IPv4 ポリシーベースルーティングの設定

ポリシーベース ルーティングの概要

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

PBR（ポリシーベースルーティング）は、設定されたポリシーに基づいてルーティングを決定するために使用される技術です。

ルータまたはスイッチがパケットを受信すると、転送の判断はパケットの宛先 IP アドレスに基づいて行われます。宛先 IP アドレスは、ルーティングテーブルのエントリの検索に使用されます。ただし、場合によっては、宛先 IP アドレスではなく送信元 IP アドレスなど、他の基準に基づいてパケットを転送する必要があります。そうすることで、宛先が同じ場合でも、異なる送信元から送信されるパケットを別のネットワークにルーティングできます。これは、複数のプライベートネットワークを相互接続する場合に役立ちます。

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 ip address acl1 acl2

  match ip address acl3

  （注） IPv6 はサポートされていません。

  パケットは、acl1、acl2、または acl3 で許可されている場合に許可されます。

  - 下された判断が許可の場合は、set コマンドで指定されたアクションがパケットに適用されます。
  - 下された判断が拒否の場合は、PBR アクション（set コマンドで指定）は適用されません。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と ACL はサポートされません。

標準 IP ACL を使用すると、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。優先順位番号または名前を使用して IP 優先順位値を設定することもできます。

ポリシーベースルーティングに関する注意事項と制約事項

- PBR を使用するには、スイッチ上で Network Advantage ライセンスを有効にしておく必要があります。
- デフォルトでは、ポリシーベースルーティング（PBR）はスイッチ上で無効になっています。PBR は、ルートマップが設定され、インターフェイスに適用されると有効になります。

- スイッチ（CPU）で生成されたパケットまたはローカルパケットは、通常どおりにポリシールーティングされません。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ユニキャストパケットがローカル PBR の影響を受けます。ローカルPBRに関してサポートされているプロトコルは、NTP、DNS、MSDP、SYSLOG、およびTFTP です。ローカルPBRは、デフォルトで無効に設定されています。
- PBR には、**route-map deny** ステートメントはサポートされません。
- ACL と拒否 ACE との照合はサポートされていません。
- 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。
- 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。
- ポリシールートマップが ACL および QoS とともにインターフェイスに適用される場合、ACL と QoS が優先されます。
- ルールが同じインターフェイス上の PBR ルールと一致する場合、IP ソースガードの優先順位が高くなります。
- SVI インターフェイスでは、IP ソースガードと PBR ルールが要件に基づいてマージされます。
- 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。
- スイッチには最大 64 個の IP ポリシー ルート マップを定義できます。
- スイッチには、PBR 用として最大 64 個のアクセス コントロール エントリ（ACE）を定義できます。
- 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。エントリの最大数は 256 です。
- 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。
- WCCP と PBR は、スイッチ インターフェイス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、WCCPを有効にできません。その反対の場合も同じで、WCCP 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。
- 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。

- 単一のシーケンスルートマップでは、一度に 1 つの set 句のみがサポートされます。複数のシーケンスを持つルートマップでは、同じタイプの set 句のみが許可されます。たとえば、**set ip next-hop** が最初のシーケンスで使用される場合、2 番目のシーケンスにも同じ set 句 **set ip next-hop** が必要になります。
- 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。一致パケット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パケットに適用されます。

次の表に、スイッチの ACL [Match Field] オプションに対する PBR のサポートを示します。

表 *1 : PBR* でサポートされる *ACL [Match Field]* オプション

Match Field	**サポート対象（Y/N）**
Source IP address	Y
Destination IP address	Y
Next Header（ICMP、IGMP など）	N
TCP/UDP Port	N
Type of Service（TOS）	N
Fragmentation Bit	N

次の表に、スイッチでサポートされる PBR 機能を示します。

表 *2 : PBR* 機能のサポート

機能	**サポート/スケール**
入力トラフィックの PBR	Y
出力トラフィックの PBR	N
物理インターフェイス（L2 ポート）の PBR	N
物理インターフェイス（ルーテッドポート）の PBR	Y
SVI インターフェイスの PBR	Y
ポートチャネル（L2）の PBR	N
ポートチャネル（L3）の PBR	N
VRF を使用した PBR	N

機能	サポート/スケール
IPv4 ACL の照合	Y （注） PBR でサポートされる ACL [Match Field] オプションについては、上記の表を参照してください。
拡張/標準 IPv4 ACL の照合	Y
パケット長に基づいた照合	N
拒否 ACE との照合	N
フラグメントビットを設定するアクション	N
優先順位を設定するアクション	N
ネクストホップを設定するアクション	Y
再帰的ネクストホップアクション	N
インターフェイスを設定するアクション	N
デフォルトインターフェイスを設定するアクション	N
IP 優先順位を設定するアクション	Y
IP VRF を設定するアクション	Y
IP デフォルトネクストホップの設定	N
IP デフォルト VRF の設定	N
マルチキャストトラフィックの PBR	N
IPv6 トラフィックの PBR	N
ルートマップ拒否	N
サポートされるルートマップの最大数	64
サポートされる ACL ポリシーの最大数	64
ローカル PBR	Y

PBR の設定方法

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。

始める前に

ポリシーベースルーティングに関する注意事項と制約事項（2ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**route-map** *map-tag* [**permit**] [*sequence number*] 例： `Device(config)# route-map pbr-map permit`	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。 • *map-tag* — ：ルートマップ用のわかりやすい名前を指定します。 **ip policy route-map** 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 map-tag がある複数の route-map 文は、1 つの route-map を定義します。 •（任意） **permit** — ： **permit** 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、set 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。 •（任意） *sequence number* — ：シーケンス番号は、特定のルートマップ内の route-map ステートメントの位置を示します。

	コマンドまたはアクション	目的
ステップ 4	**match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* |*...access-list-name*] 例： `Device(config-route-map)# match ip address 110 140`	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。 **match** 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 5	**set ip next-hop** *ip-address* [*...ip-address*] 例： `Device(config-route-map)# set ip next-hop 10.1.6.2`	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）。
ステップ 6	**set ip vrf** *vrf-name* **next-hop** *ip-address* [*...ip-address*] 例： `Device(config-route-map)# set ip vrf myvrf next-hop 10.5.5.5`	VRF インターフェイスにポリシーベースルーティングを適用できます。
ステップ 7	**set ip precedence** [*number* | *name*] 例： `Device(config-route-map)# set ip precedence 5`	• 0：routine • 1：priority • 2：immediate • 3：flash • 4：flash-override • 5：critical • 6：internet • 7：network IP ヘッダーに優先順位を設定します。
ステップ 8	**exit** 例： `Device(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 9	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/1`	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 10	**ip policy route-map** *map-tag* 例： `Device(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

	コマンドまたはアクション	目的
		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 11	**exit** 例： `Device(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	**ip local policy route-map** *map-tag* 例： `Device(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	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show route-map** [*map-name*] 例： `Device# 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	**show ip policy** 例： `Device# 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。
ステップ 16	**show ip local policy** 例： `Device# 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。