



# ポリシーベース ルーティングの設定

この章は、次の項で構成されています。

- [ポリシーベース ルーティングについて \(1 ページ\)](#)
- [ポリシーベース ルーティングの前提条件 \(5 ページ\)](#)
- [ポリシーベース ルーティングの注意事項と制約事項 \(5 ページ\)](#)
- [ポリシーベース ルーティングのデフォルト設定 \(8 ページ\)](#)
- [ポリシーベース ルーティングの設定 \(8 ページ\)](#)
- [ポリシーベース ルーティングの設定の確認 \(18 ページ\)](#)
- [ポリシーベース ルーティングの設定例 \(19 ページ\)](#)
- [ポリシーベース ルーティングの関連資料 \(22 ページ\)](#)

## ポリシーベース ルーティングについて

ポリシーベース ルーティングを使用すると、IPv4 および IPv6 トラフィックフローに定義済みのポリシーを設定し、ルーティングプロトコルから派生したルートへの依存を弱めることができます。ポリシーベース ルーティングがイネーブルのインターフェイスで受信するすべてのパケットは、拡張パケットフィルタまたはルートマップを経由して渡されます。ルートマップでは、パケットの転送先を決定するポリシーを記述します。

ポリシーベース ルーティングには、次の機能が含まれます。

- 送信元ベース ルーティング：異なるユーザセットを起点とするトラフィックをポリシールータ上のそれぞれ異なる接続を使用してルーティングします。
- QoS (Quality of Service)：ネットワークの周辺で IP パケット ヘッダーに優先または ToS (タイプ オブ サービス) 値を設定することによって、またはキューイング メカニズムを利用して、ネットワークのコアまたはバックボーンでトラフィックにプライオリティを設定することによって、トラフィックを差別化します (『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』を参照)。
- ロードシェアリング：トラフィックの特性に基づいて、複数のパスにトラフィックを分散します。

## ポリシールートマップ

ルートマップのエントリごとに、**match** 文と **set** 文の組み合わせが 1 つずつ含まれています。**match** 文では、該当するパケットが特定のポリシーを満たす基準（つまり、満たすべき条件）を定義します。**set** 文節で、**match** 基準を満たしたパケットをどのようにルーティングするかを説明します。

ルートマップ文を許可または拒否として指定できます。文の解釈は次のとおりです。

- 文に許可が指定されていて、なおかつパケットが一致基準を満たしている場合は、の **set** 文節が適用されます。そのアクションの 1 つに、ネクストホップの選択が含まれます。
- 文に拒否が指定されている場合、一致基準を満たすパケットは標準のフォワーディングチャンネルを通じて送り返され、宛先ベースルーティングが実行されます。
- 文が **permit** とマークされ、パケットがいずれのルートマップ文にも一致しない場合、そのパケットは通常の転送チャンネルを介して返送され、宛先ベースのルーティングが実行されます。



(注) ポリシールーティングは、パケットの送信元となるインターフェイスではなく、パケットを受信するインターフェイス上で指定します。

## ポリシーベースルーティングの **set** 基準

Cisco Nexus 9000 シリーズスイッチは、ポリシーベースルーティングで使用されるルートマップに対して次の **set** コマンドをサポートしています。

- **set {ip | ipv6} next-hop address1 [address2...] [load-share]**
- **set {ip | ipv6} default next-hop address1 [address2...] [load-share]**
- **set {ip | ipv6} vrf vrf-name next-hop address1 [address2...] [load-share]**
- **set interface null0**

これらの **set** コマンドは、ルートマップシーケンス内では相互に排他的です。

最初のコマンドで、IP アドレスでは、パケットの転送先である宛先へのパス上の隣接ネクストホップルータを指定します。その時点でアップの接続インターフェイスに関連付けられた最初の IP アドレスがパケットのルーティングに使用されます。



(注) 任意に、最大 32 の IP アドレスにバランシングトラフィックをロードするように、ネクストホップアドレスのこのコマンドを設定できます。この場合、Cisco NX-OS は各 IP フローのすべてのトラフィックを特定の IP ネクストホップアドレスに送信します。

パケットが定義された一致基準のいずれにも一致しない場合、そのパケットは標準の宛先ベースルーティングプロセスを使用してルーティングされます。

## ポリシーベースルーティングのルートマップサポートマトリックス

次の表に、最新の出荷リリースを実行しているCisco Nexus 9000シリーズスイッチでのポリシーベースルーティングの設定可能なmatchおよびsetステートメントを示します。

次の凡例がテーブルに適用されます。

- [はい (Yes) ] : ステートメントはポリシーベースルーティングでサポートされます。
- No : ステートメントはポリシーベースルーティングではサポートされません。
- ステートメントがポリシーベースルーティングに適用されない場合は、ステートメントの横の列にダッシュ (—) が表示されます。
- 説明が必要な場合は、適切な行/列に情報が追加されます。

表 1:ポリシーベースルーティングの SET ルートマップステートメント

SET ルートマップステートメント	ポリシーベースルーティング (PBR)
IPv4 ネクストホップ	はい
IPv6 ネクストホップ	はい
IPv4 VRF ネクストホップ	はい
IPv6 VRF ネクストホップ	はい
デフォルト IPv4 ネクストホップ	はい
デフォルト IPv6 ネクストホップ	はい
IPv4 ネクストホップの可用性の確認	はい
IPv6 ネクストホップの可用性の確認	はい
デフォルトのIPv4ネクストホップの可用性の確認	はい
デフォルトのIPv6ネクストホップの可用性の確認	はい
インターフェイス null0	はい
VRF	いいえ

## ルート マップ処理ロジック

ルートマップを持つインターフェイスがパケットを受信すると、転送ロジックはシーケンス番号に従い各ルートマップ ステートメントを処理します。

ルート マップ文が `route-map...permit` 文の場合、パケットは **match** コマンドの基準と照合されます。このコマンドは、1つ以上のアクセスコントロールエントリ (ACE) を持つACLを参照する場合があります。パケットがACLの許可ACEに一致すると、ポリシーベースルーティングロジックは **set** コマンドがパケットで指定しているアクションを実行します。

ルート マップ文に `route-map... deny` 拒否文がある場合、パケットは一致コマンドの基準と照合されます。このコマンドは、1つ以上のACEを持つACLを参照する場合があります。パケットがACLの許可ACEに一致すると、ポリシーベース ルーティングプロセスが停止し、パケットはデフォルト 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。



(注) **set** コマンドは、**route-map... deny** 文内部に影響しません。

- ルートマップ設定に **match** 文が含まれていない場合、ポリシーベースルーティングロジックは **set** コマンドで指定されているアクションをパケットに対して実行します。すべてのパケットは、ポリシーベースルーティングを使用してルーティングされます。
- ルートマップコンフィギュレーションが **match** ステートメントを参照し、**match** ステートメントがアクセスコントロールエントリ (ACE) のない既存のACLまたは既存のACLを参照する場合、パケットはデフォルト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。
- **set { ip | ipv6 } next-hop** コマンドで指定されているネクスト ホップがダウンしているか、アクセス不能であるか、削除されている場合、パケットはデフォルトルーティング テーブルを使用してルーティングされます。

Cisco NX-OS リリース 9.2(3)以降では、**next-hop ip-address load-share** コマンドを使用して、ECMPパス上でネクストホップが再帰的である場合、ポリシーベースルーティングトラフィックのバランスをとることができます。この状況は、次のスイッチ、ラインカード、およびモジュールでサポートされます。

- N9K-C9372TX
- N9K-X9564TX
- N9K-X9732C-EX

すべてのネクストホップルーティング要求について、ルーティングプロファイルマネージャ (RPM) はユニキャスト ルーティング情報ベース (uRIB) を使用してそれらを解決します。また、RPM はすべての ECMP パスをプログラムするため、すべての ECMP パスを均等にロード バランシングできます。PMP over ECMP は IPv4 でのみサポートされます。

## ポリシーベース ルーティングの前提条件

ポリシーベース ルーティングの前提条件は、次のとおりです。

- 有効なライセンスをインストールします。
- ポリシーベース ルーティングを有効にする必要があります。
- インターフェイスに IP アドレスを割り当て、インターフェイスをアップにしてから、ポリシーベース ルーティング用のルート マップをインターフェイス上で適用します。

## ポリシーベース ルーティングの注意事項と制約事項

ポリシーベース ルーティングに関する注意事項および制約事項は、次のとおりです。

- 9700-EX/FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチは、IPv4 ポリシーベース ルーティングのみをサポートします。
- 次のスイッチは、IPv4 および IPv6 のポリシーベース ルーティングをサポートします。
  - Cisco Nexus 9200 プラットフォーム スイッチ
  - Cisco Nexus 9300-EX/FX/FX2/FX3/GX プラットフォーム スイッチ
  - 9636C-R、9636C-RX、および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチプロトコルネイバーが直接接続されている場合は、明示的なホワイトリストが必要になることがあります。
- ポリシーベース ルーティングのルート マップでは、1 つのルート マップ文に `match` 文を 1 つだけ指定できます。
- ポリシーベース ルーティングのルート マップでは、1 つのルート マップ文に `match` 文を 1 つだけ指定できます。IP SLA ポリシーベース ルーティングの詳細については、「*Cisco Nexus 9000 シリーズ NX-OS IP SLA 設定ガイド*」を参照してください。



---

(注) 9636C-R、9636C-RX、および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチは、IP SLA をサポートしていません。

---

- `match` コマンドで、ポリシーベース ルーティング用ルート マップの複数の ACL を参照できません。
- インターフェイスが同じ仮想ルーティング/転送 (VRF) インスタンスに所属している場合は、ポリシーベース ルーティング対応のさまざまなインターフェイス間で、同じルート マップを共有できます。

- 一致基準としてプレフィックスリストを使用することはサポートされていません。ポリシーベースルーティングルートマップではプレフィックスリストを使用しないでください。
- ポリシーベースルーティングは、ユニキャストトラフィックのみをサポートします。マルチキャストトラフィックはサポートされていません。
- ポリシーベースルーティングは、FEX ポートの着信トラフィックでサポートされていません。
- ポリシーベースルーティングは、Cisco Nexus 9300-EX プラットフォーム スイッチの FEX ポートではサポートされません。
- 9636C-R、9636C-RX、および 9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチのみが、レイヤ3ポートチャネルサブインターフェイスを使用したポリシーベースルーティングをサポートします。
- Cisco NX-OS リリース 10.1 (2) 以降、レイヤ3ポートチャネルサブインターフェイスを使用したポリシーベースルーティングは、Cisco Nexus 9300-X クラウドスケールスイッチでサポートされます。
- ポリシーベースルーティングのルート マップで使用する ACL には拒否アクセス コントロール エントリ (ACE) 含めることができません。
- ポリシーベースルーティングは、デフォルトのシステムルーティングモードでのみサポートされます。
- Cisco Nexus 3164Q スイッチは、**set vrf** コマンドをサポートしていません。
- インターフェイス上に複数の機能 (PBR や入力 ACL など) を設定すると、それらの機能の ACL は TCAM 最適化のためにマージされます。その結果、統計情報はサポートされません。
- VXLAN を使用する PBR の場合、load-share キーワードは必要ありません。



---

(注) 9700-EX/FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチは、VXLAN 経由の IPv4/IPv6 ポリシーベースルーティングをサポートします。9636C-R、9636C-RX、および 9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチは、VXLAN を介したポリシーベースルーティングをサポートしません。

---

- Cisco Nexus 9000 シリーズ スイッチはポリシーベース ACL (PBACL) をサポートしています (オブジェクトグループ ACL とも呼びます)。詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』を参照してください。



(注) 9636C-R、9636C-RX、および 9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチは、PBACL をサポートしません。

- PBR over VXLAN EVPN には、次の注意事項と制限事項が適用されます。
  - PBR over VXLAN EVPN は、Cisco Nexus 9300-EX/FX/GX/FX2/GX2 プラットフォーム スイッチでのみサポートされます。
  - PBR over VXLAN は、IP SLA、VTEP ECMP、および **set {ip | ipv6} next-hop ip-address** コマンドの **load-share** キーワードをサポートしていません。
  - PBR over VXLAN EVPN は、**set {ip | ipv6} vrf vrf-name next-hop ip-address** コマンドをサポートします。**set {ip | ipv6} vrf vrf-name next-hop ip-address** コマンドの複数の行を使用することにより、PBR over VXLAN EVPN は、複数のネクストホップごとに異なる VRF をサポートします。
- PBR 高速コンバージェンスには、次の注意事項と制限事項が適用されます。
  - PBR 高速コンバージェンスは、複数の代替ネクスト ホップで定義されたルートマップシーケンスを持ち、ロードシェアオプションなしでネクスト ホップアベイラビリティを追跡するための SLA プローブを使用して定義されたポリシーでのみサポートされます。
  - プライマリ ホップとバックアップ ネクスト ホップの同時障害は、高速パスでは処理されません。このようなイベントでは、システムはコントロールプレーンの更新にフォールバックします。
  - PBR高速コンバージェンスは、隣接関係の損失が検出されたイベントで主にサポートされます。
  - PBR高速コンバージェンスは、VXLAN経由で到達可能なネクスト ホップではサポートされません。
  - PBR高速コンバージェンスは、可用性を追跡するためにミリ秒の SLA /トラックでネクスト ホップが指定されている場合は使用しないでください。  
SLAの設定の詳細については、『Cisco Nexus 9000 シリーズ NX-OS IP SLA 設定ガイド』を参照してください。
  - PBR高速コンバージェンスが無効の場合、ACL リダイレクトエントリの数は、PBR ポリシー全体の一意のプライマリ ネクスト ホップの数に比例します。PBR 高速コンバージェンスが有効の場合、PBR ポリシーのルートマップシーケンス全体で設定されたプライマリ ネクスト ホップとバックアップ ネクスト ホップの固有の組み合わせの数に比例する ACL リダイレクトエントリがポート スライスごとに必要になることがあります。
  - 次のプラットフォームが PBR高速コンバージェンスをサポートします。  
N9K-C93180YC-FX、N9K-C93180YC2-FX、N9K-C93180YC-FX-24、N9K-C93108TC-FX、

N9K-C93108TC2-FX、N9K-C93108TC-FX-24、N9K-C9336C-FX2、N9K-C93240YC-FX2、  
N9K-C93360YC-FX2、N9K-C93216TC-FX2、N9K-C9336C-FX2-E、N9K-C9316D-GX、  
N9K-C93600CD-GX、N9K-C9364C-GX

## ポリシーベース ルーティングのデフォルト設定

表 2: デフォルトのポリシーベース ルーティング パラメータ

パラメータ	デフォルト
ポリシーベース ルーティング	ディセーブル

## ポリシーベース ルーティングの設定

### ポリシーベース ルーティング機能のイネーブル化

ルート ポリシーを設定する前に、ポリシーベース ルーティング機能をイネーブルにしておく必要があります。

#### 手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	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 2	<b>[no] feature pbr</b> 例： switch(config)# feature pbr	ポリシーベース ルーティング機能をイネーブルにします。  ポリシーベース ルーティング機能を無効にするには、このコマンドの <b>no</b> 形式を使用します。



	コマンドまたはアクション	目的
		(注) <b>no feature pbr</b> コマンドは、インターフェイスに適用されているポリシーを削除します。ACL またはルートマップ設定は削除されず、システムチェックポイントも作成されません。
ステップ 3	(任意) <b>show feature</b> 例： switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## ECMP 上のポリシーベース ルーティングの有効化

ECMP を介した PBR は、デフォルトでは有効になっていません。ルート ポリシーを設定する前に、ポリシーベース ルーティング機能をイネーブルにしておく必要があります。

### 手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. **[no] hardware profile pbr ecmp paths max-paths**
5. **show system internal rpm state**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	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 2	<b>[no] feature pbr</b> 例： switch(config)# feature pbr	ポリシーベース ルーティング機能をイネーブルにします。  ポリシーベース ルーティング機能を無効にするには、このコマンドの <b>no</b> 形式を使用します。

	コマンドまたはアクション	目的
		(注) <b>no feature pbr</b> コマンドは、インターフェイスに適用されているポリシーを削除します。ACL またはルートマップ設定は削除されず、システムチェックポイントも作成されません。
ステップ 3	(任意) <b>show feature</b> 例： switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	<b>[no] hardware profile pbr ecmp paths max-paths</b> 例： switch(config)# hardware profile pbr ecmp paths max-paths 12 Warning!!!: The pbr ecmp path limits have been changed. Please reload the switch now for the change to take effect. switch(config)#  switch(config)# no hardware profile pbr ecmp paths max-paths 12 Warning!!!: The pbr ecmp path limits have been changed. Please reload the switch now for the change to take effect. switch(config)#	IP ネクストホップの ECMP パスの数を設定します。ただし、設定された IP ネクストホップでロードシェアを明示的に設定しない限り、トラフィックはすべてのパスを通過しない可能性があります。PBRECMC パスを削除または変更すると、その変更は次のリロード後にのみ有効になります。範囲は 1 ~ 64 です。
ステップ 5	<b>show system internal rpm state</b>	PBR ECMP パスの現在設定されている値と動作値を表示します。

## PBR 高速コンバージェンスの設定

現在 PBR で使用されているネクストホップで障害が発生した場合、PBR 高速コンバージェンスによってトラフィックのコンバージェンス時間が 1 秒未満に短縮されます。PBR 高速コンバージェンスは、複数の代替ネクストホップで定義されたルートマップシーケンスを持つポリシーを支援します。このオプションは、ロードシェアリングオプションを使用せず、ネクストホップの可用性を追跡するための SLA プローブを使用します。

PBR 高速コンバージェンスは、スイッチではデフォルトで無効になっています。PBR 高速コンバージェンスを設定し、設定を保存した後、スイッチをリロードして PBR 高速コンバージェンスをアクティブにする必要があります。

### 始める前に

PBR 高速コンバージェンスを設定するには、まずポリシーベース ルーティング機能を有効にしておく必要があります。

手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. **[no] hardware profile pbr next-hop fast-convergence**
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	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 2	<b>[no] feature pbr</b> 例： switch(config)# feature pbr	ポリシーベースルーティング機能をイネーブルにします。
ステップ 3	<b>[no] hardware profile pbr next-hop fast-convergence</b> 例： switch(config)# hardware profile pbr next-hop fast-convergence	PBR高速コンバージェンスを設定します。  PBR 高速コンバージェンスを無効にするには、このコマンドの <b>no</b> 形式を使用します。  (注) PBR高速コンバージェンスのイネーブル化またはディセーブル化は、スイッチのリロード後に有効になります。
ステップ 4	<b>copy running-config startup-config</b> 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

例

次の例では、PBR高速コンバージェンスをイネーブルにし、スイッチをリロードします。

```
switch(config)# hardware profile pbr next-hop fast-convergence
Warning: Please save config and reload the system for the configuration to take effect.
switch(config)# copy running-config startup-config
switch(config)# reload
```

次のタスク

PBR高速コンバージェンスをイネーブルまたはディセーブルにし、設定を保存したら、スイッチをリロードします。

## ルートポリシーの設定

ポリシーベースルーティングでルートマップを使用すると、着信インターフェイスにルーティングポリシーを割り当てることができます。Cisco NX-OS はネクスト ホップおよびインターフェイスを検出するときに、パケットをルーティングします。

### 始める前に

9636C-R、9636C-RX、および9636Q-R ラインカードを搭載した Cisco Nexus 9508 以外のスイッチの場合、IPv6 トラフィックに対してポリシーベースルーティングポリシーを適用する前に、IPv6 RACL TCAM リージョンを（TCAM カービングを使用して）設定する必要があります。この手順については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』の「Configuring ACL TCAM Region Sizes」および「Configuring TCAM Carving - For Cisco NX-OS Release 6.1(2)I2(1) and Later Releases」を参照してください。



(注) スイッチに IPv4、IPv4 トラフィック用の RACL TCAM リージョンがデフォルトで用意されています。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **ip policy route-map map-name**
4. switch(config-if)# **ipv6 policy route-map map-name**
5. (任意) switch(config-route-map)# **end**
6. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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 2	switch(config)# <b>interface type slot/port</b>	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# <b>ip policy route-map map-name</b>	IPv4 ポリシーベース ルーティング用のルート マップをインターフェイスに割り当てます。
ステップ 4	switch(config-if)# <b>ipv6 policy route-map map-name</b>	IPv6 ポリシーベース ルーティング用のルート マップをインターフェイスに割り当てます。
ステップ 5	(任意) switch(config-route-map)# <b>end</b>	ルートマップ設定モードを終了して、特権 EXEC 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 6	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、インターフェイスにルート マップを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip policy route-map Testmap
switch(config)# exit
switch(config)# copy running-config startup-config
```

ルート マップ設定モードで、オプションとして、ルート マップに次の match パラメータを設定できます。

コマンド	目的
<b>match {ip   ipv6} address [accesslist-name]</b> 例: <pre>switch(config-route-map)# match ip address ACL1_v4  switch(config-route-map)# match ipv6 address ACL1_v6</pre>	1 つまたは複数の IPv4 または IPv6 アクセスコントロールリスト (ACL) に対して IP または IPv6 アドレスを照合します。このコマンドはポリシーベース ルーティング用であり、ルートフィルタリングまたは再配布では無視されます。

ルートマップ設定モードで、オプションとして、ルートマップに次の `set` パラメータを設定できます。

コマンド	目的
<p><b>set {ip   ipv6} next-hop address1 [address2... ][load-share] [drop-on-fail] [force-order][verify-availability]</b></p> <p>例:</p> <pre>switch(config-route-map)# set ip next-hop 192.0.2.1  switch(config-route-map)# set ipv6 next-hop 2001:0DB8::1</pre>	<p>ポリシーベース ルーティング用の IPv4、または IPv6 ネクスト ホップアドレスを設定します。このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクスト ホップアドレスが使用されます。</p> <p>任意の <b>load-share</b> キーワードを使用して、最大 32 のネクスト ホップアドレスにトラフィックのロードバランシングを行います。</p> <p>CLI で指定されたネクストホップ順序を有効にするには、オプションの <b>force-order</b> キーワードを使用します。</p> <p>設定されたネクストホップが到達不能になったときに、デフォルトルーティングを使用する代わりに、オプションの <b>drop-on-fail</b> キーワードを使用してパケットをドロップできます。Cisco Nexus 9200、9300-EX/FX/FX2 および 9364C プラットフォーム スイッチ、および -EX および -FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチがサポートされています。</p> <p>Cisco NX-OS Release 10.2(2)F 以降、追跡対象オブジェクトの到達可能性を確認するには、オプションの <b>verify-availability</b> キーワードを使用します。</p>

コマンド	目的
<p><b>set {ip   ipv6} default next-hop address2 [address2... ] [load-share] [verify-availability]</b></p> <p>例:</p> <pre>switch(config-route-map)# <b>set ip default next-hop 192.0.2.2</b> <b>set ipv6 default next-hop 2001:0DB8::1</b></pre>	<p>宛先への明示的ルートがない場合に使用する、ポリシーベースルーティング用のIPv4、またはIPv4 ネクストホップアドレスを設定します。このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクストホップアドレスが使用されます。これは、ネクストホップトラッキングでのみ実行できます。</p> <ul style="list-style-type: none"> <li>• 任意の <b>load-share</b> キーワードを使用して、最大16のネクストホップアドレスにトラフィックのロードバランシングを行います。</li> </ul> <p>(注) ソフトウェア転送トラフィックの場合、パケット指定の宛先またはパケットが受信されたVRFのユニキャストルーティングテーブルに存在するルートで条件一致がある場合、<b>set ip default next-hop</b> コマンドで指定されたものより優先されます。VRFにデフォルトルートが存在する場合でも、そのデフォルトルートはコマンドで設定されたものを上書きします。これは、ソフトウェア転送トラフィックにのみ適用されます。</p> <p>Cisco NX-OS リリース 10.2(2)F 以降、以下がサポートされます。</p> <ul style="list-style-type: none"> <li>• <b>set ip default next-hop</b> コマンドは、GX、GX2、およびFX3プラットフォームスイッチでサポートされています。</li> <li>• 追跡対象オブジェクトの到達可能性を確認するには、オプションの <b>verify-availability</b> キーワードを使用します。</li> </ul> <p>(注) このコマンドはN9K-C950xで現在サポートされていません。</p>

コマンド	目的
<pre> set {ip   ipv6} vrf vrf-name next-hop address1 [address2... ][force-order] [drop-on-fail][load-share]  例:  switch(config-route-map) # set ip vrf vrf1 next-hop 192.0.2.2 set ipv6 vrf vrf1 next-hop 2001:0DB8::1 </pre>	<p>ポリシーベースルーティングのデフォルトまたはユーザ定義の vrf に基づいて、IPv4 または IPv6 ネクスト ホップアドレスを設定します。</p> <p>このコマンドは、VRF インターフェイスに到着する VRF 間ルーティングパケットが、設定されたネクスト ホップに基づいて他の VRF を介してルーティングされることをサポートします。</p> <p>このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクストホップ アドレスが使用されます。</p> <p>(注) このコマンドでは、set ステートメントで複数の vrfs を使用できません。</p> <p>CLI で指定されたネクストホップ順序を有効にするには、オプションの <b>force-order</b> キーワードを使用します。</p> <p>設定されたネクストホップが到達不能になったときに、デフォルトルーティングを使用する代わりに、オプションの <b>drop-on-fail</b> キーワードを使用してパケットをドロップできます。Cisco Nexus 9200、9300-EX/FX/FX2 および 9364C プラットフォーム スイッチ、および -EX および -FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチがサポートされています。</p> <p>任意の <b>load-share</b> キーワードを使用して、最大 32 のネクストホップアドレスにトラフィックのロードバランシングを行います。</p>



コマンド	目的
<p>(オプション) <b>set {ip   ipv6} next-hop verify-availability next-hop-address track object</b></p> <p>例:</p> <pre>switch(config-route-map)# set ip next-hop verify-availability 192.0.2.2 track 1</pre>	<p>スイッチがそのネクストホップへのポリシールーティングを実行する前に、ルートマッピングのネクストホップの到達可能性を確認するポリシールーティングを設定するには、このコマンドを使用します。この手順を繰り返して、他のトラッキング対象オブジェクトの到達可能性を確認するためのルートマップを設定します。</p> <p>(注) オブジェクトトラッキングに関する詳細情報については、『Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide』を参照してください。</p>
<p>(オプション) <b>set {ip   ipv6} default next-hop verify-availability next-hop-address track object</b></p> <p>例:</p> <pre>switch(config-route-map)# set ip default next-hop verify-availability 192.0.2.2 track 1</pre>	<p>スイッチがそのネクストホップへのポリシールーティングを実行する前に、ルートマッピングのネクストホップの到達可能性を確認するポリシールーティングを設定するには、このコマンドを使用します。この手順を繰り返して、他のトラッキング対象オブジェクトの到達可能性を確認するためのルートマップを設定します。</p> <p>(注) オブジェクトトラッキングに関する詳細情報については、『Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide』を参照してください。</p>
<p>(オプション) <b>set {ip   ipv6} vrf vrf-name next-hop verify-availability next-hop-address track object</b></p> <p>例:</p> <pre>switch(config-route-map)# set ip vrf vrf1 next-hop verify-availability 192.0.2.2 track 1</pre>	<p>スイッチがそのネクストホップへのポリシールーティングを実行する前に、ルートマッピングのネクストホップの到達可能性を確認するポリシールーティングを設定するには、このコマンドを使用します。この手順を繰り返して、他のトラッキング対象オブジェクトの到達可能性を確認するためのルートマップを設定します。</p> <p>(注) オブジェクトトラッキングの設定の詳細については、『Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide』を参照してください。</p>

コマンド	目的
<pre>set interface {null0 } 例: switch(config-route-map)# set interface null0</pre>	<p>ルーティングに使用するインターフェイスを設定します。パケットをドロップするには <b>null0</b> インターフェイスを使用します。</p>

### 次のタスク

次に、ePBR の構成の出力例を示します。

```
epbr service lb_12 type 12
  probe ctp
  mode full-duplex
  service-endpoint interface eth1/1
  reverse interface eth1/2

epbr service fw_12
  probe ctp
  mode full-duplex
  service-endpoint interface eth1/4
  reverse interface eth1/5

epbr policy 12_policy
  match ip address traffic_acl vlan 10
  10 set service fw_12 fail-action forward
  20 set service lb_2 fail-action drop
  match ipv6 address traffic_acl_1 vlan 11
  10 set service fw_12 fail-action forward
  20 set service lb_2 fail-action drop
  match 12 address traffic_acl_2 vlan 12
  10 set service fw_12 fail-action forward
  20 set service lb_2 fail-action drop

interface eth1/10
epbr 12 policy 12_policy egress-interface eth1/11
epbr 12 policy 12_eth_1_2_policy egress-interface eth1/12 reverse
```

## ポリシーベース ルーティングの設定の確認

ポリシーベース ルーティングの設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
<b>show [ip   ipv6] policy [name]</b>	IPv4 または IPv6 ポリシーに関する情報を表示します。
<b>show route-map [name] pbr-statistics</b>	ポリシー統計情報を表示します。

ポリシー統計を有効にするには、**route-map map-name pbr-statistics** を使用します。ポリシー統計を消去するためには、**clear route-map map-name pbr-statistics** コマンドを使用します。

## ポリシーベース ルーティングの設定例

インターフェイス上で単純なルート ポリシーを設定する例を示します。

```
feature pbr
ip access-list pbr-sample_1
  permit tcp host 10.1.1.1 host 192.168.2.1 eq 80
ip access-list pbr-sample_2
  permit tcp host 10.1.1.2 host 192.168.2.2 eq 80
!
route-map pbr-sample permit 10
match ip address pbr-sample_1
set ip next-hop 192.168.1.1
route-map pbr-sample permit 20
match ip address pbr-sample_2
set ip next-hop 192.168.1.2
!
route-map pbr-sample pbr-statistics

interface ethernet 1/2
  ip policy route-map pbr-sample
```

次の出力で、この設定を確認します。

```
switch# show route-map pbr-sample

route-map pbr-sample, permit, sequence 10
  Match clauses:
    ip address (access-lists): pbr-sample_1
  Set clauses:
    ip next-hop 192.168.1.1
route-map pbr-sample, permit, sequence 20
  Match clauses:
    ip address (access-lists): pbr-sample_2
  Set clauses:
    ip next-hop 192.168.1.2

switch# show route-map pbr-sample pbr-statistics

route-map pbr-sample, permit, sequence 10
Policy routing matches: 84 packets

route-map pbr-sample, permit, sequence 20
Policy routing matches: 94 packets

Default routing: 233 packets
```



- (注) すべてのルートマップ シーケンスに対して表示される **ポリシー ルーティング マッチ数**には、ルートマップ内のシーケンスとマッチする着信データトラフィックの packets 数が含まれません。このカウンタは、PBR リダイレクション (そのシーケンスの「set」コマンド) が解決されたかどうかに関係なく増加します。同様に、上記の例では、`show route-map pbr-statistics pbr-sample` の出力の 2 つのルートマップ シーケンス (シーケンス 10 と 20) に対するポリシー ルーティング マッチ数が示されています。



- (注) デフォルトルーティングには、ルートマップ内のどのシーケンスともマッチしない着信データトラフィックのパケット数が含まれます。同様に上記の例では、デフォルトルーティングは、`show route-map pbr-statistics pbr-sample` 出力の最後に 1 回だけ表示されます。

この例は、ECMP パスと非 ECMP パス間のロードシェアリングを示しています。

```
switch# show run rpm
!Command: show running-config rpm
!Running configuration last done at: Sun Dec 23 16:02:32 2018
!Time: Sun Dec 23 16:06:13 2018

version 9.2(3) Bios:version 08.35
feature pbr

route-map policy1 pbr-statistics
route-map policy1 permit 10
  match ip address acl2
  set ip next-hop 131.1.1.2 load-share
route-map policy2 pbr-statistics
route-map policy2 permit 10
  match ip address acl2
  set ip next-hop verify-availability 131.1.1.2 track 1
  set ip next-hop verify-availability 30.1.1.2 track 2 load-share

interface Ethernet1/31
  ip policy route-map policy2
```

この例は、ネクストホップルーティング要求に関する情報を表示しています。

```
switch# show system internal rpm pbr ip nexthop
PBR IPv4 nexthop table for vrf default

30.1.1.2 Usable
  via 28.1.1.2 Ethernet1/18 a46c.2ae3.02a7

131.1.1.2 Usable
  via 111.1.1.2 Vlan81 8478.ac58.afc1
Usable
  via 112.1.1.2 Vlan82 8478.ac58.afc1
Usable
  via 113.1.1.2 Vlan83 8478.ac58.afc1
Usable
  via 114.1.1.2 Vlan84 8478.ac58.afc1
Usable
  via 115.1.1.2 Vlan85 8478.ac58.afc1
Usable
  via 116.1.1.2 Vlan86 8478.ac58.afc1
Usable
  via 117.1.1.2 Vlan87 8478.ac58.afc1
Usable
  via 118.1.1.2 Vlan88 8478.ac58.afc1
```

この例は、ユニキャスト RIB から受け取ったルートを表示しています。

```
switch# show ip route 130.1.1.2
IP Route Table for VRF "default"
```

```
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

130.1.1.0/24, ubest/mbest: 8/0
  *via 111.1.1.2, Vlan81, [110/120], 00:07:57, ospf-1, inter
  *via 112.1.1.2, Vlan82, [110/120], 00:07:57, ospf-1, inter
  *via 113.1.1.2, Vlan83, [110/120], 00:07:57, ospf-1, inter
  *via 114.1.1.2, Vlan84, [110/120], 00:07:57, ospf-1, inter
  *via 115.1.1.2, Vlan85, [110/120], 00:07:57, ospf-1, inter
  *via 116.1.1.2, Vlan86, [110/120], 00:07:57, ospf-1, inter
  *via 117.1.1.2, Vlan87, [110/120], 00:07:57, ospf-1, inter
  *via 118.1.1.2, Vlan88, [110/120], 00:07:57, ospf-1, inter
```

```
switch# show ip route 30.1.1.2
IIP Route Table for VRF "default"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

30.1.1.0/24, ubest/mbest: 1/0
  *via 28.1.1.2, [1/0], 00:38:36, static
```

次に、vrfベースのネクストホップを使用したポリシーベースルーティングの例を示します。

```
route-map policy_vrf_default_v4 permit 10
  match ip address acl1_v4_tc1
  set ip vrf default next-hop 31.1.1.1

route-map policy_vrf_nondefault_v4 permit 10
  match ip address acl1_v4_tc2
  set ip vrf vrf1 next-hop 32.1.1.1

show route-map policy_vrf_default_v4
route-map policy_vrf_default_v4, permit, sequence 10
  Match clauses:
    ip address (access-lists): acl1_v4_tc1
  Set clauses:
    ip vrf default next-hop 31.1.1.1

show route-map policy_vrf_nondefault_v4
route-map policy_vrf_nondefault_v4, permit, sequence 10
  Match clauses:
    ip address (access-lists): acl1_v4_tc2
  Set clauses:
    ip vrf vrf1 next-hop 32.1.1.1
```

次の例では、デフォルトのネクストホップを使用したポリシーベースルーティングを示します。

```
route-map policy_default_v4 permit 10
  match ip address acl1_v4_tc1
  set ip default next-hop 21.1.1.2

show route-map policy_default_v4
route-map policy_default_v4, permit, sequence 10
  Match clauses:
    ip address (access-lists): acl1_v4_tc1
  Set clauses:
    ip default next-hop 21.1.1.2
```

## ポリシーベースルーティングの関連資料

関連項目	マニュアルタイトル
IP SLA PBR オブジェクト トラッキング	<a href="#">『Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide』</a>
トラブルシューティング情報	<a href="#">『Cisco Nexus 9000 Series NX-OS Troubleshooting Guide』</a>

## 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。