに記載されている機能の一部が、ご使用のソフトウェア リリースでサポートされていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「パフォーマンス ルーティングを使用した BGP インバウンド最適化に関する機能情報」（P.23）を参照してください。

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

マニュアルの内容

パフォーマンス ルーティングを使用した BGP インバウンド最適化の概要

BGP インバウンド最適化

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

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

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

PfR を使用したプレフィクス トラフィック クラスの学習

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

PfR は、次の 2 種類のプレフィクスを自動的に学習できます。

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

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

PfR リンク使用率の測定

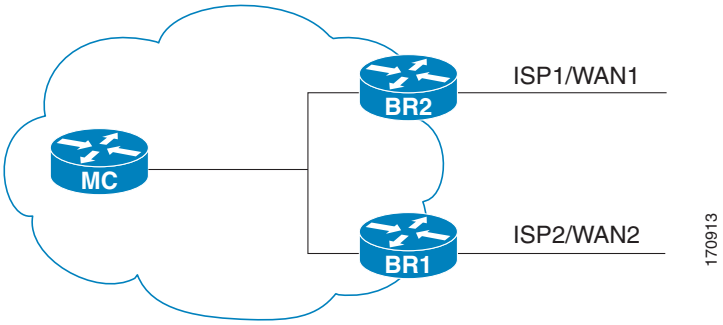
リンク使用率のしきい値

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

リンク使用率範囲

また、PfR では、すべてのリンクに対する使用率の範囲を計算するよう設定することもできます。出力（送信済み）と入力（受信済み）の両方のトラフィック使用率の値がマスター コントローラにレポートされます。図 1 に、個別の ISP 経由でインターネットに接続する出口リンクを持つ 2 つのボーダー ルータを示します。マスター コントローラは、いずれのボーダー ルータのリンク、つまり図 1 の BR1 または BR2 がトラフィック クラスによって使用されているかを判断します。

図 1　　PfR ネットワーク図



PfR 範囲機能は、確実にトラフィックの負荷を分散するために、出口または入口リンクが相互に相対的な使用率の範囲内に収まるよう動作します。範囲は割合で指定されます。この値はマスター コントローラ上で設定され、そのマスター コントローラで管理されているボーダー ルータ上のすべての出口リンクまたは入口リンクに適用されます。たとえば、範囲が 25 % に指定され、BR1（図 1）の出口リンクの使用率が 70 % のとき、BR2（図 1）の出口リンクの使用率が 40 % に低下すると、2 つの出口リンク間のパーセンテージ範囲は 25 % を上回るので、PfR は BR1 の出口リンクを使用するために一部のトラフィック クラスを移動して、トラフィックの負荷を均一にします。BR1（図 1）が入口リンクとして設定されている場合は、使用率の値が送信済みトラフィックではなく受信済みトラフィックに関するものでない限り、出口リンクの場合と同じ方法でリンク使用率範囲が計算されます。

PfR リンク ポリシー

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

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

リンク ポリシーで管理されるパフォーマンス特性は次のとおりです。

- トラフィック負荷（使用率）
- 範囲
- コスト：コスト ポリシーは BGP インバウンド最適化機能によってサポートされません。コスト ポリシーの詳細については、「Configuring Performance Routing Cost Policies」モジュールを参照してください。

トラフィック負荷

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

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

範囲

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

PfR 入口リンク選択の制御テクニック

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

入口リンクの選択を強制的に行うために、PfR は次の方法を提供します。

- 「BGP 自律システム番号のプリペンド」（P.5）
- 「BGP 自律システム番号コミュニティのプリペンド」（P.5）

BGP 自律システム番号のプリペンド

PfR が内部プレフィクスに最適な入口を選択したら、追加の自律システム ホップ（最大 6 個）が他の入口よりも優先的に内部プレフィクスの BGP アドバタイズメントにプリペンドされます。他の入口の追加の自律システム ホップにより、内部プレフィクスに対して最適な入口が使用される可能性が高まります。これは内部プレフィクスを制御するために PfR が使用するデフォルトの方法であり、ユーザ設定は必要ありません。

BGP 自律システム番号コミュニティのプリペンド

PfR が内部プレフィクスに対して最適な入口を選択すると、BGP プリペンド コミュニティがネットワークから ISP などの別の自律システムへの内部プレフィクス BGP アドバタイズメントに添付されます。BGP プリペンド コミュニティは、ISP からピアへの内部プレフィクスのアドバタイズメントで自律システム ホップの数を増加させます。自律システム プリペンド BGP コミュニティは、ローカル ISP が追加の自律システム ホップをフィルタリングする可能性がないため、PfR BGP インバウンド最適化で推奨される方法です。この場合、すべての ISP が BGP プリペンド コミュニティをサポートするわけではないこと、ISP ポリシーが自律システム ホップを無視または変更する場合があること、中継 ISP が自律システム パスをフィルタリングする可能性があることなどいくつかの問題点があります。インバウンドを最適化するこの方法を使用している場合、自律システムを変更するには、**clear ip bgp** コマンドを使用してアウトバウンドの再設定を行う必要があります。

内部プレフィクスに対する PfR マップ操作

PfR マップの操作はルート マップの操作に似ています。PfR マップは、match 句を使用して IP プレフィクス リストまたは PfR 学習ポリシーを選択し、set 句を使用して PfR ポリシー設定を適用するよう設定されます。PfR マップはルートマップと同様にシーケンス番号で設定され、シーケンス番号が最小の PfR マップが最初に評価されます。BGP インバウンド最適化機能では、内部プレフィクスを識別するために **inside** キーワードが **match ip address**（PfR）コマンドに導入されました。

パフォーマンス ルーティングを使用して BGP インバウンド最適化の設定方法

- 「内部プレフィクスを使用したトラフィック クラスの自動学習のための PfR の設定」（P.6）
- 「PfR モニタリングに対して内部プレフィクスを手動で選択」（P.8）

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

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

前提条件

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

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **learn**
5. **inside bgp**
6. **monitor-period** *minutes*
7. **periodic-interval** *minutes*
8. **prefixes** *number*
9. **expire after** {**session** *number* | **time** *minutes*}
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pfr master** **例：** `Router(config)# pfr master`	PfR マスター コントローラ コンフィギュレーション モードを開始して、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**learn** **例：** `Router(config-pfr-mc)# learn`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを開始して、プレフィクス学習ポリシーとタイマーを設定します。
ステップ 5	**inside bgp** **例：** `Router(config-pfr-mc-learn)# inside bgp`	ネットワーク内部のプレフィクスを学習します。
ステップ 6	**monitor-period** *minutes* **例：** `Router(config-pfr-mc-learn)# monitor-period 10`	（任意）PfR マスター コントローラがトラフィック フローを学習する期間を設定します。 • デフォルトの学習期間は 5 分です。 • モニタリング期間の長さは **periodic-interval** コマンドで設定されます。 • 学習するプレフィクスの数は **prefixes** コマンドで設定されます。 • この例では、各モニタリング期間の長さを 10 分に設定します。
ステップ 7	**periodic-interval** *minutes* **例：** `Router(config-pfr-mc-learn)# periodic-interval 20`	（任意）プレフィクス学習期間の間隔を設定します。 • デフォルトでは、プレフィクス学習期間の間隔は 120 分です。 • この例では、モニタリング期間の間隔を 20 分に設定します。
ステップ 8	**prefixes** *number* **例：** `Router(config-pfr-mc-learn)# prefixes 30`	（任意）モニタリング期間中にマスター コントローラが学習するプレフィクスの数を設定します。 • デフォルトでは、上位 100 のトラフィック フローが学習されます。 • この例では、マスター コントローラがモニタリング期間中に 30 個のプレフィクスを学習するよう設定します。 **（注）** モニタリング期間中に学習可能な内部プレフィクスの最大数は 30 です。

	コマンドまたはアクション	目的
ステップ 9	**expire after** {**session** *number* | **time** *minutes*} **例：** `Router(config-pfr-mc-learn)# expire after session 100`	（任意）学習されたプレフィクスが中央ポリシー データベース内に保持される期間を設定します。 • **session** キーワードは、指定された数のモニタリング期間が経過した後に、学習されたプレフィクスが削除されるように設定します。 • **time** キーワードは、指定された期間の経過後に、学習されたプレフィクスが削除されるように設定します。時間の値は分単位で入力されます。 • この例では、100 回のモニタリング期間経過後に、学習されたプレフィクスを削除するよう設定します。
ステップ 10	**end** **例：** `Router(config-pfr-mc-learn)# end`	PfR Top Talker/Top Delay 学習コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

PfR モニタリングに対して内部プレフィクスを手動で選択

PfR BGP インバウンド最適化機能は、自律システム内部プレフィクス宛ての自律システム外部のプレフィクスから送信されたトラフィックに対する最適な入口の選択をサポートするようになりました。このタスクを実行して内部プレフィクスまたはプレフィクス範囲を定義する IP プレフィクス リストを作成することにより、PfR モニタリングに対して内部プレフィクスを手動で選択します。次に、プレフィクス リストは、PfR マップで match 句を設定することにより Monitored Traffic Class（MTC）リストにインポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **oer-map** *map-name sequence-number*
5. **match ip address prefix-list** *name* [**inside**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*] **例：** `Router(config)# ip prefix-list INSIDE_PREFIXES seq 20 permit 192.168.1.0/24`	プレフィクス リストを作成し、モニタリングのためにプレフィクスを手動で選択します。 • マスター コントローラは、デフォルト ルートを含む任意の長さの、完全に一致するプレフィクスを監視し、制御できます。マスター コントローラは設定されたプレフィクスでだけ動作します。 • マスター コントローラは、le 32 オプションを使用して包含プレフィクスを監視および制御できます。マスター コントローラは設定されたプレフィクスで動作し、RIB 内の特定のプレフィクスが同じ出口を使用するよう強制します。 **（注）** このオプションは慎重に適用する必要があります。これは一般的な導入では必要ありません。 • 例では、PfR が 192.168.1.0/24 の特定のプレフィクスを監視および制御するために IP プレフィクス リストを作成します。
ステップ 4	**pfr-map map-name** *sequence-number* **例：** `Router(config)# pfr-map INSIDE_MAP 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを作成または設定します。 • PfR マップの操作はルート マップの操作に似ています。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • パフォーマンスを最大化するために、共通シーケンスおよび拒否シーケンスは最小の PfR マップ シーケンスに適用する必要があります。 • 例では、INSIDE_MAP という名前の PfR マップを作成します。

	コマンドまたはアクション	目的
ステップ 5	**match ip address prefix-list** *name* [**inside**] **例：** `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	PfR ポリシーを適用するプレフィクス リスト match 句エントリを PfR マップで作成します。 • このコマンドは IP プレフィクス リストだけをサポートします。 • **inside** キーワードを使用して内部プレフィクスを識別します。 • 例では、match 句を作成し、プレフィクス リスト INSIDE_PREFIXES を使用して内部プレフィクスが一致するよう指定します。
ステップ 6	**end** **例：** `Router(config-pfr-map)# end`	PfR マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インバウンド トラフィックに対する PfR リンク使用率の変更

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

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pfr master** **例：** `Router(config)# pfr master`	PfR マスター コントローラ コンフィギュレーション モードを開始して、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**border** *ip-address* [**key-chain** *key-chain-name*] **例：** `Router(config-pfr-mc)# border 10.1.1.2`	PfR 管理ボーダー ルータ コンフィギュレーション モードを開始して、ボーダー ルータとの通信を確立します。 • ボーダー ルータを識別するために、IP アドレスを設定します。 • PfR 管理のネットワークを作成するには、少なくとも 1 つのボーダー ルータを指定する必要があります。1 台のマスター コントローラで制御できるボーダー ルータは、最大 10 台です。 **（注）** ボーダー ルータが最初に設定されている場合は、**key-chain** キーワードおよび *key-chain-name* 引数を入力する必要があります。ただし、既存のボーダー ルータを再設定する場合、このキーワードは省略可能です。
ステップ 5	**interface** *type number* **external** **例：** `Router(config-pfr-mc-br)# interface Ethernet 1/0 external`	PfR 管理の外部インターフェイスとしてボーダー ルータを設定し、PfR ボーダー出口インターフェイス コンフィギュレーション モードを開始します。 • 外部インターフェイスは、トラフィックの転送およびアクティブ モニタリングに使用されます。 • PfR 管理のネットワークには、最低 2 つの外部ボーダー ルータ インターフェイスが必要です。各ボーダー ルータでは、少なくとも 1 つの外部インターフェイスを設定する必要があります。1 台のマスター コントローラで制御できる外部インターフェイスは、最大 20 です。 **（注）** **external** キーワードまたは **internal** キーワードを指定せずに **interface** コマンドを入力すると、ルータは、PfR ボーダー出口コンフィギュレーション モードではなく、グローバル コンフィギュレーション モードで開始されます。アクティブ インターフェイスがルータ設定から削除されないように、このコマンドの **no** 形式は慎重に適用してください。

	コマンドまたはアクション	目的
ステップ 6	**maximum utilization receive** {**absolute** *kbps* | **percent** *percentage*} **例：** `Router(config-pfr-mc-br-if)# maximum utilization receive percent 90`	設定された PfR 管理リンク インターフェイスに対して最大受信使用率のしきい値を設定します。 • **absolute** キーワードと *kbps* 引数を使用してすべての入口リンクのスループットの絶対しきい値を 1 秒あたりのキロバイト数（kbps）で指定します。 • **percent** キーワードと *percentage* 引数を使用してすべての入口リンクで受信される帯域幅の割合として最大使用率しきい値を指定します。 • この例では、ボーダー ルータのこの入口リンクに対するインバウンド トラフィックの最大使用率しきい値を 90% 以下に指定する必要があります。
ステップ 7	**end** **例：** `Router(config-pfr-mc-br-if)# end`	PfR ボーダー出口インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PfR 入口リンク使用率範囲の変更

マスター コントローラでこのタスクを実行し、すべてのボーダー ルータに対する最大入口リンク使用率範囲を変更します。デフォルトでは、PfR はボーダー ルータ上の外部リンクの使用率を 20 秒ごとに自動監視し、ボーダー ルータがマスター コントローラに使用率を報告します。BGP インバウンド最適化機能では、インバウンド トラフィック使用率をマスター コントローラに報告し、入口リンクのリンク使用率範囲を指定できるようになりました。

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

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

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **max range receive percent** *percentage*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pfr master** **例：** `Router(config)# pfr master`	PfR マスター コントローラ コンフィギュレーション モードを開始して、マスター コントローラとしてルータを設定し、グローバル処理およびポリシーを設定します。
ステップ 4	**max range receive percent** *percentage* **例：** `Router(config-pfr-mc)# max range receive percent 20`	ボーダー ルータにあるすべての入口リンク間の受信使用率範囲の上限を指定します。 • **percent** キーワードと *percentage* 引数は範囲の割合を指定するために使用されます。 • この例では、ボーダー ルータにあるすべての入口リンク間の受信使用率範囲は 20% 以内である必要があります。
ステップ 5	**end** **例：** `Router(config-pfr-mc)# end`	PfR マスター コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

学習された内部プレフィクスに対する PfR ポリシーの設定および適用

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

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

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match pfr learn** {**delay** | **inside** | **throughput**}
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}

7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pfr-map** *map-name sequence-number* **例：** `Router(config)# pfr-map INSIDE_LEARN 10`	PfR マップ コンフィギュレーション モードを開始して、選択した IP プレフィクスにポリシーを適用するように PfR マップを設定します。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • deny シーケンスは、最初に IP プレフィクス リストに定義してから、**match** コマンドを使用して適用します。 • 例では、INSIDE_LEARN という名前の PfR マップを作成します。
ステップ 4	**match pfr learn** {**delay** | **inside** | **throughput**} **例：** `Router(config-pfr-map)# match pfr learn inside`	PfR 学習プレフィクスに一致する match 句エントリを PfR マップで作成します。 • プレフィクスは内部プレフィクスであるプレフィクスを学習したり、最小の遅延または最大のアウトバウンド スループットに基づいてプレフィクスを学習したりするよう設定できます。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • 例では、内部プレフィクスを使用して学習されたトラフィックに一致する match 句エントリを作成します。

	コマンドまたはアクション	目的
ステップ 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set delay threshold 2000`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 2000 ミリ秒に設定する set 句が設定されます。
ステップ 6	**set loss** {**relative** *average* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set loss relative 20`	マスター コントローラが出口リンクに対して許容する相対または最大パケット損失制限を設定する set 句エントリを作成します。 • PfR マップを設定して、出口リンクでの送信中に PfR が許可するパケット損失の相対割合または最大数を指定するには、このコマンドを使用します。パケット損失がユーザ定義またはデフォルトの値を超えると、マスター コントローラはその出口リンクをポリシー違反であると判断します。 • **relative** キーワードは、相対パケット損失割合を設定するために使用されます。相対パケット損失割合は、短期的なパケット損失と長期的なパケット損失の比較に基づきます。 • **threshold** キーワードは、絶対最大パケット損失を設定するために使用されます。最大値は、百万パケットに対して実際に損失したパケットの数に基づきます。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックに対して許容できるパケット損失の相対割合を 20% に設定する set 句を作成します。

	コマンドまたはアクション	目的
ステップ 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set unreachable relative 10`	到達不能ホストの最大数を設定する set 句エントリを作成します。 • このコマンドは、PfR がトラフィック エントリに許可する到達不能ホストの相対割合または最大数（100 万フローあたりのフロー数（fpm））を指定するために使用します。到達不能ホストの絶対数または相対割合がユーザ定義の値またはデフォルト値を超える場合、PfR はトラフィック クラス エントリが OOP であると判断し、代替出口リンクを検索します。 • 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。到達不能ホストの相対割合は、短期測定値および長期測定値の比較に基づいています。 • 到達不能ホストの絶対最大数を fpm に基づいて設定するには **threshold** キーワードを使用します。 • 例では、最大の遅延に基づいて学習されたトラフィックに対して到達不能ホストの相対割合が 10% 以上である場合に、トラフィック クラス エントリの新しい出口リンクを検索するようマスター コントローラを設定する set 句エントリを作成します。
ステップ 8	**end** **例：** `Router(config-pfr-map)# end`	（任意）PfR マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

設定された内部プレフィクスに対する PfR ポリシーの設定および適用

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

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

手順の概要

1. **enable**
2. **configure terminal**
3. **pfr-map** *map-name sequence-number*
4. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name* [**inside**]}
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}

6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | threshold *maximum*}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pfr-map map-name** *sequence-number* **例：** `Router(config)# pfr-map INSIDE_CONFIGURE 10`	PfR マップ コンフィギュレーション モードを開始して、PfR マップを作成または設定します。 • PfR マップの操作はルート マップの操作に似ています。 • 各 PfR マップ シーケンスには、match 句を 1 つだけ設定できます。 • パフォーマンスを最大化するために、共通シーケンスおよび拒否シーケンスは最小の pfr マップ シーケンスに適用する必要があります。 • 例では、INSIDE_CONFIGURE という名前の PfR マップを作成します。
ステップ 4	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name* [**inside**] **例：** `Router(config-pfr-map)# match ip address prefix-list INSIDE_PREFIXES inside`	PfR マップ内の一致基準として拡張 IP アクセス リストまたは IP プレフィクス リストを参照します。 • **inside** キーワードを使用して、自律システム内部プレフィクス宛ての自律システム外部のプレフィクスから送信されたトラフィックに対する最適な入口の選択をサポートする PfR BGP インバウンド最適化をサポートする内部プレフィクスを指定します。 • 例では、内部プレフィクスを指定するプレフィクス リスト INSIDE_PREFIXES を使用して match 句エントリを作成しています。

	コマンドまたはアクション	目的
ステップ 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set delay threshold 2000`	set 句エントリを作成して、遅延しきい値を設定します。 • 遅延しきい値は、相対割合または一致基準の絶対値として設定できます。 • 相対遅延割合を設定するには **relative** キーワードを使用します。相対遅延割合は、短期測定値および長期測定値の比較に基づいています。 • 絶対最大遅延期間をミリ秒単位で設定するには **threshold** キーワードを使用します。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックの絶対最大遅延しきい値を 2000 ミリ秒に設定する set 句が設定されます。
ステップ 6	**set loss** {**relative** *average* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set loss relative 20`	マスター コントローラが出口リンクに対して許容する相対または最大パケット損失制限を設定する set 句エントリを作成します。 • PfR マップを設定して、出口リンクでの送信中に PfR が許可するパケット損失の相対割合または最大数を指定するには、このコマンドを使用します。パケット損失がユーザ定義またはデフォルトの値を超えると、マスター コントローラはその出口リンクをポリシー違反であると判断します。 • **relative** キーワードは、相対パケット損失割合を設定するために使用されます。相対パケット損失割合は、短期的なパケット損失と長期的なパケット損失の比較に基づきます。 • **threshold** キーワードは、絶対最大パケット損失を設定するために使用されます。最大値は、百万パケットに対して実際に損失したパケットの数に基づきます。 • 例では、同じ PfR マップ シーケンスで一致するトラフィックに対して許容できるパケット損失の相対割合を 20% に設定する set 句を作成します。

	コマンドまたはアクション	目的
ステップ 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **例：** `Router(config-pfr-map)# set unreachable relative 10`	到達不能ホストの最大数を設定する set 句エントリを作成します。 • このコマンドは、PfR がトラフィック エントリに許可する到達不能ホストの相対割合または最大数（100 万フローあたりのフロー数（fpm））を指定するために使用します。到達不能ホストの絶対数または相対割合がユーザ定義の値またはデフォルト値を超える場合、PfR はトラフィック クラス エントリが OOP であると判断し、代替出口リンクを検索します。 • 到達不能ホストの相対割合を設定するには **relative** キーワードを使用します。到達不能ホストの相対割合は、短期測定値および長期測定値の比較に基づいています。 • 到達不能ホストの絶対最大数を fpm に基づいて設定するには **threshold** キーワードを使用します。 • 例では、最大の遅延に基づいて学習されたトラフィックに対して到達不能ホストの相対割合が 10% 以上である場合に、トラフィック クラス エントリの新しい出口リンクを検索するようマスター コントローラを設定する set 句エントリを作成します。
ステップ 8	**end** **例：** `Router(config-pfr-map)# end`	PfR マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

パフォーマンス ルーティングを使用した BGP インバウンド最適化の設定例

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

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

```
Router> enable
Router# configure terminal
Router(config)# pfr master
Router(config-pfr-mc)# learn
Router(config-pfr-mc-learn)# inside bgp
Router(config-pfr-mc-learn)# monitor-period 10
Router(config-pfr-mc-learn)# periodic-interval 20
Router(config-pfr-mc-learn)# prefixes 30
Router(config-pfr-mc-learn)# end
```

例：PfR モニタリングに対して内部プレフィクスを手動で選択

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

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

例：インバウンド トラフィックに対する PfR リンク使用率の変更

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

```
Router(config)# pfr master
Router(config-pfr-mc)# border 10.1.2.1
Router(config-pfr-mc-br)# interface Ethernet 1/0 external
Router(config-pfr-mc-br-if)# maximum receive utilization percentage 65
Router(config-pfr-mc-br-if)# end
```

例：PfR 入口リンク使用率範囲の変更

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

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

例：学習された内部プレフィクスに対する PfR ポリシーの設定および適用

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

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

例：設定された内部プレフィクスに対する PfR ポリシーの設定および適用

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

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

参考資料

関連資料

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

シスコのテクニカル サポート

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

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

表 1 に、この機能のリリース履歴を示します。

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

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　パフォーマンス ルーティングを使用した BGP インバウンド最適化に関する機能情報

機能名	リリース	機能情報
OER BGP インバウンド最適化	12.4(9)T 12.2(33)SRB	PfR BGP インバウンド最適化は、自律システム内部プレフィクス宛ての自律システム外部のプレフィクスから送信されたトラフィックに対する最適な入口選択をサポートします。自律システムからインターネット サービス プロバイダー（ISP）への外部 EGP（eBGP）アドバタイズメントにより、ネットワークに入るトラフィックの入口パスが影響を受けることがあります。PfR では、eBGP アドバタイズメントを使用して最適な入口選択を行います。 この機能により、次のコマンドが導入または変更されました。**clear pfr master prefix**、**downgrade bgp（PfR）**、**inside bgp（PfR）**、**match ip address（PfR）**、**match pfr learn**、**max range receive（PfR）**、**maximum utilization receive（PfR）**、**show pfr master prefix**。
expire after コマンド[1]	12.3(14)T 12.2(33)SRB	**expire after（PfR）** コマンドは、学習済みプレフィクスの有効期間の設定に使用します。デフォルトでは、マスター コントローラは、中央ポリシー データベースから非アクティブなプレフィクスを削除します。これは、メモリが必要とされるためです。このコマンドを使用すると、制限に基づいて時間またはセッションを設定することによって、この動作を改良できます。時間ベースの制限は、分単位で設定します。セッション ベースの制限は、監視期間数（またはセッション数）に対して設定します。

1. これは、マイナーな機能拡張です。マイナーな機能拡張は、通常、Feature Navigator には表示されません。