NAT を使用したパフォーマンス ルーティング

Performance Routing（PfR; パフォーマンス ルーティング）は、Network Address Translation（NAT; ネットワーク アドレス変換）を使用するネットワークでスタティック ルーティングによりトラフィック クラス ルーティングを制御できるようになりました。また、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 機能が同じルータで設定されていて、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数の Internet Service Provider（ISP; インターネット サービス プロバイダー）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのために Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト リバース パス転送）フィルタリングを使用する場合に発生します。

新しいキーワードが設定されている場合、新しい NAT 変換に、PfR がパケットに選択したインターフェイスのソース IP アドレスが提供され、PfR は、この NAT 変換が作成されたときのインターフェイスを介して、既存のフローを強制的にルーティングします。

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。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「NAT を使用したパフォーマンス ルーティングの機能情報」（P.10）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

NAT を使用したパフォーマンス ルーティングの制約事項

Cisco Catalyst 6500 Switch プラットフォームでは、NAT が PfR 管理のネットワークで設定されている場合、フロー マスク競合が発生します。フロー マスク競合要件により、トラフィックがソフトウェアでスイッチングされます。この競合を解決するには、次の NAT 設定を追加します。

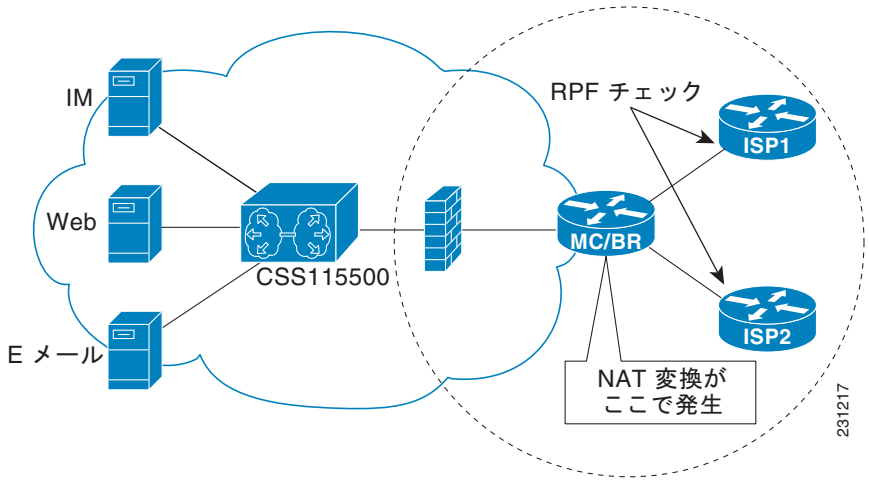
```
mls ip nat netflow-frag-l4-zero
```

NAT を使用したパフォーマンス ルーティングの概要

PfR および NAT

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数の Internet Service Provider（ISP; インターネット サービス プロバイダー）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御するときに、1 つ以上の ISP がセキュリティのために Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト リバース パス転送）フィルタリングを使用する場合に発生します。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 変換が実行された後で PfR によりトラフィック クラスの発信パケット ルートの出口インターフェイスが変更されると、ユニキャスト RPF を実行する入口ルータでパケットがドロップされます。パケットが転送されると、入口ルータ（たとえば、ISP ルータ）のユニキャスト RPF フィルタリングは、NAT により割り当てられるソース IP アドレス プールとは異なるソース IP アドレスを示し、パケットがドロップされます。たとえば、図 1 に、NAT を使用した PfR の機能を示します。

図 1　NAT を使用した PfR



NAT 変換は、内部ネットワークに接続されているルータで発生します。このルータには、ボーダー ルータまたはマスター コントローラとボーダー ルータの組み合わせを使用できます。PfR が、ルートを変更してトラフィック 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と、インターフェイスを介して ISP1 にルーティングされた、図 1 のボーダー ルータからのトラフィックは、トラフィック パフォーマンスが測定され、ポリシーしきい値が適用された後で、インターフェイスを介して ISP2 に再ルーティングされることがあります。RPF チェックは ISP ルータで発生し、ISP2 を介してルーティングされるパケットは、ISP2 の入口ルータでの RPF チェックに失敗します。これは、送信元インターフェイスの IP アドレスが変更されたためです。

このソリューションでは、**ip nat inside source** コマンドに追加された新しいキーワード **pfr** で設定を最小限変更します。**pfr** キーワードが設定されている場合、新しい NAT 変換に、PfR がパケットに選択したインターフェイスのソース IP アドレスが提供され、PfR は、この NAT 変換が作成されたときのインターフェイスを介して、既存のフローを強制的にルーティングします。たとえば、PfR は、図 1 で ISP1 の InterfaceA と ISP2 の InterfaceB の 2 つのインターフェイスがあるボーダー ルータでトラフィックを管理するように設定されます。PfR は、最初に、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ます。このトラフィックの NAT 変換は、InterfaceA に設定されているパケットのソース IP アドレスにすでに存在します。PfR は、トラフィック パフォーマンスを測定して、InterfaceB が現在トラフィック フローに最適な出口であると判断しますが、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 クラスを学習および測定するように設定され、E メール トラフィックが開始されると、NAT 変換が InterfaceB で発生します。PfR スタティック ルーティング NAT ソリューションは、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。NAT、および Cisco IOS ソフトウェアを実行しない PIX ファイアウォールなどのデバイスを使用したネットワーク設定はサポートされていません。

PfR スタティック ルーティング NAT ソリューションの詳細については、「NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する」（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 では、未登録の IP アドレスを使用するプライベート IP インターネットワークがインターネットに接続できます。NAT は、ルータ（通常、2 つのネットワークを接続）で機能し、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（グローバルに一意ではない）アド

レスを有効なアドレスに変換します。NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設定できます。この機能により、そのアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT は、エンタープライズ エッジでも使用され、内部ユーザのインターネットへのアクセスを許可し、メール サーバなど内部デバイスへのインターネット アクセスを許可します。

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

ルータで多くのローカル アドレスに 1 つのグローバル アドレスを使用できるようにすることで、内部グローバル アドレス プールのアドレスを節約できます。このオーバーロードが設定されている場合、ルータは、より高いレベルのプロトコルから十分な情報（たとえば、TCP または UDP ポート番号）を保持して、グローバル アドレスを正しいローカル アドレスに戻します。複数のローカル アドレスが 1 つのグローバル アドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカル アドレスが区別されます。

NAT を使用したパフォーマンス ルーティングの設定方法

- 「NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する」（P.4）

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する

NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定するには、次のタスクを実行します。このタスクを行うと、内部ユーザによりインターネットへのアクセスを許可しつつ、PfR がトラフィック クラスを最適化できるようになります。

Cisco IOS PfR および NAT 機能が同じルータで設定され、PfR がスタティック ルーティングを使用してトラフィック クラスのルーティングを制御する場合、アプリケーションによっては、ドロップされるパケットにより操作が失敗することがあります。このパケット ドロップは、スタティック ルーティングが同じルータからの複数の Internet Service Provider（ISP; インターネット サービス プロバイダー）の接続に使用されている状況で、PfR がスタティック ルーティングを使用してトラフィック クラス ルーティングを制御し、1 つ以上の ISP がセキュリティのために Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト リバース パス転送）フィルタリングを使用する場合に発生します。

このタスクでは、**pfr** キーワードが **ip nat inside source** コマンドで使用されます。**pfr** キーワードが設定されている場合、新しい NAT 変換に、PfR がパケットに選択したインターフェイスのソース IP アドレスが提供され、PfR は、この NAT 変換が作成されたインターフェイスを介して、既存のフローを強制的にルーティングします。このタスクでは、1 つの IP アドレスを使用していますが、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 プールの設定例については、「NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する」（P.4）を参照してください。

（注） PfR スタティック ルーティング NAT ソリューションは、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

NAT の設定の詳細については、『*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. 必要に応じて、ステップ 4 ～ステップ 7 を繰り返して、以降のルート マップ設定を行います。
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*] [**pfr**]
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	**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	**access-list** *access-list-number* {**permit** | **deny**} *ip-address* mask **例：** `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	変換する IP アドレスを許可する標準のアクセス リストを定義します。 • アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセス リストの最後には暗黙的な「deny all」があるので注意してください）。アクセス リストでアドレスを許可しすぎると、予期しない結果になる可能性があります。
ステップ 4	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **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 モードを開始して、ルート マップを設定します。 • 例では、BGP という名前のルート マップを作成します。
ステップ 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **例：** `Router(config-route-map)# match ip address access-list 1`	NAT により変換されるトラフィックを識別するアクセス リストまたはプレフィクス リスト match 句エントリをルート マップに作成します。 • 例では、ステップ 3 で作成した、一致条件として 10.1.0.0 0.0.255.255 プレフィクスを指定するアクセス リストを参照します。
ステップ 6	**match interface** *interface-type interface-number* [*...interface-type interface-number*] **例：** `Router(config-route-map)# match interface serial 1/0`	ルート マップに match 句を作成して、指定されたいずれかのインターフェイスに一致するルートを分散します。 • 例では、match 句を作成して、ステップ 5 の match 句をシリアル インターフェイス 1/0 経由で通過するルートを配布します。
ステップ 7	**exit** **例：** `Router(config-route-map)# exit`	ルート マップ インターフェイス コンフィギュレーション モードを終了して、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	必要に応じて、ステップ 4 ～ステップ 7 を繰り返して、以降のルート マップ設定を行います。	—
ステップ 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*] [**pfr**] **例：** `Router(config)# ip nat inside source interface FastEthernet1/0 overload pfr`	インターフェイスを指定して、オーバーロードでのダイナミックな送信元変換を確立します。 • インターフェイスを指定するには、**interface** キーワードと、type および number 引数を使用します。 • PfR が NAT とともに稼動し、スタティック ルーティングを使用してトラフィック クラス ルーティングを制御できるようにするには、**pfr** キーワードを使用します。
ステップ 10	**interface** *type number* **例：** `Router(config)# interface FastEthernet1/0`	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。

	コマンドまたはアクション	目的
ステップ 11	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.114.11.8 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat inside** **例：** `Router(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 13	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	別のインターフェイスを指定して、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	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 172.17.233.208 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 16	**ip nat outside** **例：** `Router(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 17	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NAT を使用したパフォーマンス ルーティングの設定例

- 「例：NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する」（P.7）

例：NAT を使用するネットワークでスタティック ルーティングによりトラフィックを制御するように PfR を設定する

次に、NAT を使用するネットワークで PfR がスタティック ルーティングにより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例を示します。この例では、NAT 変換の IP アドレスのプールを使用する方法を示します。

図 2　PfR および NAT ネットワークの図

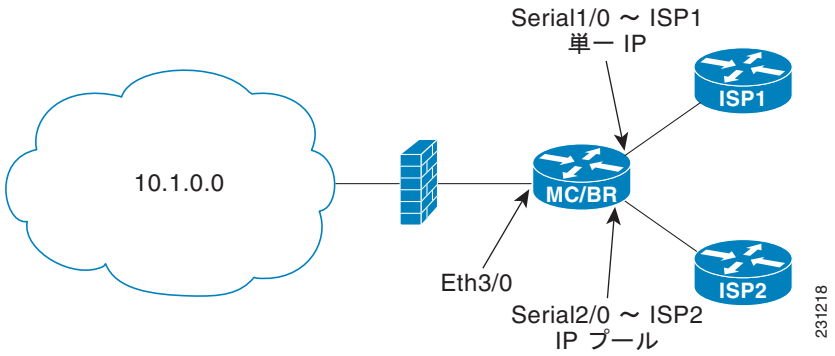


図 2 では、2 種類の ISP を介してインターネットに接続されるマスター コントローラとボーダー ルータの組み合わせが使用されています。次の設定では、PfR は、内部ユーザのインターネットへのアクセスを許可しつつ、トラフィック クラスを最適化できます。この例では、NAT を使用して変換されるトラフィック クラスは、アクセス リストおよびルート マップを使用して指定されます。次に、NAT 変換で IP アドレスのプールを使用するように設定されます。また、**pfr** キーワードが **ip nat inside source** コマンドに追加され、既存のトラフィック クラスが NAT により変換された送信元アドレスであるインターフェイスを経由するように PfR を設定します。新しい NAT 変換には、PfR がパケットに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、シングル ボックス ソリューションであるため、NAT を使用し PfR で管理される複数のルータでのインターフェイスの設定はサポートされていません。

```
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 pfr
Router(config)# interface FastEthernet 3/0
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
```

次の作業

他のパフォーマンス ルーティング機能の詳細または一般的な概念に関する資料については、「関連資料」（P.9）に記載の資料を参照してください。

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco PfR コマンド（コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例）	『*Cisco IOS Performance Routing Command Reference*』
ベーシック PfR 設定	「Configuring Basic Performance Routing」モジュール
アドバンスド PfR の設定	「Configuring Advanced Performance Routing」モジュール
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
NAT に関する一般的な情報	「Configuring NAT for IP Address Conservation」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

NAT を使用したパフォーマンス 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。

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　NAT を使用したパフォーマンス 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[1]	12.3(14)T 12.2(33)SRB	NAT を使用するネットワークでスタティック ルーティングを使用してトラフィック クラス ルーティングを制御するように PfR を許可できます。 **ip nat inside source** コマンドが、この機能によって変更されました。

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。