



## Policy-Based Routing (PBR)

---

- 「PBR の前提条件」 (P.33-1)
- 「PBR の制約事項」 (P.33-1)
- 「PBR について」 (P.33-2)
- 「PBR のデフォルト設定」 (P.33-3)
- 「PBR の設定方法」 (P.33-3)
- 「PBR の設定例」 (P.33-7)



(注)

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

[http://www.cisco.com/en/US/products/ps11846/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html)

- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。



**ヒント** Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

技術マニュアルのアイデア フォーラムに参加する

### PBR の前提条件

なし。

### PBR の制約事項

PFC および DFC では、次がハードウェアでサポートされます。

- 次の IPv4 PBR コマンド：
  - `match ip address`

- **match length**
  - **set ip next-hop** (2,000 インスタンス)
  - **set ip default next-hop**
  - **set interface null0**
  - **set default interface null0**
  - **set ip vrf**
  - **set ip default vrf**
- RP のアドレスが PBR ACL の範囲内にある場合、RP にアドレス指定されたトラフィックは RP に転送されずに、ハードウェアでポリシー ルーティングされます。RP にアドレス指定されたトラフィックのポリシー ルーティングを防止するには、RP にアドレス指定されたトラフィックを拒否するように PBR ACL を設定します。
  - ローカル PBR。
  - ロード バランシングによる IPv4 PBR 再帰ネクスト ホップ。
  - IPv6 PBR はソフトウェアでサポートされます。
  - IPv6 PBR 再帰ネクスト ホップはサポートされません。

## PBR について

- 「PBR の概要」(P.33-2)
- 「IPv4 トラフィックの PBR 再帰ネクスト ホップ」(P.33-3)

## PBR の概要

PBR は、ルーティング プロトコルの代替手段であり、ユニキャスト トラフィック フローのポリシーを設定できます。これによって、ルーティングに対して、ルーティング プロトコルよりも強化した制御を実施し、インターフェイス レベルのトラフィック分類設定の必要を避けられます。PBR は、ルーティング プロトコルが使用するのとは異なるパスにユニキャスト トラフィックをルーティングできます。PBR は次を提供します。

- 同等アクセス
- プロトコル別のルーティング
- 送信元別のルーティング
- 双方向対パッチ トラフィックに基づくルーティング
- 専用リンクに基づくルーティング

PBR ルート マップは、次のように設定できます。

- 特定のエンド システムのアイデンティティ、アプリケーション プロトコル、またはパケットのサイズ、あるいはこれらの値の組み合わせに基づいて、パスを許可または拒否する。
- 拡張アクセス リスト基準に基づいてトラフィックを分類する。
- IP precedence ビット設定する。
- 特定のパスにパケットをルーティングする。

PBR は、PBR 対応インターフェイスで受信されるすべての入力ユニキャスト トラフィックにルートマップを適用します。PBR は、出力トラフィックまたはマルチキャスト トラフィックに適用できません。

入力ユニキャスト トラフィックがルート マップ ステートメントと一致しない場合、ルート マップは、設定済みのすべての `set` 句を適用します。ルーティング プロトコルは、ルート マップの `deny` ステートメントと一致するトラフィックおよびルート マップの `permit` ステートメントと一致しないトラフィックを転送します。

## IPv4 トラフィックの PBR 再帰ネクスト ホップ

PBR 再帰ネクスト ホップ機能は、PBR ルート マップの再帰ネクスト ホップ アドレスの設定をイネーブルにします。再帰ネクストホップ アドレスはルーティング テーブルにインストールされ、直接接続されていないサブネットにすることができます。再帰ネクストホップ アドレスを使用できない場合、トラフィックはデフォルト ルートを使ってルーティングされます。

## PBR のデフォルト設定

なし。

## PBR の設定方法

- [PBR の設定](#)
- [ローカル PBR の設定](#)
- [PBR 再帰ネクスト ホップの設定](#)



(注) ポリシー ベース ルーティングを使用した複数の VRF 選択 (PBR VRF) については、次のマニュアルを参照してください。

[http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp\\_mltrvrflct\\_pbr.html](http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_mltrvrflct_pbr.html)

## PBR の設定

PBR をインターフェイスに設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]	パケットの出力先を制御するためのルート マップを定義します。このコマンドを入力すると、ルータはルートマップ コンフィギュレーション モードになります。
ステップ 2	Router(config-route-map)# <b>match length</b> <i>min max</i>  Router(config-route-map)# <b>match ip address</b> { <i>access-list-number</i>   <i>name</i> } [... <i>access-list-number</i>   <i>name</i> ]	一致基準を指定します。  多くのルート マップ マッチング オプションがありますが、ここでは、長さおよび/または IP アドレスだけを指定できます。  <ul style="list-style-type: none"> <li><b>length</b> はレベル 3 パケット長と一致します。</li> <li><b>ip address</b> は、1 つまたは複数の標準または拡張 アクセス リストで許可される送信元または送信先 IP アドレスを照合します。</li> </ul> <b>match</b> コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。
ステップ 3	Router(config-route-map)# <b>set ip precedence</b> [ <i>number</i>   <i>name</i> ]  Router(config-route-map)# <b>set ip df</b>  Router(config-route-map)# <b>set ip vrf</b> <i>vrf_name</i>  Router(config-route-map)# <b>set ip next-hop</b> <i>ip-address</i> [... <i>ip-address</i> ]  Router(config-route-map)# <b>set ip next-hop recursive</b> <i>ip-address</i> [... <i>ip-address</i> ]  Router(config-route-map)# <b>set interface</b> <i>interface-type interface-number</i> [... <i>type number</i> ]  Router(config-route-map)# <b>set ip default next-hop</b> <i>ip-address</i> [... <i>ip-address</i> ]  Router(config-route-map)# <b>set default interface</b> <i>interface-type interface-number</i> [... <i>type ...number</i> ]	基準に一致したパケットで実行されるアクション (1 つまたは複数) を指定します。次のうちの任意の項目またはすべてを指定できます。  <ul style="list-style-type: none"> <li><b>precedence</b> : IP ヘッダーに <b>precedence</b> 値を設定します。 <b>precedence</b> の番号または名前のいずれかを指定できます。</li> <li><b>df</b> : IP ヘッダー内に、「Don't Fragment」(DF) ビットを設定します。</li> <li><b>vrf</b> : VPN ルーティング/転送 (VRF) インスタンスを設定します。</li> <li><b>next-hop</b> : パケットをルーティングするネクスト ホップを設定します。</li> <li><b>next-hop recursive</b> : ホップが隣接していないルータへの場合にパケットをルーティングするネクスト ホップを設定します。</li> <li><b>interface</b> : パケットの出力インターフェイスを設定します。</li> <li><b>default next-hop</b> : その宛先に明示パスがない場合にパケットをルーティングするネクスト ホップを設定します。</li> <li><b>default interface</b> : その宛先に明示パスがない場合のパケットの出力インターフェイスを設定します。</li> </ul>

	コマンド	目的
ステップ 4	Router(config-route-map)# <b>interface</b> interface-type interface-number	インターフェイスを指定し、ルータでインターフェイス コンフィギュレーション モードを開始します。
ステップ 5	Router(config-if)# <b>ip policy route-map</b> map-tag	PBR で使用するルート マップを識別します。1 つのインターフェイスにはただ 1 つのルート マップ タグしか指定できませんが、シーケンス番号を持つ複数のルート マップ項目を作成できます。項目は、最初の一致が現れるまで、シーケンス番号の順に評価されます。一致する項目がない場合、パケットは通常どおりにルーティングされます。

**set** コマンドは、他のコマンドとともに使用できます。これらは、上記のステップ 3 に示す順序に従って評価されます。使用可能なネクスト ホップはインターフェイスで暗黙指定されます。ローカル ルータは、ネクスト ホップと使用可能なインターフェイスを検出したら、パケットをルーティングします。

## ローカル PBR の設定

スイッチで発信されるすべてのトラフィックに PBR を設定する手順は、次のとおりです。

コマンド	目的
Router(config)# <b>ip local policy route-map</b> map-tag	ローカル PBR で使用するルート マップを識別します。



(注)

- ローカル PBR トラフィックは RP のソフトウェアで処理されます。
- ローカル PBR で使用するルート マップを表示するには、**show ip local policy** コマンドを使用します。

## PBR 再帰ネクスト ホップの設定

- 「再帰ネクストホップ IP アドレスの設定」(P.33-5)
- 「再帰ネクストホップ設定の確認」(P.33-6)

## 再帰ネクストホップ IP アドレスの設定



(注)

PBR がサポートする再帰ネクストホップ IP アドレスは、ルートマップ エントリごとに 1 つのみです。

	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>パスワードを入力します（要求された場合）。</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 permit source</code>  例： Router(config)# access-list 101 permit 10.60.0.0 0.0.255.255	アクセス リストを設定します。設定例では、 <b>10.60.0.0.0.0.255.255</b> サブネット内に分類されるすべての発信元 IP アドレスが許可されます。
ステップ 4	<code>route-map map-tag</code>  例： Router(config)# route-map abccomp	ポリシー ルーティングをイネーブルにし、ルートマップ コンフィギュレーション モードを開始します。
ステップ 5	<code>set ip next-hop ip-address</code>  例： Router(config-route-map)# set ip next-hop 10.10.1.1	ネクストホップ ルータ IP アドレスを設定します。 <b>(注)</b> この IP アドレスは、ネクストホップ再帰ルータ設定とは別に設定します。
ステップ 6	<code>set ip next-hop {ip-address [...ip-address]   recursive ip-address}</code>  例： Router(config-route-map)# set ip next-hop recursive 10.20.3.3	再帰ネクストホップ IP アドレスを設定します。 <b>(注)</b> 中継 IP アドレスが宛先への短いルートである場合、この設定によって、パケットが再帰 IP アドレスを使ってルーティングされるとは限りません。
ステップ 7	<code>match ip address access-list-number</code>  例： Router(config-route-map)# match ip address 101	一致するアクセス リストを設定します。
ステップ 8	<code>end</code>  例： Router(config-route-map)# end	現在のルート マップ 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。

## 再帰ネクストホップ設定の確認

再帰ネクストホップ設定を確認するには、次の手順を実行します。

### ステップ 1 show running-config | begin abccomp

このコマンドを次の例のように使用し、ネクストホップの IP アドレスおよび再帰ネクストホップ IP アドレスを確認します。

```
Router# show running-config | begin abccomp

route-map abccomp permit 10
  match ip address 101 ! Defines the match criteria for an access list.
  set ip next-hop recursive 10.3.3.3 ! If the match criteria are met, the recursive IP
  address is set.
  set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
```

## ステップ 2 show route-map map-name

このコマンドを次の例のように使用し、ルート マップを表示します。

```
Router# show route-map abccomp

route-map abccomp, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop recursive 10.3.3.3
    ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
  Policy routing matches: 0 packets, 0 bytes
```

# PBR の設定例

- [同等アクセス例](#)
- [ネクスト ホップを変更する例](#)
- [再帰ネクストホップ IP アドレス : 例](#)



(注) 次に、**access-list** コマンド (ACL) の使用が含まれる例を示します。ACL の割り込みレベルでログインがサポートされていないため、**log** キーワードは、ポリシー ベース ルーティング (PBR) でこのコマンドと共に使用してはなりません。

## 同等アクセス例

次に、2 つの送信元が、異なるサービス プロバイダーに対して同等アクセスを持つ例を示します。ルータにパケットの宛先について明示パスがない場合、送信元 209.165.200.225 から非同期インターフェイス 1 に着信したパケットは、209.165.200.228 にあるルータへ送信されます。ルータにパケットの宛先について明示パスがない場合、送信元 209.165.200.226 から着信したパケットは、209.165.200.229 にあるルータへ送信されます。宛先についての明示的なルートがルータにない他のすべてのパケットは破棄されます。

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface async 1
  ip policy route-map equal-access
!
route-map equal-access permit 10
  match ip address 1
  set ip default next-hop 209.165.200.228
route-map equal-access permit 20
  match ip address 2
  set ip default next-hop 209.165.200.229
```

```
route-map equal-access permit 30
  set default interface null0
```

## ネクスト ホップを変更する例

次に、異なる送信元から異なる場所（ネクスト ホップ）へルーティングし、IP ヘッダーに **Precedence** ビットを設定する例を示します。送信元 209.165.200.225 から着信したパケットはプライオリティに **Precedence** ビットを設定されて 209.165.200.227 にあるネクスト ホップに送信され、送信元 209.165.200.226 から着信したパケットはクリティカルに **Precedence** ビットを設定されて 209.165.200.228 にあるネクスト ホップへ送信されます。

```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
interface ethernet 1
  ip policy route-map Texas
!
route-map Texas permit 10
  match ip address 1
  set ip precedence priority
  set ip next-hop 209.165.200.227
!
route-map Texas permit 20
  match ip address 2
  set ip precedence critical
  set ip next-hop 209.165.200.228
```

## 再帰ネクストホップ IP アドレス : 例

次に、IP アドレス 10.3.3.3 を再帰ネクストホップ ルータとして設定する例を示します。

```
route-map abccomp
  set ip next-hop 10.1.1.1
  set ip next-hop 10.2.2.2
  set ip next-hop recursive 10.3.3.3
  set ip next-hop 10.4.4.4
```



**ヒント** Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

技術マニュアルのアイデア フォーラムに参加する