



# ポリシーベースルーティング（PBR）の設定

- [ポリシーベースルーティング（1 ページ）](#)

## ポリシーベースルーティング

### ポリシーベースルーティングの概要

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティングプロトコルから取得したルートへの信頼度を小さくします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティングポリシーを設定したり、実装したりできます。

- 特定のエンドシステムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、インタラクティブ対バ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を実現できます。たとえば、在庫記録を本社に送信する場合は高帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーションデータは低帯域で低コストのリンクで送信できます。

PBR が有効な場合は、アクセスコントロールリスト（ACL）を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR が有効なインターフェイスで受信されたすべてのパケットは、ルートマップを通過します。ルートマップで定義された基準に基づいて、パケットは適切なネクストホップに転送（ルーティング）されます。

- 許可とマークされているルートマップ文は次のように処理されます。

- `match` コマンドは長さまたは複数の ACL で照合できます。ルート マップ文には複数の `match` コマンドを含めることができます。論理関数またはアルゴリズム関数は、許可または拒否の決定がされるまで、すべての `match` コマンドで実行されます。

次に例を示します。

```
match length A B
match ip address acl1 acl2
match ip address acl3
```

パケットは、`match length A B` または `acl1` または `acl2` または `acl3` により許可される場合に許可されます。

- 決定が許可の場合は、`set` コマンドで指定されたアクションがパケットで適用されます。
- 下された決定が拒否の場合は、PBR アクション (`set` コマンドで指定された) が適用されません。代わりに、処理ロジックが、シーケンス内の次のルートマップ文 (シーケンス番号が次に高い文) に移動します。次の文が存在しない場合は、PBR 処理が終了し、パケットがデフォルトの IP ルーティング テーブルを使用してルーティングされます。
- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

標準 IP ACL を使用すると、アプリケーション、プロトコルタイプ、またはエンドステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定できます。一致が見つかるまで、ルートマップにこのプロセスが行われます。一致が見つからない場合、通常の宛先ベースルーティングが行われます。`match` ステートメントリストの末尾には、暗黙の拒否ステートメントがあります。

`match` 句が満たされた場合は、`set` 句を使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

## PBR の設定方法

- PBR を使用するには、スイッチまたはアクティブスタック上でフィーチャセットを有効にしておく必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR を有効にできます。
- スイッチは一致長に基づき PBR をサポートします。
- レイヤ 3 モードの EtherChannel ポート チャンネルにはポリシー ルート マップを適用できませんが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとする、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。

- スイッチまたはスイッチ スタックには最大 128 個の IP ポリシー ルート マップを定義できます。
- スイッチまたはスイッチ スタックには、PBR 用として最大 512 個のアクセス コントロール エントリ (ACE) を定義できます。
- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
  - ローカル アドレス宛ての packets を許可する ACL と照合させないでください。PBR がこれらの packets を転送するため、ping または Telnet の失敗やルート プロトコルのフラッピングを発生させる可能性があります。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスで有効になっているときは、VRF を有効にはできません。その反対の場合も同じで、VRF がインターフェイスで有効になっているときは、PBR を有効にできません。
- PBR で使用されるハードウェア エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- TOS、DSCP、および IP Precedence に基づく PBR はサポートされません。
- set interface、set default next-hop、および set default interface はサポートされません。
- ip next-hop recursive および ip next-hop verify availability 機能は使用できません。next-hop は、直接接続される必要があります。
- set アクションのないポリシー マップはサポートされます。一致 packets は通常どおりにルーティングされます。
- match 句のないポリシー マップはサポートされます。set アクションはすべての packets に適用されます。

デフォルトでは、PBR はスイッチ上で無効です。PBR を有効にするには、一致基準および結果アクションを指定するルートマップを作成する必要があります。次に、特定のインターフェイスでそのルートマップ用の PBR を有効にします。指定したインターフェイスに着信した packets のうち、match 句と一致したものはすべて PBR の対象になります。

スイッチで生成された packets またはローカル packets は、通常どおりにポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルに有効にすると、そのスイッチから送信されたすべての packets がローカル PBR の影響を受けます。ローカル PBR は、デフォルトで無効に設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>configure terminal</b></p> <p>例 :</p> <pre>スイッチ# configure terminal</pre>	グローバル設定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 2	<p><b>route-map</b> <i>map-tag</i> [<b>permit</b>] [<i>sequence number</i>]</p> <p>例 :</p> <pre>スイッチ(config)# route-map pbr-map permit</pre>	<p>パケットの出力場所を制御するために使用するルートマップを定義し、ルートマップのコンフィギュレーションモードを開始します。</p> <ul style="list-style-type: none"> <li>• <i>map-tag</i> - : ルートマップ用のわかりやすい名前を指定します。 <b>ip policy route-map</b> インターフェイス コンフィギュレーション コマンドは、この名前を使用して、このルートマップを参照します。同じ <i>map-tag</i> がある複数の <b>route-map</b> 文は、1 つの <b>route-map</b> を定義します。</li> <li>• (任意) <b>permit</b> - : <b>permit</b> が指定され、このルートマップの一致条件が満たされている場合は、<b>set</b> アクションの制御に従ってルートがポリシールーティングされます。</li> <li>• (任意) <i>sequence number</i> - : シーケンス番号は、特定のルートマップ内の <b>route-map</b> ステートメントの位置を示します。</li> </ul>
ステップ 3	<p><b>match ip address</b> {<i>access-list-number</i>   <i>access-list-name</i>} [<i>access-list-number</i> ...<i>access-list-name</i>]</p> <p>例 :</p> <pre>スイッチ(config-route-map)# match ip address 110 140</pre>	<p>1 つ以上の標準または拡張アクセスリストで許可されている送信元および宛先 IP アドレスを照合します。ACL は、複数の送信元および宛先 IP アドレスでも照合できます。</p> <p><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。</p>
ステップ 4	<p><b>match length</b> <i>min max</i></p> <p>例 :</p> <pre>スイッチ(config-route-map)# match length 64 1500</pre>	<p>パケット長と照合します。</p>
ステップ 5	<p><b>set ip next-hop</b> <i>ip-address</i> [...<i>ip-address</i>]</p> <p>例 :</p> <pre>スイッチ(config-route-map)# set ip next-hop 10.1.6.2</pre>	<p>基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します (ネクスト ホップは隣接している必要があります)。</p>
ステップ 6	<p><b>set ip next-hop verify-availability</b> [<i>next-hop-address</i> <i>sequence track object</i>]</p> <p>例 :</p> <pre>スイッチ(config-route-map)# set ip next-hop verify-availability 95.1.1.2.1 track 100</pre>	<p>ルートマップを設定し、トラッキング対象オブジェクトの到達可能性を確認します。</p> <p>(注) このコマンドは、IPv6 および VRF ではサポートされません。</p>

	コマンドまたはアクション	目的
ステップ 7	<b>exit</b> 例： スイッチ(config-route-map)# exit	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	<b>interface interface-id</b> 例： スイッチ(config)# interface gigabitethernet 1/0/1	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、設定するインタフェースを指定します。
ステップ 9	<b>ip policy route-map map-tag</b> 例： スイッチ(config-if)# ip policy route-map pbr-map	レイヤ 3 インターフェイス上で PBR を有効にし、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設定できるルートマップは、1つだけです。ただし、異なるシーケンス番号を持つ複数のルート マップ エントリを設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。
ステップ 10	<b>ip route-cache policy</b> 例： スイッチ(config-if)# ip route-cache policy	(任意) PBR の高速スイッチングを有効にします。PBR の高速スイッチングを有効にするには、PBR を有効にする必要があります。
ステップ 11	<b>exit</b> 例： スイッチ(config-if)# exit	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 12	<b>ip local policy route-map map-tag</b> 例： スイッチ(config)# ip local policy route-map local-pbr	(任意) ローカル PBR を有効にして、スイッチから送信されるパケットに PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 13	<b>end</b> 例： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 14	<b>show route-map [map-name]</b> 例： スイッチ# show route-map	(任意) 設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 15	<b>show ip policy</b> 例： スイッチ# show ip policy	(任意) インターフェイスに付加されたポリシー ルート マップを表示します。

	コマンドまたはアクション	目的
ステップ 16	<b>show ip local policy</b>  例 : スイッチ# show ip local policy	(任意) ローカル PBR が有効であるかどうか、および有効である場合は使用されているルートマップを表示します。

## PBR を設定するための機能情報

表 1: PBR の機能情報

機能名	リリース	機能情報
ポリシーベース ルーティング	Cisco IOS リリース 15.2(6)E2	ポリシーベースのルーティングを使用して、トラフィックフローに定義済みポリシーを設定します。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。