CHAPTER 39

ポリシーベース ルーティングの設定

この章では、Catalyst 4500 シリーズ スイッチ上でのポリシーベース ルーティング（PBR）の設定作業について説明します。主な内容は次のとおりです。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

（注） 機能に関連するハードウェア プラットフォームまたはソフトウェア イメージ情報を確認するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリースノートを参照してください。

ポリシーベース ルーティングについて

ここでは、次の内容について説明します。

PBR は、トラフィック フローに関するポリシーを定義し、ルーティング プロトコルから派生したルートへの依存度を軽減することによって、パケット ルーティングを柔軟に行えるようにします。PBR は、ルーティング プロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すれば、高コスト リンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することができます。

設定したポリシーに基づいてパケットをルーティングする方法として、PBR を設定できます。たとえば、特定のエンド システムの ID またはアプリケーション プロトコルに基づいてパスを許可または拒否するルーティング ポリシーを実装することができます。

PBR を使用すると、次の作業を実行できます。

- 拡張アクセス リスト基準に基づいたトラフィックの分類。リストにアクセスし、一致基準を設定します。
- 特定のトラフィック処理が行われたパスへのパケットのルーティング。

ポリシーは、IP アドレス、ポート番号、またはプロトコルをベースとします。単純なポリシーの場合はこれらの記述子のいずれかを使用し、複雑なポリシーの場合はこれらのすべてを使用します。

PBR について

PBR がイネーブルの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 マップという拡張パケット フィルタを通過します。PBR で使用するルート マップはポリシーを要求し、パケットの転送先を判断します。

ルート マップは、許可または拒否としてマークできる文で構成されます。これは、次の方法で解釈されます。

- 文が deny とマークされている場合、一致基準に合致したパケットは通常転送チャネルを使用して送り返され、宛先ベースのルーティングを実行します。
- 文が permit とマークされていてパケットがアクセス リストと一致している場合、最初の有効な set 句がそのパケットに適用されます。

これについては、「ルート マップについて」（P.39-2）で詳しく説明します。

PBR を着信インターフェイス（パケットを受信するインターフェイス）に指定できますが、発信インターフェイスには指定できません。

ルート マップについて

PBR は、着信インターフェイス上でルート マップを適用することによって実装されます。インターフェイスごとに 1 つずつのルート マップを設定することができます。

ルート マップは、グローバル コンフィギュレーション パーサー モードで設定されます。その後で、1 つ以上のインターフェイスにこのルート マップを（インターフェイス コンフィギュレーション パーサー サブモードで）適用することができます。

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。

各ルート マップ文には、**match** コマンドと **set** コマンドが含まれています。**match** コマンドは、パケット データに適用される一致基準を示します。**set** コマンドは、パケットに対して実行される PBR アクションを示します。

次に、rm-test という名前の 1 つのルート マップと 6 つのルート マップ文の例を示します。

```
route-map rm-test permit 21
 match ip address 101
 set ip next-hop 21.1.1.1
!
route-map rm-test permit 22
 match ip address 102
 set ip next-hop 22.2.2.1
!
```

```
    route-map rm-test permit 23
     match ip address 101 2102
     set interface vlan23
!
    route-map rm-test deny 24
     match ip address 104
     set ip next-hop 24.4.4.1
    !
    route-map rm-test deny 25
     match ip address 105
     set ip next-hop 25.5.5.1
    !
    route-map rm-test permit 26
     match ip address 2104
     set ip next-hop 26.6.6.1
```

数字の 21、22、... 26 は、ルート マップ文のシーケンス番号です。

ここでは、次の内容について説明します。

- 「PBR ルート マップ処理ロジック」（P.39-3）
- 「再帰ネクストホップによるロード バランシング」（P.39-4）
- 「PBR ルート マップ処理ロジックの例」（P.39-4）

PBR ルート マップ処理ロジック

パケットがルート マップで設定されたインターフェイスに到着すると、転送ロジックがシーケンス番号順にそれぞれのルート マップ文を処理します。

出現したルート マップ文が **route-map... permit** 文の場合：

- パケットが **match** コマンド内の基準と照合されます。このコマンドは、1 つ以上の permit 式または deny 式を含めることが可能な ACL を参照することができます。パケットが ACL 内の式と照合され、許可 / 拒否の決定が下されます。
- 下された決定が許可の場合は、PBR ロジックがパケット上の **set** コマンドで指定されたアクションを実行します。
- 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。

出現したルート マップ文が **route-map... deny** 文の場合：

- パケットが **match** コマンドで指定された基準と照合されます。このコマンドは、1 つ以上の permit 式または deny 式を含めることが可能な ACL を参照することができます。パケットが ACL 内の式と照合され、許可 / 拒否の決定が下されます。
- 基準の決定が許可の場合は、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。
- 基準の決定が拒否の場合は、PBR 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。

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

ルート マップ文は次のプライオリティで適用される複数の **set** コマンドを持つことができます。

set ip next-hop

set ip next-hop recursive

set interface

set default ip next-hop

set default interface

set ip next-hop と **set ip next-hop recursive** コマンドの両方が同じルート マップ文に存在する場合は、**next-hop set** コマンドが適用されます。

set ip next-hop コマンドを使用できない場合は、**set ip next-hop recursive** コマンドが適用されます。

set ip recursive-next-hop と **set** interface コマンドがない場合、パケットはドロップされなければデフォルトのルーティング テーブルを使用してルーティングされます。パケットがドロップされる必要がある場合は、**set interface null0 configuration** コマンドが後に続く **set next-hop recursive** コマンドを使用します。

再帰ネクストホップによるロード バランシング

サブネットへの複数の等コスト ルートが **set ip next-hop recursive** コマンドによって設定されている場合は、ロード バランシングはルートへのすべての隣接関係が解決された場合にだけ行われます。いずれかの隣接関係が解決されていなければ、ロード バランシングは行われず、隣接関係が解決されたルートのうち 1 つだけが使用されます。隣接関係がいずれも解決しない場合は、パケットはソフトウェアで処理され、少なくとも 1 つの隣接関係がハードウェアで解決およびプログラムされます。PBR は、ルーティング プロトコルまたはその他の手段に依存して、すべての隣接関係を解決し、ロード バランシングを行わせます。

PBR ルート マップ処理ロジックの例

次のように定義された rm-test という名前のルート マップを取り上げます。

```
access-list 101  permit tcp host 61.1.1.1 host 133.3.3.1 eq 101
access-list 102  deny   tcp host 61.1.1.1 host 133.3.3.1 eq 102
access-list 2102 permit tcp host 61.1.1.1 host 133.3.3.1 eq 102
access-list 104  deny   tcp host 61.1.1.1 host 133.3.3.1 eq 104
access-list 2104 permit tcp host 61.1.1.1 host 133.3.3.1 eq 104
access-list 105  permit tcp host 61.1.1.1 host 133.3.3.1 eq 105


route-map rm-test permit 21
 match ip address 101
 set ip next-hop 21.1.1.1
!
route-map rm-test permit 22
 match ip address 102
 set ip next-hop 22.2.2.1
!
route-map rm-test permit 23
 match ip address 101 2102
 set interface vlan23
!
route-map rm-test deny 24
 match ip address 104
 set ip next-hop 24.4.4.1
!

route-map rm-test deny 25
 match ip address 105
 set ip next-hop 25.5.5.1
!
```

```
route-map rm-test permit 26
 match ip address 2104
 set ip next-hop 26.6.6.1
```

- 宛先ポートが 101 で 61.1.1.1 から 133.3.3.1 に転送される TCP パケット
  - シーケンス番号 21 の ACL 101 と一致します。
  - PBR がネクストホップ 21.1.1.1 経由でスイッチされます。

（注）　ACL 101 は、シーケンス番号 23 とも一致しますが、処理がその時点まで到達しません。

- 宛先ポートが 102 で 61.1.1.1 から 133.3.3.1 に転送される TCP パケット
  - シーケンス番号 21 で、ACL 101 アクションがこのパケットを拒否します（理由は、すべての ACL に黙示的拒否が含まれているためです）。処理がシーケンス番号 22 に進みます。
  - シーケンス番号 22 で、ACL 102 が TCP ポート 102 と一致しますが、ACL アクションは拒否です。処理がシーケンス番号 23 に進みます。
  - シーケンス番号 23 で、ACL 2102 が TCP ポート 102 と一致しますが、ACL アクションは許可です。
  - パケットが出力インターフェイス VLAN 23 にスイッチされます。
- 宛先ポートが 105 で 61.1.1.1 から 133.3.3.1 に転送される TCP パケット
  - 処理が、シーケンス番号 21 からシーケンス番号 24 に移動します。これは、これらのシーケンス番号内の ACL にポート 105 に対する拒否アクションが含まれているためです。
  - シーケンス番号 25 で、ACL 105 に TCP ポート 105 に対する許可アクションが含まれています。
  - ルート マップの拒否が実行され、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。

Catalyst 4500 シリーズ スイッチは、ルート マップの一致基準内の ACL で記述された一連のパケットと一致する TCAM 内のエントリをインストールすることによって、ルート マップ アクションとパケットを照合します。これらの TCAM エントリは、ハードウェアがそのアクションをサポートしない、またはハードウェアのリソースが消費されている場合に、必要な出力アクションを実行するか、または、パケットをソフトウェアに転送する隣接関係を示します。

ルート マップで **set interface ...** アクションが指定されている場合は、**match** 文と一致するパケットがソフトウェアでルーティングされます。同様に、ルート マップで **set default interface ...** アクションが指定されており、一致するパケットの IP ルートが存在しない場合は、パケットがソフトウェアでルーティングされます。

（注）　TCAM サイズとハードウェアにプログラミングする前に ACL をフラットにするために CPU に必要な時間とでハードウェア ベース PBR のスケールは決定されます。後者は PBR ポリシーに相当数のクラス マップが必要な場合に著しく増加します。たとえば、1,200 のクラス マップの PBR ポリシーにはハードウェアにプログラミングする前に「フラット化」の時間が 60 ～ 90 分必要になることがあります。このプロセスは、隣接関係の変更で PBR の再プログラミングが必要な場合に繰り返すことがあります。

PBR の使用

PBR で特定のパケットのルーティング パスを IP ルーティングによって選択されるデフォルト パスから変更することができます。たとえば、次の機能を提供するために、PBR を使用できます。

- 同等アクセス
- プロトコル依存ルーティング
- 送信元依存ルーティング
- 双方向対バッチ 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

アプリケーションまたはトラフィックによっては、送信元依存ルーティングが有効です。たとえば、在庫記録を本社に送信する場合は高帯域幅で高コストのリンクを短時間使用し、電子メールなどの日常的に使うアプリケーション データは低帯域幅で低コストのリンクで送信します。

（注）　PBR の設定は、グローバル ルーティング テーブルに属しているインターフェイス上でのみ可能です。PBR は、VRF に属しているインターフェイス上ではサポートされません。

ポリシーベース ルーティング（PBR）の設定作業

ここでは、PBR を設定するために実行する作業について説明します。最初の項の作業は必須ですが、残りの項の作業は任意です。設定例については、「PBR の設定例」（P.39-9）を参照してください。

- 「PBR のイネーブル化」（P.39-6）（必須）
- 「ローカル PBR のイネーブル化」（P.39-8）（任意）

PBR のイネーブル化

PBR をイネーブルにするには、一致基準およびすべての match 句と一致した場合の動作を指定するルート マップを作成する必要があります。次に、そのルート マップを特定のインターフェイスに適用する必要があります。指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

特定のインターフェイス上で PBR をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# route-map map-tag [permit | deny] [sequence-number]`	パケットの送信先を制御するルート マップを定義します。このコマンドは、スイッチをルート マップ コンフィギュレーション モードにします。
ステップ 2	`Switch(config-route-map)# match ip address {access-list-number | name} [...access-list-number | name]`	一致基準を指定します。一致基準は、1 つまたは複数の標準アクセス リストまたは拡張 IP アクセス リストの形式を取ります。アクセス リストでは、送信元 IP アドレスと宛先 IP アドレス、プロトコル タイプ、およびポート番号を指定することができます。標準アクセス リストと拡張 IP アクセス リストの詳細については、第 52 章「ACL によるネットワーク セキュリティの設定」を参照してください。

	コマンド	目的
ステップ 3	Switch(config-route-map)# **set ip next-hop** *ip-address* [*... ip-address*] Or	一致するパケットが送信されるネクストホップ IP アドレスを指定します。ここで指定したネクストホップ IP アドレスは、このスイッチに直接接続されたサブネットに属している必要があります。 複数のネクストホップ IP アドレスを指定した場合は、最初に使用可能なネクストホップが、一致するパケットのルーティングで選択されます。何らかの理由でネクストホップが使用できない（または使用できなくなった）場合は、リスト内で次のネクストホップが選択されます。
ステップ 4	Switch(config-route-map)# **set ip next-hop recursive** *ip-address*	再帰ネクストホップ IP アドレスを指定します。 **（注）** 再帰ネクスト ホップは直接接続されていないサブネットにできます。 **set ip next-hop recursive** コマンドは、ルートが再帰ネクストホップを通過しないような、宛先へのより短いルートを持つ中間ノードが存在する場合、パケットが再帰ネクストホップによってルーティングされることを保証しません。
ステップ 5	Switch(config-route-map)# **set interface** *interface-type interface-number* [*... type number*] Or	パケットが送信される出力インターフェイスを指定します。この動作は、パケットがローカル インターフェイスの外に転送されるように指定します。このインターフェイスはレイヤ 3 インターフェイス（スイッチポートではない）にする必要があります。 パケットは、次の条件のいずれかが満たされた場合にのみ、指定されたインターフェイスに転送されます。 • パケット内の宛先 IP アドレスが、指定されたインターフェイスが属している IP サブネット内に収まっている。 • パケット内の宛先 IP アドレスが、指定されたインターフェイス経由で到達可能である（IP ルーティング テーブル経由）。 パケット上の宛先 IP アドレスがこれらの条件のいずれも満たしていない場合は、パケットがドロップされます。このアクションは、一致するパケットをソフトウェアでスイッチするように強制します。
ステップ 6	Switch(config-route-map)# **set ip default next-hop** *ip-address* [*... ip-address*] Or	パケット内の宛先 IP アドレスに関する明示ルートが存在し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。ネクスト ホップにパケットを転送する前に、スイッチはパケットの宛先アドレスをユニキャスト ルーティング テーブル内で検索します。一致するものが見つかった場合、パケットはルーティング テーブルを経由して転送されます。一致するものが見つからなかった場合、パケットは指定されたネクスト ホップに転送されます。

	コマンド	目的
ステップ 7	`Switch(config-route-map)# set default interface interface-type interface-number [...type ...number]`	この宛先に関する明示ルートが存在しない場合にパケットが送信される出力インターフェイスを指定します。ネクスト ホップにパケットを転送する前に、スイッチはパケットの宛先アドレスをユニキャスト ルーティング テーブル内で検索します。一致するものが見つかった場合、パケットはルーティング テーブルを使用して転送されます。一致するものが見つからなかった場合、パケットは指定された出力インターフェイスに転送されます。 パケットは、次の条件のいずれかが満たされた場合にのみ、指定されたインターフェイスに転送されます。 • パケット内の宛先 IP アドレスが、指定されたインターフェイスが属している IP サブネット内に収まっている。 • パケット内の宛先 IP アドレスが、指定されたインターフェイス経由で到達可能である（IP ルーティング テーブル経由）。 パケット上の宛先 IP アドレスがこれらの条件のいずれも満たしていない場合は、パケットがドロップされます。このアクションは、一致するパケットをソフトウェアでスイッチするように強制します。
ステップ 8	`Switch(config-route-map)# interface interface-type interface-number`	インターフェイスを指定します。このコマンドは、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 9	`Switch(config-if)# ip policy route-map 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対して使用できるルート マップ タグは 1 つだけですが、異なるシーケンス番号を持つルート マップ エントリを複数設定できます。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 コマンドを相互に使用します。これらのコマンドは、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 スイッチがネクスト ホップを発見して、それが使用可能なインターフェイスの場合は、そのスイッチがパケットをルーティングします。

既存のルート マップを表示するには、**show route-map map-tag** コマンドを使用します。

（注）　**show route-map map-tag** コマンドの出力のパケット カウンタおよびバイト カウンタは更新されません。

ローカル PBR のイネーブル化

スイッチで生成されたパケットは、通常どおりにポリシー ルーティングされません。このようなパケットに対してローカル PBR をイネーブルにするために、次のコマンドを入力して、スイッチで使用されるルート マップを指定します。

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

これで、スイッチから発信されるすべてのパケットがローカル PBR の対象となります。

ローカル PBR で使用するルート マップ（ある場合）を表示するには、**show ip local policy** コマンドを使用します。

サポートされていないコマンド

ルートマップ コンフィギュレーション モードの次の PBR コマンドは CLI のものですが、Catalyst 4500 シリーズ スイッチの Cisco IOS ではサポートされていません。これらのコマンドを使用しようとすると、エラー メッセージが表示されます。

- **match-length**
- **set ip qos**
- **set ip tos**
- **set ip precedence**
- **set ip df**

PBR の設定例

ここでは、PBR の設定例を示します。

- 「同等アクセス」（P.39-9）
- 「ネクスト ホップの変更」（P.39-10）
- 「ACE の拒否」（P.39-10）

PBR の設定方法については、この章の「ポリシーベース ルーティング（PBR）の設定作業」を参照してください。

同等アクセス

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。スイッチにパケットの宛先に関する明示ルートが設定されていない場合は、送信元 1.1.1.1 からインターフェイス fastethernet 3/1 に到着したパケットが 6.6.6.6 にあるスイッチに送信されます。スイッチにパケットの宛先に関する明示ルートが設定されていない場合は、送信元 2.2.2.2 から到着したパケットが 7.7.7.7 にあるスイッチに送信されます。スイッチに宛先に関する明示ルートが設定されていないその他のパケットはすべて廃棄されます。

```
Switch (config)# access-list 1 permit ip 1.1.1.1
access-list 1 permit ip 1.1.1.1
!
interface fastethernet 3/1
 ip policy route-map equal-access
!
```

```
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 6.6.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 7.7.7.7
route-map equal-access permit 30
 set default interface null0
```

（注）　ドロップするパケットが最初の 2 つのルート マップ句のいずれとも一致しない場合は、**set default interface null0** を **set interface null0** に変更します。

ネクスト ホップの変更

次に、異なる送信元から異なる場所（ネクスト ホップ）へルーティングする例を示します。送信元 1.1.1.1 から着信したパケットは 3.3.3.3 にあるネクスト ホップに送信され、送信元 2.2.2.2 から着信したパケットは 3.3.3.5 にあるネクスト ホップへ送信されます。

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip next-hop 3.3.3.3
!
route-map Texas permit 20
 match ip address 2
 set ip next-hop 3.3.3.5
```

ACE の拒否

次に、指定されたルート マップ シーケンスの処理を停止し、次のシーケンスに飛ぶ例を示します。送信元 1.1.1.1 から着信したパケットは、シーケンス 10 をスキップしてシーケンス 20 に飛びます。サブネット 1.1.1.0 から着信する他のすべてのパケットは、シーケンス 10 の set 文に従います。

```
access-list 1 deny ip 1.1.1.1
access-list 1 permit ip 1.1.1.0 0.0.0.255
access-list 2 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 3/1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip next-hop 3.3.3.3
!
route-map Texas permit 20
match ip address 2
set ip next-hop 3.3.3.5
```