拡張型ポリシーベースルーティング

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1*：機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN の拡張版ポリシーベースルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	このリリースでは、拡張版ポリシーベースルーティング（ePBR）が Cisco Catalyst SD-WAN に拡張されています。 ePBR は、トラフィックフローの柔軟なポリシーに基づいてトラフィックをルーティングする、プロトコルに依存しないトラフィック ステアリング メカニズムです。ePBR ポリシーの作成には、Cisco SD-WAN Manager の CLI アドオンテンプレートを使用できます。

- ePBR の概要 （2 ページ）
- ePBR の設定 （3 ページ）
- ePBR のモニター （7 ページ）

ePBR の概要

拡張ポリシーベースルーティング（ePBR）は、ポリシーベースルーティング（PBR）の高度なバージョンです。この機能を使用すると、トラフィック転送はルーティングテーブルではなくポリシーに基づいて行われるため、ルーティングをより詳細に制御できます。ePBR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および補完し、IPv4およびIPv6アドレス、ポート番号、プロトコル、パケットサイズなどの柔軟な一致基準に基づいてトラフィックをルーティングする、高度なローカルデータポリシーです。

ePBR は、柔軟性の高い Cisco Common Classification Policy Language（C3PL 言語）を使用してトラフィックを照合します。プレフィックス、アプリケーション、Differentiated Services Code Point（DSCP; DiffServ コードポイント）、セキュリティグループタグ（SGT）などの照合をサポートします。ePBR ではマッチ条件に基づいて、トラフィック転送用に単一または複数のネクストホップを設定できます。また、インターネット プロトコル サービス レベル契約（IP SLA）トラッキングを設定するオプションもあります。設定されたネクストホップが使用できない場合、トラフィックは IP SLA トラッカーによって有効にされたダイナミックプローブを介して、使用可能なネクストホップにルーティングされます。

機能と利点

- IPv4 と IPv6 の両方をサポートします。
- 複数のネクストホップをサポートします。ネクストホップに到達できない場合、ePBR は次に利用可能なネクストホップに自動的に切り替えます。
- IP SLA トラッキングを設定するオプションがあります。これが設定されている場合、ネクストホップは IP SLA プローブが成功した場合にのみ選択されます。

  SLA プローブは、同じ VRF または異なる VRF で設定できます。
- 現在のホップに到達できない場合はsyslogメッセージが生成され、ユーザーに通知されます。

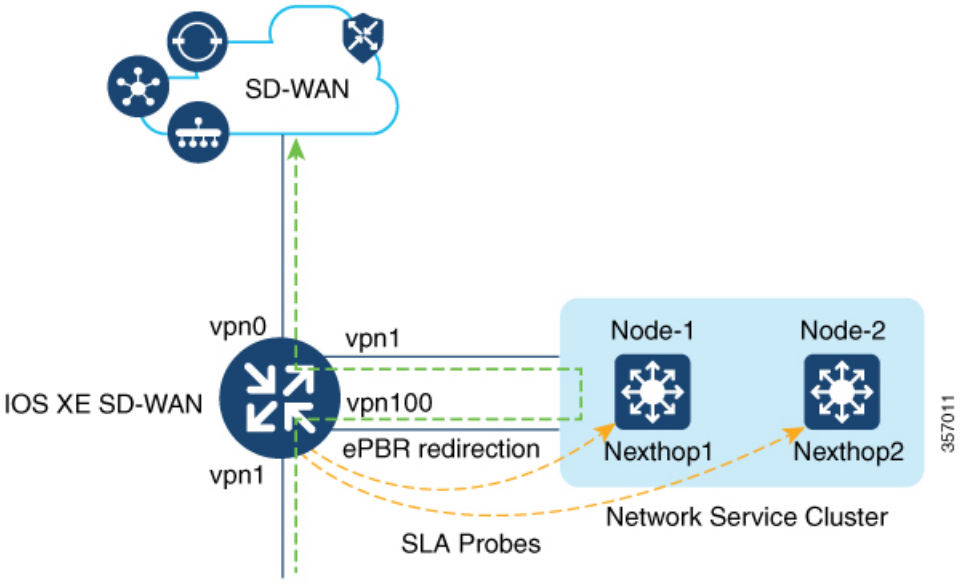
ePBR の仕組み

- ePBRはユニキャストルーティングにのみ適用され、C3PLを使用したトラフィック照合に基づきます。
- ePBR 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、ポリシーマップを通過します。ePBR で使用するポリシーマップはポリシーを規定し、パケットの転送先を判断します。
- ePBRポリシーは、トラフィックフローに適用される分類基準（match）とアクション基準（set）に基づきます。
- ePBR を有効にするには、パケットの一致基準と目的のポリシールーティング アクションを指定するポリシーマップを作成する必要があります。次に、そのポリシーマップを必要なインターフェイスに関連付けます。

- 一致基準は、クラスで指定されます。その後、ポリシーマップはクラスを呼び出し、set ステートメントに基づいてアクションを実行します。
- ePBR ポリシーの set ステートメントは、ネクストホップ、DSCP、VRF などの観点からルートを定義します。

使用例

図 *1 : ePBR* を使用したトラフィックのリダイレクト



この例は、トラフィックがVPN1インターフェイスに着信することを示しています。トラフィックは VPN 1 で設定された分類に基づき、通常のルート転送をオーバーライドして VPN 100 のネクストホップにリダイレクトされます。トラフィックが VPN 100 にリダイレクトされると、追加のネットワークサービスが着信トラフィックに適用されます。WAN 最適化などのネットワークサービスは、リダイレクトされたトラフィックに適用された後、VPN 0 を介して Cisco Catalyst SD-WAN オーバーレイネットワークに転送されます。

ePBR の設定

Cisco SD-WAN Manager を使用して ePBR を設定するには、CLI アドオン機能テンプレートを作成し、デバイステンプレートに添付します。

このセクションでは、CLI アドオンテンプレートに追加できる ePBR の設定例を示します。

IPv4 での ePBR の設定

この例では、次のようになります。

- 拡張 ACL は、ネットワークまたはホストを定義します。
- クラスマップでは、ACL のパラメータを照合します。
- ePBR を使用したポリシーマップは、設定された set ステートメントに基づいて詳細なアクションを実行します。
- 複数のネクストホップが設定されています。ePBR は使用可能な最初のネクストホップを選択します。

```
ip access-list extended test300
 100 permit ip any 192.0.2.1 0.0.0.255
ip access-list extended test100
 100 permit ip any 192.0.2.20 0.0.0.255
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test1
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 10.0.0.2 10.0.40.1 10.0.50.1 ...
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 10.10.0.2 10.20.20.2 10.30.30.2 ...
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

IPv4 トラッキングの設定

トラッキングとともに ePBR を設定する例を次に示します。この例では次の動作になります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。
- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- `set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2` の番号 10 は、シーケンス番号を表します。

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip access-list extended test300
 100 permit ip any 10.10.0.2 0.0.0.255
ip access-list extended test100
 100 permit ip any 10.10.0.3 0.0.0.255
```

```
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

IPv6 での ePBR の設定

この例では、次のようになります。

- 拡張 ACL は、ネットワークまたはホストを定義します。
- クラスマップは、ACL のパラメータを照合するために使われます。
- ePBR を使用したポリシーマップは、設定された set ステートメントに基づいて詳細なアクションを実行します。.
- 単一または複数のネクストホップアドレスを設定できます。 ePBR は、使用可能な最初のネクストホップアドレスを選択します。

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB81::/32
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001:DB82::/32
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2001:DB8::1
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001:DB8::2 2001:DB8:FFFF:2 ...
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

IPv6 トラッキングの設定

IPv6 の ePBR を設定し、トラッキングを有効にする例を次に示します。この例では、次のようになります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。

- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- トラッキングは、IP SLA の結果が使用できない場合、クラスで設定されたネクストホップにパケットが送信されないように設定されます。

```
ip sla 3
  icmp-echo 2001:DB8::1
  vrf 100
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip sla 4
  icmp-echo 2001:DB8::2
  vrf 300
ip sla schedule 4 life forever start-time now
track 4 ip sla 4 state
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB8::/32
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any  2001:DB8::1/32
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop verify-availability 2001:DB8::2 10 track 4
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop verify-availability 2001:DB8::1 10 track 3
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

複数のネクストホップと SLA トラッキングを使用した IPv4 での ePBR の設定

この例では、次のようになります。

- ICMP エコータイプの IP SLA 動作が設定され、ACL が定義されます。
- その後、クラスマップを使用して ACL 内のパラメータを照合し、ポリシーマップは設定された set ステートメントに基づいてアクションを実行します。
- ネクストホップに対するトラッキングの設定は、前の IP アドレスが到達不能であり、IP SLA がネクストホップを到達可能であると確認した場合、パケットはネクストホップアドレスに流れます。

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip sla 3
  icmp-echo 10.20.0.2
```

```
  vrf 400
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip access-list extended test300
 100 permit ip any 192.0.2.1  255.255.255.0
ip access-list extended test100
 100 permit ip any 192.0.2.10 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
  set ipv4 vrf 400 next-hop verify-availability 10.20.0.2 11 track 3
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
!
```

（注） ネクストホップがトラッカーとともに設定されているとき、ネクストホップが到達不能であるか、または IP SLA が失敗した場合、次に使用可能なホップが選択されます。つまり、トラッカーが設定された場合、ネクストホップの可用性と IP SLA の結果の両方がチェックされることになります。

ePBR のモニター

ePBR は Cisco SD-WAN Manager ではモニタリングできません。設定の確認や、ePBR 統計情報のモニタリングを行うには、以下の show コマンドを使用します。

ネクストホップの可用性の確認

show platform software epbr track コマンドの出力例を次に示します。

```
Device# show platform software epbr track
Track Object:
obj num:2:
  track:0x7F94B4376760
   seq:10, nhop:123.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE240,
   global:0, vrf_name:300, track_reachable:1
   parent:0x7F94B4383778, oce:0x7F94B81193A8
obj num:1:
  track:0x7F94B8187810
   seq:10, nhop:100.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE1D0,
   global:0, vrf_name:100, track_reachable:1
   parent:0x7F94B8187778, oce:0x7F94B81188B8
```

この例では nhop_reachable の値は 1 で、ネクストホップが到達可能であることを示します。track_reachable は SLA プローブの結果を表し、値は 1 で、ネクストホップが到達可能であることを示します。ネクストホップに到達できない場合、これらのパラメータの値は 0 になります。

ネクストホップの設定の表示

show platform software epbr R0 feature-object redirect でネクストホップの設定を表示します。

（注） 出力を表示するには、トラッカーを設定する必要があります。

```
Device# show platform software epbr r0 feature-object redirect
FMAN EPBR Redirect Feature Objectep

Feature Object ID: 9876543211
  Flags: 0x3
  Table ID: 0x4
  Next-hop: 10.10.10.2
  P2P ADJ-ID: 0

Feature Object ID: 1234567890
  Flags: 0x3
  Table ID: 0x2
  Next-hop: 172.16.0.0
  P2P ADJ-ID: 0
```

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。