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

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。

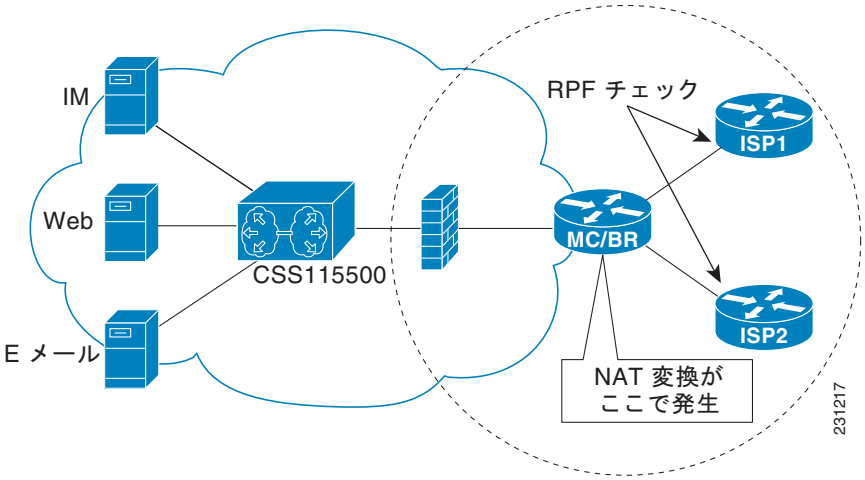
NAT を使用するパフォーマンス ルーティングについて

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

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を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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。 • 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。
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、ルート マップを設定します。 • この例では、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`	アクセス リストまたはプレフィクス リストの match 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。 • この例では、match 条件として 10.1.0.0 0.0.255.255 を指定する、ステップ 3 で作成したアクセス 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`	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 match 句を作成します。 • この例では、シリアル インターフェイス 1/0 を介してステップ 5 の match 句に合格するルートを配布する match 句を作成します。
ステップ 7	**exit** **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、必要に応じてステップ 4 からステップ 7 を繰り返します。	—
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*] [**oer**] **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。 • **interface** 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。 • **oer** 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。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* **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	**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	**ip nat inside** **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	**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、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 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	**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	**ip nat outside** **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	**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、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	『*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 リリースでの基本的な PfR 設定	『Configuring Basic Performance Routing』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	『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
NAT に関する一般情報	『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　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[1]	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 **ip nat inside source** 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。