ポリシーベース ルーティングの設定

この章では、Cisco NX-OS デバイスでポリシー ベース ルーティングを設定する方法について説明します。

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

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 3600 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 3600 プラットフォーム 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 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。

ルート マップ処理ロジック

ルートマップが設定されたインターフェイスでパケットが受信されると、転送ロジックはシーケンス番号に従って各ルート 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 内の許可 ACE と一致する場合、ポリシーベース ルーティング ロジックはパケットに対して set コマンドで指定されたアクションを実行します。

ルート マップ文に route-map... 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、ネクストホップが ECMP パス上で再帰的である場合、Cisco Nexus 36180YC-R スイッチ上でポリシーベース ルーティング トラフィックを分散できます。すべてのネクストホップ ルーティング要求については、ルーティング プロファイル マネージャ (RPM) がユニキャスト ルーティング情報ベース (uRIB) を使用してそれらを解決し、すべての ECMP パスをプログラムします。これにより、すべての ECMP パスの負荷が均一に分散されます。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 フィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

ポリシーベースのルーティング ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 送信元アドレスおよび/または宛先アドレス
- TCP/UDP ポート

ポリシーベース ルーティングの前提条件

追加のオプションを使用してトラフィックを識別できます。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

ポリシーベースのルーティング ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 送信元アドレスおよび/または宛先アドレス
- TCP/UDP ポート

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。

- Cisco NX-OS リリース 7.0(3)F3(3) 以降、Cisco Nexus 3600 プラットフォーム スイッチは IPv4 および IPv6 ポリシーベース ルーティングをサポートします。これらのスイッチの場合、PBR ポリシーは、接続されているルートおよびローカル ルートよりも高い優先度を持ちます。プロトコル ネイバーが直接接続されている場合は、明示的な許可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。
- 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。
- レイヤ 3 ポート チャネル サブインターフェイスによるポリシーベース ルーティングがサポートされます。
- 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。
- ネクストホップが ECMP パス上で再帰的である場合、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はできません。代わりに、 **set {ip | ipv6} next-hop** *ip-address* **load-share** コマンドを使用して隣接ネクスト ホップを指定します。
- ポリシーベース ルーティングは、VXLAN で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 ポリシー統計情報はサポートされていません。

デフォルト設定

下の表に、ポリシーベース ルーティング パラメータのデフォルト設定を示します。

表 *1:* 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	無効化

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	[**no**] **feature pbr** 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 no 形式を使用します。 （注） no feature pbr 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） **show feature** 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） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	[**no**] **feature pbr** 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 **no** 形式を使用します。 （注） **no feature pbr** 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） **show feature** 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	**[no] hardware profile pbr ecmp paths max-paths**
	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。PBR ECMP 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	**show system internal rpm state**	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。

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。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. { **ip** | **ipv6** } **policy route-map** *map-name*
4. **route-map map-name [permit | deny] [seq]**
5. **match** {**ip** | **ipv6**} **address access-list-name** *name* [*name...*]
6. （任意） **set ip next-hop** *address1* [*address2...*] **[load-share] [drop-on-fail]**
7. **set ipv6 next-hop** *address1* [*address2...*]**[load-share] [drop-on-fail]**
8. （任意） **set ip next-hop verify-availability**
9. （任意） **set interface null0**
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	{ **ip** | **ipv6** } **policy route-map** *map-name* 例： `switch(config-if)# ip policy route-map Testmap`	IPv4 または 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 4	**route-map map-name [permit | deny] [seq]**
	例：
	`switch(config-if)# route-map Testmap`
	`switch(config-route-map)#`
		ルート マップを作成するか、または既存のルートマップに対応するルート マップ設定モードを開始します。seq を使用して、ルート マップ エントリを順序付けます。

	コマンドまたはアクション	目的
ステップ 5	**match** {**ip** | **ipv6**} **address access-list-name** *name* [*name...*] 例： `switch(config-route-map)# match ip address access-list-name ACL1`	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。
ステップ 6	（任意） **set ip next-hop** *address1* [*address2...*] **[load-share] [drop-on-fail]** 例： `switch(config-route-map)# set ip next-hop 192.0.2.1`	ポリシーベース ルーティング用の 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。 任意の **load-share** 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。 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 **drop-on-fail** キーワードを使用してパケットをドロップできます。
ステップ 7	**set ipv6 next-hop** *address1* [*address2...*]**[load-share] [drop-on-fail]** 例： `switch(config-route-map)# set ipv6 next-hop 2001:0DB8::1`	ポリシーベース ルーティング用の 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。 任意の **load-share** 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。 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 **drop-on-fail** キーワードを使用してパケットをドロップできます。
ステップ 8	（任意） **set ip next-hop verify-availability**	`switch(config-route-map)# set ip next-hop verify-availability` 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。
ステップ 9	（任意） **set interface null0** 例： `switch(config-route-map)# set interface null0`	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 null0 インターフェイスを使用します。

	コマンドまたはアクション	目的
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	この設定変更を保存します。

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
show [ip | ipv6] policy [*name*]	IPv4 または IPv6 ポリシーに関する情報を表示します。

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。

```
ip access-list pbr-sample
permit tcp host 10.1.1.1 host 192.168.2.1 eq 80
!
route-map pbr-sample
match ip address pbr-sampl
set ip next-hop 192.168.1.1
!
route-map pbr-sample
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
Set clauses:

ip next-hop 192.168.1.1
switch# show ip policy
Interface Route-map Status VRF-Name
Ethernet1/2 pbr-sample Active --
```

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
```

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。