CHAPTER 32

PBR の設定

（注） PBR は Supervisor Engine 6-E ではサポートされて*いません*。

この章では、ルータ上での Policy-Based Routing（PBR; ポリシーベース ルーティング）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） この章のスイッチ　コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

（注） 機能に関するハードウェア　プラットフォームまたはソフトウェア　イメージの情報を確認するには、Cisco.com の Feature Navigator を使用してその機能に関する情報を検索するか、特定のリリースに対応するソフトウェア リリース ノートを参照してください。

PBR の概要

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 フローに定義ポリシーを設定し、ルートにおけるルーティング プロトコルへの依存度を軽くして、パケットのルーティングを柔軟に行えるようにします。このため PBR は、ルーティング プロトコルが提供する既存のメカニズムを拡張、補完することでルーティングの制御を強化します。PBR により、高コスト リンクにおけるプライオリティ 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、アプリケーション プロトコル、またはパケット サイズに基づいてパスの permit や deny を行うルーティング ポリシーを実装できます。

PBR を使用すると、次の作業が可能になります。

- 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。ポリシーを単純にするには、これらの記述子のいずれか 1 つを使用します。複雑なポリシーにするには、これらをすべて使用します。

PBR の概要

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 マップは文で構成されています。ルート マップ文は permit または deny とマークでき、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通じて送り返され、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。

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。

PBR フロー スイッチングの概要

Catalyst 4500 スイッチング エンジンは、[set next-hop] ルートマップ アクションと許可 Access Control List（ACL; アクセス コントロール リスト）のパケットとの照合をサポートします。その他すべてのルートマップ アクション（拒否 ACL の照合を含む）は、フロー スイッチング モデルによってサポートされています。このモデルでは、ルートマップに一致するフローの最初のパケットは、転送目的でソフトウェアに配信されます。ソフトウェアは、パケットの正しい宛先を判別し、Ternary CAM（TCAM）にエントリをインストールするので、そのあとのフローのパケットがハードウェアでスイッチングされるようになります。Catalyst 4500 スイッチング エンジンは、最大 4096 のフローをサポートします。

PBR の使用

PBR をイネーブルにして、特定のパケットのルーティング パスを最短と思われるパスから変更できます。たとえば、PBR は次のような機能を提供します。

- 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。

PBR の設定作業リスト

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。最初に説明する作業は必須で、そのあとの作業は任意です。この章の最後にある「PBR の設定例」を参照してください。

- PBR のイネーブル化（必須）
- ローカル PBR のイネーブル化（任意）

PBR のイネーブル化

PBR をイネーブルにするには、一致基準とすべての match コマンドが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、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。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 コマンド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]`	パケットが出力される場所を制御するルート 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	`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。1 つまたは複数の標準または拡張アクセス リストで許可された送信元および宛先 IP アドレスを照合します。
ステップ 3、4、5、または 6 を実行します。		
ステップ 3	`Switch(config-route-map)# set ip next-hop ip-address [... ip-address]`	基準と一致するパケットの動作を指定します。 パケットをルーティングするネクスト ホップを指定します（ネクスト ホップは隣接している必要があります）。この動作は、通常のルーティング テーブルで指定されているネクスト ホップと同じです。
	または	
ステップ 4	`Switch(config-route-map)# set interface interface-type interface-number [... type number]`	基準と一致するパケットの動作を指定します。 パケットの出力インターフェイスを設定します。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。インターフェイスは（スイッチ ポートではない）レイヤ 3 インターフェイスでなければならず、パケットの宛先アドレスはそのインターフェイスに割り当てられた IP ネットワーク内に存在している必要があります。パケットの宛先アドレスがネットワークにない場合、パケットはドロップされます。
	または	
ステップ 5	`Switch(config-route-map)# set ip default next-hop ip-address [... ip-address]`	基準と一致するパケットの動作を指定します。 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。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。
	または	

	コマンド	目的
ステップ 6	`Switch(config-route-map)# set default interface interface-type interface-number [...type ...number]`	基準と一致するパケットの動作を指定します。 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。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出力インターフェイスに転送されます。パケットの宛先アドレスがネットワークにない場合、パケットはドロップされます。
ステップ 7	`Switch(config-route-map)# interface interface-type interface-number`	インターフェイスを設定します。このコマンドを入力すると、ルータはインターフェイス コンフィギュレーション モードになります。
ステップ 8	`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、一致するものが見つかるまでシーケンス番号順に評価されます。一致するものがない場合、パケットは通常どおり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 ルータがネクスト ホップを見つけ、それが使用可能なインターフェイスである場合、ローカル ルータはパケットをルーティングします。

ローカル PBR のイネーブル化

ルータ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。これらのパケットのためのローカル PBR をイネーブルにするには、ルータが使用すべきルート マップを示すために、次の作業を行います。

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、ルータから発信されたパケットはすべて、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。

サポートされない機能

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（コマンドライン インターフェイス）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**

PBR の設定例

ここでは、PBR の設定例を示します。

- 同等アクセス例（p.32-6）
- ネクスト ホップを変更する例（p.32-7）
- ACE の拒否例（p.32-7）

PBR の設定方法については、この章の「PBR の設定作業リスト」を参照してください。

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 1.1.1.1 からインターフェイス FastEthernet 3/1 に着信したパケットは、6.6.6.6 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 2.2.2.2 から着信したパケットは、7.7.7.7 にあるルータへ送信されます。ルータに宛先の明示パスがない他のすべてのパケットは廃棄されます。

```
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 route-map 句と一致しない場合、**set default interface null0** を **set interface null0** に変更します。

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 の拒否例

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
```