BGP フロースペックの実装

フロースペックは、任意のアプリケーションで使用できるボーダー ゲートウェイ プロトコルのネットワーク層到達可能性情報（BGP NLRI）として BGP を介してフロー仕様ルールを配布する手順を指定し、フロー仕様ルールを符号化するための手順を定義します。また、（分散型）サービス妨害攻撃を軽減するためのパケットフィルタリングを目的とするアプリケーションも定義します。

（注） このモジュールに示されている BGP フロースペックの詳細と BGP フロースペックのコマンドに関する詳細な説明については、*Routing Command Reference for Cisco ASR 9000 Series Routers* の「*BGP Flowspec Commands*」の章を参照してください。

BGP フロースペックの実装の機能履歴

リリース 5.2.0	この機能が導入されました。
リリース 5.3.2	BGP フロースペックでの NLRI ポリシーのサポート

• BGP フロー仕様 （1 ページ）

BGP フロー仕様

BGP フロー仕様（フロースペック）機能を使用すると、多数の BGP ピアルータ間でフィルタリングおよびポリシング機能を迅速に展開および伝達して、ネットワーク上で分散型サービス妨害（DDoS）攻撃の影響を軽減できます。

RTBH（リモートでトリガーされたブラックホール）などの DDoS 攻撃の軽減に対する従来の方法では、特別なコミュニティを使用して攻撃を受けている Web サイトのアドレスのアドバタイズに BGP ルートが挿入されます。境界ルータ上のこの特別なコミュニティは、ネクストホップを破棄またはヌルにするための特殊なネクストホップに設定します。これにより、疑わ

しい送信元からネットワークへのトラフィックが防止されます。これによって優れた保護がもたらされますが、サーバは完全に到達不能になります。

一方、BGP フロースペックでは、よりきめ細やかなアプローチを可能にし、送信元、宛先、L4 パラメータ、および長さ、フラグメントなどのパケットの詳細と特定のフローを照合するための手順を効果的に構築できるようにします。フロースペックでは、境界ルータで次のいずれかのアクションを動的にインストールできます。

- トラフィックをドロップする
- 分析のために別の VRF にトラフィックを挿入する、または
- トラフィックを許可する一方で、定義された特定のレートでポリシングする

そのため、ルートポリシー言語でドロップするために境界ルータをネクストホップに関連付ける必要がある特別なコミュニティを使用してルートを送信する代わりに、BGP フロースペックは特定のフロー形式を境界ルータに送信し、クラスマップとポリシーマップを使用してある種の ACL を作成するように指示して、アドバタイズするルールを実装します。これを実現するため、BGP フロースペックは BGP プロトコルに新しい NLRI（ネットワーク層到達可能性情報）を追加します。BGP フロースペックの実装に関する情報 （4 ページ）に、フロー仕様、サポートされている一致基準、およびトラフィックのフィルタリングアクションの詳細を示します。

フロースペックは、RPL を使用したフロースペック NLRI の送信元と宛先に基づいてフィルタリングでき、また、ネイバーの接続点に適用できます。

制限事項

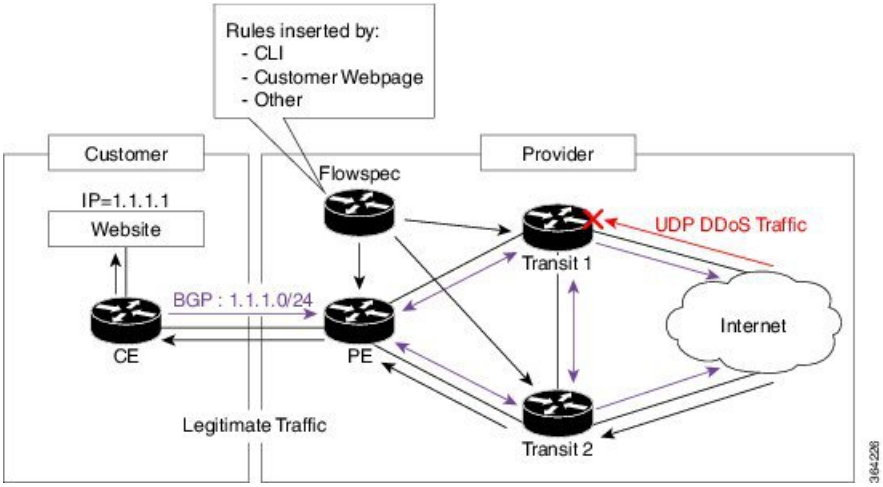
BGP フロースペックには、次の制限が適用されます。

- フロースペックは、次の Cisco ASR 9000 第 1 世代イーサネットラインカードではサポートされていません。
  - A9K-40G（40 ポート 10/100/1000）
  - A9K-4T（4 ポート 10GE）
  - A9K-2T20G（コンボカード）
  - A9K-8T/4
  - A9K-8T
  - A9K-16T/8（16 ポート 10GE）
- フロースペックは、サブスクライバとサテライトインターフェイスではサポートされていません。
- フロースペックルールでは、最大 5 つの複数値の範囲を指定できます。
- フロースペックルールでは、アドレスファミリを混在させることはできません。

- 複数の一致シナリオでは、最初に一致したフロースペックルールのみが適用されます。
-
- QoS は BGP フロースペックよりも優先されます。
- BGP フロースペックは、マルチキャストまたは MPLS トラフィックをサポートしていません。

BGP フロースペックの概念アーキテクチャ

次の図では、フロースペックルータ（コントローラ）はフロー（一致基準とアクション）を使用してプロバイダーエッジ上に設定されています。フロースペックルータは、これらのフローを他のエッジルータと AS（つまり、Transit 1、Transit 2、および PE）にアドバタイズします。これらの中継ルータは、フローをハードウェアにインストールします。フローがハードウェアにインストールされると、中継ルータはルックアップを実行して、着信トラフィックが定義されたフローと一致するかどうかを確認し、適切なアクションを実行することができます。このシナリオでのアクションは、ネットワーク自体のエッジにある DDoS トラフィックを「ドロップ」し、カスタマーエッジにクリーンで正当なトラフィックのみを配信することです。



この項では、フロースペックの機能に関する CLI 設定の例を示します。最初に、フロースペックルータで、着信トラフィックに対して実行する一致アクションの基準を定義します。これには、設定の PBR の部分が含まれています。**service-policy type** で、実際の PBR ポリシーを定義し、フロースペックに追加する必要がある一致とアクション基準の組み合わせを含んでいます。この例では、ポリシーはアドレスファミリ IPv4 の下に追加されるため、IPv4 フロースペックルールとして伝達されます。

```
Flowspec router CLI example:

class-map type traffic match-all cm1
     match source-address ipv4 100.0.0.0/24

policy-map type pbr pm1
    class type traffic cm1
      drop
```

```
flowspec
    address-family ipv4
       service-policy type pbr pm0

Transient router CLI:

flowspec
    address-family ipv4
       service-policy type pbr pm1
```

フロースペックの設定に使用する手順の詳細とコマンドについては、ePBR を使用した BGP フロースペックの設定 （13 ページ）を参照してください。

BGP フロースペックの実装に関する情報

BGP フロースペックを実装するには、次の概念を理解する必要があります。

フロー仕様

フロー仕様は、IP トラフィックに適用可能な複数の一致基準から成る n タプルです。特定の IP パケットは、指定されたすべての基準に一致する場合に、定義されたフローと一致していると見なされます。特定のフローは、特定のアプリケーションに応じて、属性のセットに関連付けることができます。このような属性には、到達可能性情報（つまり、NEXT_HOP）が含まれている場合と含まれていない場合があります。

どのフロー固有ルートも、実質的にはルールであり、一致部分（NLRI フィールドで符号化）とアクション部分（BGP 拡張コミュニティとして符号化）から構成されています。BGP フロースペックルールは、一致パラメータとアクションパラメータを表す同等の C3PL ポリシーに内部的に変換されます。一致とアクションのサポートは、基盤となるプラットフォーム ハードウェア機能によって異なります。サポートされている一致基準とアクション （4 ページ）およびトラフィック フィルタリング アクション （9 ページ）で、サポートされている一致（タプル定義）パラメータとアクションパラメータについて説明します。

サポートされている一致基準とアクション

フロー仕様 NLRI タイプには、宛先プレフィックス、送信元プレフィックス、プロトコル、ポートなどの複数のコンポーネントが含まれている場合があります。この NLRI は、BGP によって不透明ビット文字列プレフィックスとして処理されます。各ビット文字列は、一連の属性を関連付けることができるデータベースエントリのキーを識別します。この NLRI 情報は、MP_REACH_NLRI 属性と MP_UNREACH_NLRI 属性を使用してエンコードされます。対応するアプリケーションがネクストホップ情報を必要としない場合は常に、MP_REACH_NLRI 属性で 0 オクテット長のネクストホップとしてエンコードされ、受信時に無視されます。MP_REACH_NLRI と MP_UNREACH_NLRI の NLRI フィールドは、その後に可変長 NLRI 値が続く 1 オクテットまたは 2 オクテットの NLRI 長フィールドとしてエンコードされます。NLRI の長さはオクテットで表されます。

フロー仕様 NLRI タイプはオプションの複数のサブコンポーネントで構成されます。特定のパケットがフロースペックと一致すると見なされるのは、そのスペック内に存在するすべてのコ

ンポーネントの共通点（AND）に合致する場合です。定義できるサポート対象コンポーネントのタイプまたはタプルを次に示します。

タプル定義の可能性

BGP フロースペック NLRI タイプ	QoS 一致フィールド	説明とシンタックスの構築	値の入力方法
タイプ 1	IPv4 または IPv6 の宛先アドレス	照合する宛先プレフィックスを定義します。プレフィックスは、BGP UPDATE メッセージで、プレフィックス情報を格納するための十分なオクテットが続く長さでエンコードされます。 エンコーディング：<type (1 octet), prefix length (1 octet), prefix> **構文**： **match destination-address** {**ipv4** | **ipv6**} *address/mask length*	プレフィックス長
タイプ 2	IPv4 または IPv6 の送信元アドレス	照合する送信元プレフィックスを定義します。 エンコーディング：<type (1 octet), prefix-length (1 octet), prefix> **構文**： **match source-address** {**ipv4** | **ipv6**} *address/mask length*	プレフィックス長
タイプ 3	IPv4 最終ネクストヘッダーまたは IPv6 プロトコル	IP パケットの IP プロトコル値バイトとの照合に使用する {operator, value} ペアのセットが含まれています。 エンコーディング：<type (1 octet), [op, value]+> **構文**： タイプ 3： **match protocol** {*protocol-value* | *min-value* −*max-value*}	複数値の範囲

タイプ 4	IPv4 または IPv6 の送信元ポートまたは宛先ポート	送信元または宛先の TCP/UDP ポートと照合する {operation, value} ペアのリストを定義します。値は、1 バイトまたは 2 バイトの数量としてエンコードされます。パケットの IP プロトコル フィールドに TCP または UDP 以外の値がある場合、パケットがフラグメント化されていて最初のフラグメントではない場合、またはシステムがトランスポートヘッダーを見つけることができない場合は、ポート、送信元ポート、および宛先ポートの各コンポーネントは、FALSE と評価されます。 1 つの一致文字列でサポートされるポート番号は最大 5 つです。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match source-port** {*source-port-value* | *min-value* **-** *max-value*} **match destination-port** {*destination-port-value* | *min-value* **-** *max-value*}	複数値の範囲
タイプ 5	IPv4 または IPv6 の宛先ポート	TCP パケットまたは UDP パケットの宛先ポートの照合に使用する {operation, value} ペアのリストを定義します。値は、1 バイトまたは 2 バイトの数量としてエンコードされます。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match destination-port** {*destination-port-value* | [*min-value* **-** *max-value*]}	複数値の範囲

タイプ 6	IPv4 または IPv6 の送信元ポート	TCP パケットまたは UDP パケットの送信元ポートの照合に使用する {operation, value} ペアのリストを定義します。値は、1 バイトまたは 2 バイトの数量としてエンコードされます。 1 つの一致文字列でサポートされるポート番号は最大 5 つです。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match source-port** {*source-port-value* | [*min-value* **-** *max-value*]}	複数値の範囲
タイプ 7	IPv4 または IPv6 の ICMP タイプ	ICMP パケットのタイプフィールドの照合に使用する {operation, value} ペアのリストを定義します。値は、1 バイトを使用してエンコードされます。ICMP タイプとコード指定子は、プロトコル値が ICMP ではない場合は常に FALSE と評価されます。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match** {**ipv4** | **ipv6**} **icmp-type** {*value* | *min-value* *-max-value*}	単一の値 （注） 複数の値の範囲はサポートされていません。
タイプ 8	IPv4 または IPv6 の ICMP コード	ICMP パケットのコードフィールドの照合に使用する {operation, value} ペアのリストを定義します。値は、1 バイトを使用してエンコードされます。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match** {**ipv4** | **ipv6**} **icmp-code** {*value* | *min-value* *-max-value*}	単一の値 （注） 複数の値の範囲はサポートされていません。

タイプ 9	IPv4 または IPv6 の TCP フラグ（2 バイトに予約ビットを含む） （注） 予約済みビットと NS ビットはサポートされていません	ビットマスク値は、1 バイトまたは 2 バイトのビットマスクとしてエンコードできます。1 バイトが指定されている場合は、TCP ヘッダーのバイト 13 に一致します。これには、4 番目の 32 ビットワードのビット 8 ～ 15 が含まれています。2 バイトエンコーディングが使用されている場合、TCP ヘッダーのバイト 12 と 13 は、「don't care」値を持つデータオフセットフィールドと一致します。ポート指定子と同様に、このコンポーネントは、TCP パケットではないパケットについては FALSE と評価します。このタイプは、ビットマスクオペランド形式を使用します。これは、下位ニブルの数値演算子形式とは異なります。 エンコーディング：<type (1 octet), [op, bitmask]+> **構文**： **match tcp-flag** *value* **bit-mask** *mask_value*	ビット マスク
タイプ 10	IPv4 または IPv6 のパケット長	IP パケットの合計長（レイヤ 2 を除くが、IP ヘッダーを含む）に一致します。値は、1 バイトまたは 2 バイトの数量を使用してエンコードされます。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **matchpacket length** {*packet-length-value* | *min-value* *−max-value*}	複数値の範囲

タイプ 11	IPv4 または IPv6 の DSCP	6 ビット DSCP フィールドの照合に使用する {operation, value} ペアのリストを定義します。値は 1 バイトを使用してエンコードされます。この場合、最上位 2 ビットがゼロで、最下位 6 ビットに DSCP 値が含まれています。 エンコーディング：<type (1 octet), [op, value]+> **構文**： **match dscp** {*dscp-value* | *min-value* **-***max-value*}	複数値の範囲
タイプ 12	IPv4 または IPv6 のフラグメンテーションビット	クラスマップの一致基準としてフラグメントタイプを識別します。 エンコーディング：<type (1 octet), [op, bitmask]+> **構文**： **match fragment type** [**is-fragment**]	ビット マスク

特定のフロースペックルールでは、制約事項なしに複数のアクションの組み合わせを指定できます。ただし、一致基準とアクション間でのアドレスファミリの混在は許可されていません。たとえば、IPv4 のマッチングを IPv6 のアクションと組み合わせることはできず、その逆も同様です。

（注） リダイレクト IP ネクストホップは、デフォルトの VRF の場合にのみサポートされています。

トラフィック フィルタリング アクション （9 ページ）に、フローに関連付けることができるアクションに関する情報を示します。ePBR を使用した BGP フロースペックの設定 （13 ページ）では、必要なタプル定義とアクションシーケンスを使用して BGP フロースペックを設定する手順について説明します。

トラフィック フィルタリング アクション

トラフィック フィルタリング フロー仕様のデフォルトアクションでは、その特定のルールに一致する IP トラフィックを受け入れます。次の拡張コミュニティ値を使用して、特定のアクションを指定できます。

タイプ	Extended Community	PBR アクション	説明

0x8006	traffic-rate 0 traffic-rate <rate>	Drop ポリシング	トラフィックレート拡張コミュニティは、自律システム境界を越えた非過渡的な拡張コミュニティであり、次の拡張コミュニティのエンコーディングを使用します。 最初の 2 つのオクテットで 2 オクテットの ID を伝送します。この ID は 2 バイトの AS 番号から割り当てることができます。4 バイトの AS 番号がローカルに存在する場合は、このような AS 番号の最下位 2 バイトを使用できます。この値は情報にすぎません。残りの 4 オクテットで、IEEE 浮動小数点 [IEEE. 754.1985] 形式のレート情報（バイト/秒単位）を伝送します。トラフィックレートが0の場合は、特定のフローのすべてのトラフィックが破棄されることになります。 **コマンド構文** police rate < > | drop
0x8008	redirect-vrf	VRF のリダイレクト	リダイレクト拡張コミュニティを使用すると、そのインポートポリシー内の指定されたルートターゲットをリストする VRF ルーティングインスタンスにトラフィックをリダイレクトできます。複数のローカルインスタンスがこの基準に一致する場合、それらの間でローカルな選択が行われます（たとえば、ルート識別子値が最も小さいインスタンスを選択できます）。この拡張コミュニティは、ルートターゲット拡張コミュニティ [RFC4360] と同じエンコーディングを使用します。 **ルートターゲットに基づくコマンドシンタックス** redirect {ipv6} extcommunity rt <route_target_string>
0x8009	traffic-marking	DSCP の設定	トラフィックマーキング拡張コミュニティは、通過する IP パケットの DiffServ コードポイント（DSCP ）ビットを対応する値に変更するようにシステムに指示します。この拡張コミュニティは 5 つのゼロバイトのシーケンスとしてエンコードされ、その後に 6 番目のバイトの最下位 6 ビットでエンコードされた DSCP 値が続きます。 **コマンド構文** set dscp <6 bit value> set ipv6 traffic-class <8 bit value>

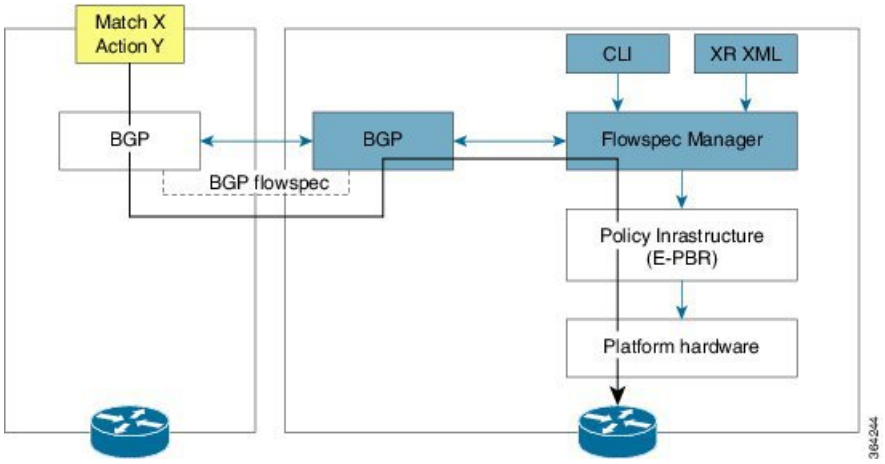
0x0800	IP NH のリダイレクト	リダイレクト IPv4 または IPv6 ネクストホップ	1 つ以上のフロースペック NLRI の到達可能性をアナウンスします。BGP スピーカーが redirect-to-IP 拡張コミュニティを使用して UPDATE メッセージを受信した場合、このパスをベストパスとして持つメッセージ内のすべてのフロースペック NLRI にトラフィック フィルタリング ルールを作成することが予想されます。フィルタエントリは、NLRI フィールドに記述されている IP パケットに一致し、それらをリダイレクトするか、または関連付けられた MP_REACH_NLRI の「Network Address of Next- Hop」フィールドに指定されている IPv4 または IPv6 アドレスにコピーします。 （注） redirect-to-IP 拡張コミュニティは、そのセットに redirect-to-VRF 拡張コミュニティ（タイプ 0x8008）が含まれており、redirect-to-IP 拡張コミュニティを無視する必要がある場合を除き、他のすべてのフロースペック拡張コミュニティのセットで有効です。 **コマンド構文** redirect {ipv6} next-hop <ipv4/v6 address> {ipv4/v6 address}

クラスマップの作成 （15 ページ） では、クラスマップの特定の一致基準を設定する方法について説明します。

BGP フロースペッククライアント/サーバ（コントローラ）モデルと ePBR を使用した設定

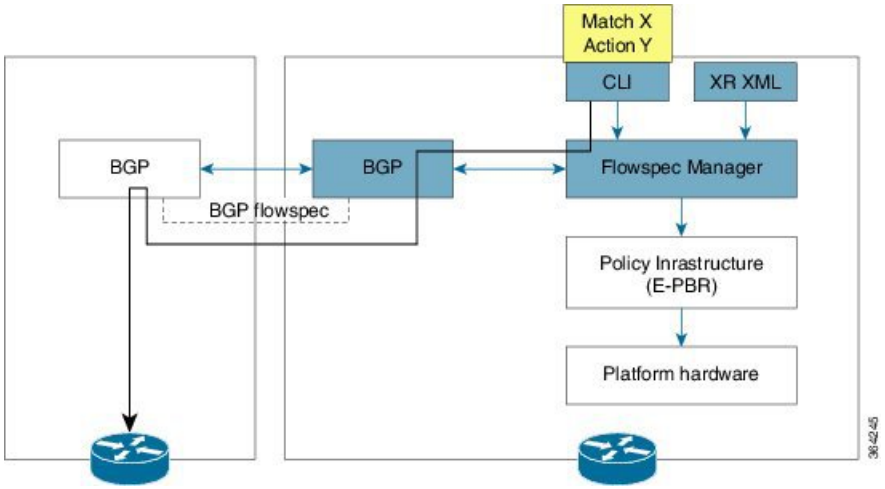
BGP フロースペックモデルは、クライアントとサーバ（コントローラ）で構成されます。コントローラは、フロースペック NRLI エントリの送信または挿入を実行します。クライアント（BGP スピーカーとして機能）はその NRLI を受信し、コントローラからの指示に従って動作するようにハードウェア転送をプログラムします。このモデルの図を下に示します。

BGP フロースペッククライアント



ここでは、左側のコントローラがフロースペック NRLI を挿入し、右側のクライアントが情報を受信し、フロースペックマネージャに送信し、ePBR（拡張ポリシーベースルーティング）インフラストラクチャを設定します。これにより、使用中の基盤プラットフォームからハードウェアがプログラムされます。

BGP フロースペックコントローラ



コントローラは、CLI を使用して NRLI インジェクション用のそのエントリを提供するように設定されます。

BGP フロースペックの設定

- **BGP 側**：アドバタイズメント用に新しいアドレスファミリを有効にする必要があります。この手順は、クライアントとコントローラの両方に適用されます。BGP フロースペックの有効化 （13 ページ）でその手順を説明します。

  クライアント側：フロースペック対応ピアの可用性を除き、固有の設定はありません。

- **コントローラ側**：これにはポリシーマップ定義が含まれており、ePBR 設定への関連付けは、クラス定義とアクションを定義するための ePBR でのそのクラスの使用という 2 つの手順で構成されます。以降のトピックで手順を説明します。

• ポリシー マップの設定 （17 ページ）
• クラスマップの作成 （15 ページ）
• ePBR ポリシーへの BGP フロースペックのリンク （18 ページ）

ePBR を使用した BGP フロースペックの設定

以降の項では、ePBR を使用して BGP フロースペックを設定する手順について説明します。

BGP フロースペック機能を有効にして設定するには、次の手順を実行します。

• BGP フロースペックの有効化 （13 ページ）
• クラスマップの作成 （15 ページ）
• ポリシー マップの設定 （17 ページ）
• ePBR ポリシーへの BGP フロースペックのリンク （18 ページ）

（注） 設定の変更を保存するには、システムでプロンプトが表示されたら、変更を確定する必要があります。

BGP フロースペックの有効化

次の手順を実行して、クライアントとサーバの両方に BGP フロースペックポリシーを伝達するためのアドレスファミリを有効にする必要があります。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **address-family** { **ipv4** | **ipv6** | **vpnv4** | **vpnv6** } **flowspec**
4. **exit**
5. **neighbor** *ip-address*
6. **remote-as** *as-number*
7. **address-family** { **ipv4** | **ipv6** } **flowspec**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router bgp** *as-number* 例： `RP/0/RSP0/cpu 0: router(config)# router bgp 100`	自律システム番号を指定し、BGP コンフィギュレーションモードを開始します。このモードでは、BGP ルーティング プロセスを設定できます。

	コマンドまたはアクション	目的
ステップ 3	**address-family** { **ipv4** | **ipv6** | **vpnv4** | **vpnv6** } **flowspec** 例： `RP/0/RSP0/cpu 0: router(config-bgp)# address-family ipv4 flowspec`	IPv4、IPv6、vpn4 または vpn6 アドレスファミリのいずれかを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始して、フロースペックポリシーのマッピングを行うグローバルアドレスファミリを初期化します。
ステップ 4	**exit** 例： `RP/0/RSP0/cpu 0: router(config-bgp-af)# exit`	ルータを BGP コンフィギュレーション モードに戻します。
ステップ 5	**neighbor** *ip-address* 例： `RP/0/RSP0/cpu 0: router(config-bgp)#neighbor 1.1.1.1`	BGP ルーティングのためにルータをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 6	**remote-as** *as-number* 例： `RP/0/RSP0/cpu 0: router(config-bgp-nbr)#remote-as 100`	ネイバーにリモート自律システム番号を割り当てます。
ステップ 7	**address-family** { **ipv4** | **ipv6** } **flowspec** 例： `RP/0/RSP0/cpu 0: router(config-bgp)# address-family ipv4 flowspec`	アドレスファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始して、フロースペックポリシーのマッピングを行うグローバルアドレスファミリを初期化します。

フロースペックポリシーマッピング用のアドレスファミリの設定：例

```
router bgp 100
 address-family ipv4 flowspec
 ! Initializes the global address family
 address-family ipv6 flowspec
 !
 neighbor 1.1.1.1
  remote-as 100
  address-family ipv4 flowspec
  ! Ties it to a neighbor configuration
  address-family ipv6 flowspec
```

!

クラスマップの作成

ePBR 設定を BGP フロースペックに関連付けるには、クラスを定義し、そのクラスを ePBR に使用してアクションを定義するためのサブステップを実行する必要があります。クラスを定義するには、次の手順を実行します。

手順の概要

1. **configure**
2. **class-map [type traffic] [match-all]** *class-map-name*
3. **match** *match-statement*
4. **end-class-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**class-map [type traffic] [match-all]** *class-map-name* 例： `RP/0/RSP0/cpu 0: router(config)# class-map type traffic match all classc1`	名前を指定したクラスとパケットの照合に使用するクラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。**match-any** を指定した場合、トラフィッククラスで受信したトラフィックがトラフィッククラスの一部と分類されるには、一致基準の 1 つを満たす必要があります。これはデフォルトです。**match-all** を指定した場合は、トラフィックがすべての一致基準を満たす必要があります。
ステップ 3	**match** *match-statement* 例： `RP/0/RSP0/cpu 0: router(config-cmap)# match protocol ipv4 1 60`	指定したステートメントに基づいてクラスマップに対して一致基準を設定します。タプル 1 ～ 13 の一致ステートメントの任意の組み合わせをここで指定できます。次に、タプル定義の可能性を示します。 • タイプ 1：**match destination-address** {**ipv4** | **ipv6**} *address/mask length* • タイプ 2：**match source-address** {**ipv4** | **ipv6**} *address/mask length* • タイプ 3： **match protocol** {*protocol-value* | *min-value* *−max-value*} （注） IPv6 の場合は、最後のネクストヘッダーにマップされます。

	コマンドまたはアクション	目的
		• タイプ 4：1 つは送信元ポート、もう 1 つは宛先ポートを持つ 2 つのクラスマップを作成します。 • **match source-port** {*source-port-value* | *min-value* *-max-value*} （注） 1 つの一致文字列でサポートされるポート番号は最大 5 つです。 • **match destination-port** {*destination-port-value* | *min-value* *-max-value*} （注） これらは、TCP プロトコルと UDP プロトコルにのみ適用されます。 • タイプ 5：**match destination-port** {*destination-port-value* |[*min-value* - *max-value*]} • タイプ 6：**match source-port** {*source-port-value* |[*min-value* - *max-value*]} • タイプ 7： **match** {**ipv4** | **ipv6**}**icmp-code** {*value* | *min-value* *-max-value*} • タイプ 8： **match**{**ipv4** | **ipv6**}**icmp-type** {*value* | *min-value* *-max-value*} • タイプ 9：**match tcp-flag** *value* **bit-mask** *mask_value* • タイプ 10： **matchpacket length** {*packet-length-value* | *min-value* *-max-value*}} • タイプ 11： **match dscp** {*dscp-value* | *min-value* *-max-value*} • タイプ 12： **match fragment-type** {**dont-fragment is-fragment first-fragment last-fragment**} • タイプ 13： **match ipv6 flow-label ipv4 flow-label** {*value* | *min-value* *-max-value*} BGP フロースペック コンフィギュレーションで使用されるさまざまなコマンドの詳細については、*Routing Command Reference for Cisco ASR 9000 Series Routers*ガイドの「*BGP Flowspec Commands*」を参照してください。

	コマンドまたはアクション	目的
ステップ 4	**end-class-map** 例： `RP/0/RSP0/cpu 0: router(config-cmap)# end-class-map`	クラス マップ コンフィギュレーション モードを終了して、ルータをグローバル コンフィギュレーション モードに戻します。

次のタスク

この手順で定義されたるクラスを、ポリシー マップの設定 （17 ページ）の説明に従って、PBR ポリシーに関連付けます。

ポリシー マップの設定

この手順では、ポリシーマップを定義し、これまでにクラスマップの作成 （15 ページ）で設定したトラフィックと関連付けることができます。

手順の概要

1. **configure**
2. **policy-map type pbr** *policy-map*
3. **class** *class-name*
4. **class type traffic** *class-name*
5. アクション
6. **exit**
7. **end-policy-map**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**policy-map type pbr** *policy-map* 例： `RP/0/RSP0/cpu 0: router(config)# policy-map type pbr policyp1`	サービスポリシーを指定するために 1 つ以上のインターフェイスに付加できるポリシーマップを作成または修正し、ポリシーマップ 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	**class** *class-name* 例： `RP/0/RSP0/cpu 0: router(config-pmap)# class class1`	ポリシーを作成または変更するクラスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 4	**class type traffic** *class-name* 例： `RP/0/RSP0/cpu 0: router(config-pmap)# class type traffic classc1`	これまでに設定したトラフィッククラスをポリシーマップに関連付け、制御ポリシーマップ トラフィック クラス コンフィギュレーション モードを開始します。
ステップ 5	アクション 例： `RP/0/RSP0/cpu 0: router(config-pmap-c)# set dscp 5`	要件に従って拡張コミュニティのアクションを定義します。オプションは次のとおりです。 • トラフィックレート： **police rate** *rate* • リダイレクト VRF：**redirect** { **ipv4ipv6** }**extcommunity rt** *route_target_string* • トラフィックマーキング： **set** {**dscp** *rate* | **destination-address** {**ipv4** | **ipv6**} *8-bit value*} • リダイレクト IP NH：**redirect** { **ipv4ipv6** } **nexthop** *ipv4 addressipv6 address* { *ipv4 addressipv6 address*}
ステップ 6	**exit** 例： `RP/0/RSP0/cpu 0: router(config-pmap-c)# exit`	ルータをポリシー マップ コンフィギュレーション モードに戻します。
ステップ 7	**end-policy-map** 例： `RP/0/RSP0/cpu 0: router(config-cmap)# end-policy-map`	ポリシー マップ コンフィギュレーション モードを終了して、ルータをグローバル コンフィギュレーション モードに戻します。

次のタスク

で説明されている手順でVRFとフロースペックのポリシーマッピングを実行し、フロースペックルールを配布します。 ePBR ポリシーへの BGP フロースペックのリンク （18 ページ）

ePBR ポリシーへの BGP フロースペックのリンク

BGP フロースペックの場合、ePBR ポリシーは VRF ごとに適用され、VRF に含まれているすべてのインターフェイスに適用されます。インターフェイス上に ePBR ポリシーがすでに設定されている場合、そのポリシーは BGP フロースペックポリシーによって上書きされません。インターフェイスからポリシーを削除すると、ePBR インフラストラクチャは、VRF レベルでアクティブだった場合は、BGP フロースペックポリシーを自動的に適用します。

（注） 一度に 1 つのインターフェイスでアクティブにできる ePBR ポリシーは 1 つのみです。

手順の概要

1. **configure**
2. **flowspec**
3. **local-install interface-all**
4. **address-family ipv4**
5. **local-install interface-all**
6. **service-policy type pbr** *policy-name*
7. **exit**
8. **address-family ipv6**
9. **local-install interface-all**
10. **service-policy type pbr** *policy-name*
11. **vrf** *vrf-name*
12. **address-family ipv4**
13. **local-install interface-all**
14. **service-policy type pbr** *policy-name*
15. **exit**
16. **address-family ipv6**
17. **local-install interface-all**
18. **service-policy type pbr** *policy-name*
19. **commit**
20. **exit**
21. **show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**flowspec** 例： `RP/0/RSP0/cpu 0: router(config)# flowspec`	フロースペック 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	**local-install interface-all** 例： `RP/0/RSP0/cpu 0: router(config-flowspec)# local-install interface-all`	（任意）フロースペックポリシーをすべてのインターフェイスにインストールします。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv4** 例： `RP/0/RSP0/cpu 0: router(config-flowspec)# address-family ipv4`	IPv4 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。
ステップ 5	**local-install interface-all** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-af)# local-install interface-all`	（任意）フロースペックポリシーをサブアドレスファミリのすべてのインターフェイスにインストールします。
ステップ 6	**service-policy type pbr** *policy-name* 例： `RP/0/RSP0/cpu 0: router(config-flowspec-af)# service-policy type pbr policys1`	インターフェイスのサービスポリシーとして使用されるポリシーマップを、IPv4 インターフェイスに付加します。
ステップ 7	**exit** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-af)# exit`	ルータをフロースペック コンフィギュレーション モードに戻します。
ステップ 8	**address-family ipv6** 例： `RP/0/RSP0/cpu 0: router(config-flowspec)# address-family ipv6`	IPv6 アドレスファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。
ステップ 9	**local-install interface-all** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-af)# local-install interface-all`	（任意）フロースペックポリシーをサブアドレスファミリのすべてのインターフェイスにインストールします。
ステップ 10	**service-policy type pbr** *policy-name* 例： `RP/0/RSP0/cpu 0: router(config-flowspec-af)# service-policy type pbr policys1`	インターフェイスのサービスポリシーとして使用されるポリシーマップを、IPv6 インターフェイスに付加します。

	コマンドまたはアクション	目的
ステップ 11	**vrf** *vrf-name* 例： `RP/0/RSP0/cpu 0: router(config-flowspec)# vrf vrf1`	VRF インスタンスを設定し、VRF フロースペック コンフィギュレーションサブモードを開始します。
ステップ 12	**address-family ipv4** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf)# address-family ipv4`	IPv4 アドレスファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。
ステップ 13	**local-install interface-all** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# local-install interface-all`	（任意）フロースペックポリシーをサブアドレス ファミリのすべてのインターフェイスにインストールします。
ステップ 14	**service-policy type pbr** *policy-name* 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# service-policy type pbr policys1`	インターフェイスのサービスポリシーとして使用されるポリシーマップを、IPv4 インターフェイスに付加します。
ステップ 15	**exit** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# exit`	ルータを VRF フロースペック コンフィギュレーション サブモードに戻します。
ステップ 16	**address-family ipv6** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。
ステップ 17	**local-install interface-all** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# local-install interface-all`	（任意）フロースペックポリシーをサブアドレス ファミリのすべてのインターフェイスにインストールします。

	コマンドまたはアクション	目的
ステップ 18	**service-policy type pbr** *policy-name* 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# service-policy type pbr policys1`	インターフェイスのサービスポリシーとして使用されるポリシーマップを、IPv6 インターフェイスに付加します。
ステップ 19	**commit**	
ステップ 20	**exit** 例： `RP/0/RSP0/cpu 0: router(config-flowspec-vrf-af)# exit`	ルータをフロースペック コンフィギュレーション モードに戻します。
ステップ 21	**show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf** 例： `RP/0/RSP0/cpu 0: routershow flowspec vrf vrf1 ipv4 summary`	（任意）インターフェイスに適用されているフロースペックポリシーを表示します。

BGP フロースペックの確認

次のさまざまな **show** コマンドを使用して、フロースペックの設定を確認します。たとえば、関連付けられた flowspec コマンドと BGP show コマンドを使用して、テーブル内のフロースペックルールの有無、存在するルールの数、定義したフロー仕様に基づいてトラフィックに対して実行されたアクションなどを確認できます。

手順の概要

1. **show processes flowspec_mgr location all**
2. **show flowspec summary**
3. **show flowspec vrf** *vrf_name* \| **all** { **afli-all** \| **ipv4** \| **ipv6** }
4. **show bgp ipv4 flowspec**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show processes flowspec_mgr location all**
	例：
	`# show processes flowspec_mgr location all`
	`node:  node0_3_CPU0`
		フロースペックプロセスがシステムで実行しているかどうかを指定します。フロースペックマネージャは、ハードウェアでのフロースペックルールの作成、配布、およびインストールを実行します。

	コマンドまたはアクション	目的
	Job Id: 10 PID: 43643169 Executable path: /disk0/iosxr-fwding-5.2.CSC33695-015.i/bin/flowspec_mgr Instance #: 1 Version ID: 00.00.0000 Respawn: ON Respawn count: 331 Max. spawns per minute: 12 Last started: Wed Apr 9 10:42:13 2014 Started on config: cfg/gl/flowspec/ Process group: central-services core: MAINMEM startup_path: /pkg/startup/flowspec_mgr.startup Ready: 1.113s Process cpu time: 0.225 user, 0.023 kernel, 0.248 total JID TID CPU Stack pri state TimeInState HR:MM:SS:MSEC NAME 1082 1 0 112K 10 Receive 2:50:23:0508 0:00:00:0241 flowspec_mgr 1082 2 1 112K 10 Sigwaitinfo 2:52:42:0583 0:00:00:0000 flowspec_mgr	
ステップ 2	**show flowspec summary** 例： # show flowspec summary FlowSpec Manager Summary: Tables: 2 Flows: 1 RP/0/3/CPU0:RA01_R4#	ノード全体に存在するフロースペックルールの概要を表示します。この例では、2 つのテーブルが IPv4 と IPv6 が有効になっており、テーブル全体で 1 つのフローが定義されていることを示します。
ステップ 3	**show flowspec vrf** *vrf_name* | **all** { **afli-all** | **ipv4** | **ipv6** } 例： # show flowspec vrf default ipv4 summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv4 Total Flows: 1 Total Service Policies: 1 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf default ipv6 summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf all afi-all summary Flowspec VRF+AFI table summary: VRF: default	フロースペックでより詳細な情報を取得するために、特定のアドレスファミリまたは特定の VRF 名に基づいて show コマンドをフィルタリングできます。この例では、「vrf default」は、フロースペックがデフォルトテーブルで定義されていることを示します。「IPv4 summary」には、そのデフォルトテーブルに存在する IPv4 フロースペックルールが表示されます。IPv6 が設定されていないため、値は、ipv6 サマリーの「Table Flows」と「Policies」パラメータに「zero」が表示されます。「VRF all」は、テーブルに設定されているすべての VRF に関する情報を表示し、afli-all はすべてのアドレスファミリ（IPv4 と IPv6）の情報を表示します。 **detail** オプションは、「Matched」フィールド、「Transmitted」フィールド、および「Dropped」フィールドを表示します。これらを使用して、定義したフロースペックルールが動作中かどうかを確認できます。この一致条件を満たすトラフィックがある場合は、何らかのアクションが実行されたかどう

	コマンドまたはアクション	目的
	AFI: IPv4 Total Flows: 1 Total Service Policies: 1 VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 --- # show flowspec vrf default ipv4 Dest:110.1.1.0/24, Source:10.1.1.0/24,DPort:>=120&<=130, SPort:>=25&<=30,DSCP:=30 detail AFI: IPv4 Flow :Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30 Actions :Traffic-rate: 0 bps (bgp.1) Statistics (packets/bytes) Matched : 0/0 Transmitted : 0/0 Dropped : 0/0	か（つまり、一致したパケットの数と、それらのパケットが送信されたか、ドロップされたか）を示します。
ステップ 4	**show bgp ipv4 flowspec** 例： # show bgp ipv4 flowspec Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 BGP routing table entry for Dest:110.1.1.0/24, Source:10.1.1.0/24,Proto:=47,DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 <snip> Paths: (1 available, best #1) Advertised to update-groups (with more than one peer): 0.3 Path #1: Received by speaker 0 Advertised to update-groups (with more than one peer): 0.3 Local 0.0.0.0 from 0.0.0.0 (3.3.3.3) Origin IGP, localpref 100, valid, redistributed, best, group-best Received Path ID 0, Local Path ID 1, version 42 Extended community: FLOWSPEC Traffic-rate:100,0	コントローラルータ上に設定されているフロースペックルールがBGP側で使用できるかどうかを確認するには、このコマンドを使用します。この例では、「redistributed」は、フロースペックルールが内部では発信されていないが、フロースペックプロセスから BGP に再配布されていることを示しています。設定されている拡張コミュニティ（一致およびアクション基準をピアルータに送信するために使用されるBGP属性）もここに表示されます。この例では、定義されたアクションはトラフィックのレート制限です。

リダイレクトネクストホップの保持

ルート指定の一部としてリダイレクトネクストホップを明示的に設定できます。リダイレクトネクストホップは、関連する拡張コミュニティとともに、BGP フロースペック NLRI で MP_REACH ネクストホップとしてエンコードされます。このような flowspec ルートが受信されると、リダイレクトネクストホップのFIBルックアップによりトラフィックはリダイレクトされ、ネクストホップは、場合により IP または MPLS トンネルを介して解決できます。ネク

ストホップ接続が複数のASに及ぶ場合、eBGP境界でMP_REACHネクストホップを上書きできるため、未変更のノブを使用することでネクストホップを保持できます。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **neighbor** *ip-address*
4. **address-family** { **ipv4** | **ipv6** }
5. **flowspec next-hop unchanged**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router bgp** *as-number* 例： `RP/0/RSP0/cpu 0: router(config)# router bgp 100`	自律システム番号を指定し、BGPコンフィギュレーションモードを開始します。このモードでは、BGPルーティング プロセスを設定できます。
ステップ 3	**neighbor** *ip-address* 例： `RP/0/RSP0/cpu 0: router(config)# router bgp 100 neighbor 1.1.1.1`	BGP ルーティングのためにルータをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 4	**address-family** { **ipv4**	**ipv6** } 例： `RP/0/RSP0/cpu 0: router(config-bgp)# router bgp 100 neighbor 1.1.1.1 address-family ipv4`	IPv4 または IPv6 のいずれかのアドレスファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始してグローバルアドレスファミリを初期化します。
ステップ 5	**flowspec next-hop unchanged** 例： `RP/0/RSP0/cpu 0: router(config-bgp)# router bgp 100 neighbor 1.1.1.1 address-family ipv4 flowspec next-hop unchanged`	フロースペックのネクストホップを変更せずに保持します。

BGP フロースペックの検証

BGP フロースペック検証は、IPv4 または IPv6 のフロースペック SAFI ルートに対してデフォルトで有効になっています。VPNルートは、フロー検証の対象にはなりません。機能を動作させるため、次の条件のいずれかをtrueの状態に保持することを確認するためにフロー仕様NLRIが検証されます。

- フロー仕様の発信元は、フロー仕様に組み込まれている宛先プレフィックスのベストマッチのユニキャストルートの発信元と一致します。
- 異なる隣接 AS から受信したフローの宛先プレフィックスを比較した場合、前の条件で決定されたベストマッチのユニキャストルート以外に特定のユニキャストルートはありません。
- フロー仕様の AS_PATH と AS4_PATH 属性は空です。
- フロー仕様の AS_PATH および AS4_PATH 属性には、AS_SET セグメントと AS_SEQUENCE セグメントは含まれていません。

これらの条件を満たさないパスは、BGP によって適切にマーキングされ、フロースペックマネージャにはインストールされません。さらに、BGP では、EBGP で学習したフロー仕様 NLRI の AS_PATH と AS4_PATH 属性内に追加された最後の AS は、フロー仕様に組み込まれた宛先プレフィックスのベストマッチのユニキャストルートの AS_PATH と AS4_PATH 属性内に追加された最後の AS と一致する必要があります。また、redirect-to-IP 拡張コミュニティが存在する場合、デフォルトでは、BGP は eBGP ピアからフロースペックルートを受信すると、次のチェックを強制的に実行します。

フロースペックルートに IP ネクストホップ X があり、redirect-to-IP 拡張コミュニティが含まれている場合、BGP スピーカは、最も長いプレフィックス一致の AS_PATH または AS4_PATH 属性の最後の AS が eBGP ピアの AS と一致しない場合、redirect-to-ip 拡張コミュニティを破棄します（また、フロースペックルートを使用してそれ以降は伝達しません）。

フロースペックリダイレクトと検証の無効化 （27 ページ） では、BGP フロースペック検証を無効にする手順について説明します。

BGP フロースペックの無効化

この手順では、インターフェイス上の BGP フロースペックポリシーを無効にします。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **{ ipv4 | ipv6 } flowspec disable**
4. **commit**

手順の詳細

ステップ 1 **configure**

ステップ 2 **interface** *type interface-path-id*

例：

```
RP/0/RSP0/cpu 0: router(config)# interface GigabitEthernet 0/1/1/1
```

インターフェイスを設定して、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3 **{ ipv4 | ipv6 } flowspec disable**

例：

```
RP/0/RSP0/cpu 0: router(config-if)# ipv4 flowspec disable
```

選択したインターフェイス上のフロースペックポリシーを無効にします。

ステップ 4 **commit**

インターフェイスでのフロースペックの無効化

次に、インターフェイス上の BGP フロースペックを無効にし、別の PBR ポリシーを適用する例を示します。

```
Interface GigabitEthernet 0/0/0/0
 flowspec [ipv4/ipv6] disable
int g0/0/0/1
service policy type pbr test_policy
 !
!
```

フロースペックリダイレクトと検証の無効化

明示的なノブを設定することによって、フロースペック検証を eBGP セッションの全体で無効にすることができます。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **neighbor** *ip-address*
4. **address-family** { **ipv4** | **ipv6** }
5. **flowspec validation** { **disable** | **redirect disable** }

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure**	
ステップ 2	**router bgp** *as-number* 例： `RP/0/RSP0/cpu 0: router(config)# router bgp 100`	自律システム番号を指定し、BGP コンフィギュレーションモードを開始します。このモードでは、BGP ルーティング プロセスを設定できます。

	コマンドまたはアクション	目的
ステップ 3	**neighbor** *ip-address* 例： `RP/0/RSP0/cpu 0: router(config)# router bgp 100 neighbor 1.1.1.1`	BGP ルーティングのためにルータをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 4	**address-family** { **ipv4** | **ipv6** } 例： `RP/0/RSP0/cpu 0: router(config-bgp)# router bgp 100 neighbor 1.1.1.1 address-family ipv4`	IPv4 または IPv6 のいずれかのアドレスファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始してグローバルアドレスファミリを初期化します。
ステップ 5	**flowspec validation** { **disable** | **redirect disable** } 例： `RP/0/RSP0/cpu 0: router(config-bgp)# router bgp 100 neighbor 1.1.1.1 address-family ipv4 flowspec validation disable`	すべての eBGP セッションの全体に対してフロースペック検証を無効にするか、またはリダイレクトネクストホップの検証を無効にするかを選択できます。

BGP フロースペックの設定例

フロースペックルールの設定

フロースペックルールの設定例

この例では、2 つの異なる VRF に対して 2 つのフロースペックルールが作成されています。これは、192/8 から 10.0.1/24 へと宛先ポート（範囲 137、139）または 8080 へのすべてのパケットと対象とし、レート制限を blue vrf で 500 bps とし、デフォルトの VRF でドロップすることを目標としています。これは、gig 0/0/0/0 で有効になっているフロースペックを無効にすることも目標としています。

```
class-map type traffic match-all fs_tuple
 match destination-address ipv4 10.0.1.0/24
 match source-address ipv4 192.0.0.0/8
 match destination-port 137-139 8080
 end-class-map
 !
!
policy-map type pbr fs_table_blue
 class type traffic fs_tuple
  police rate 500 bps
```

```
  !
 !
 class class-default
 !
 end-policy-map
policy-map type pbr fs_table_default
 class type traffic fs_tuple
  drop
  !
 !
 class class-default
 !
 end-policy-map
flowspec
 local-install interface-all
 address-family ipv4
  service-policy type pbr fs_table_default
  !
 !
 vrf blue
  address-family ipv4
   service-policy type pbr fs_table_blue local
   !
  !
 !
!
Interface GigabitEthernet 0/0/0/0
 vrf blue
 ipv4 flowspec disable
```

ドロップパケット長

次に、ドロップパケット長アクションの設定例を示します。

```
class-map type traffic match-all match-pkt-len
 match packet length 100-150
 end-class-map
!
policy-map type pbr test2
 class type traffic match-pkt-len
  drop
 !
 class type traffic class-default
 !
 end-policy-map
!
```

特定のクラスに属するパケットを破棄するようにトラフィッククラスを設定するには、ポリシー マップ コンフィギュレーション モードで drop コマンドを使用します。この例では、100 ～ 150 の複数範囲のパケット長値が定義されています。着信トラフィックのパケット長がこの条件に一致した場合、このパケットを「ドロップ」するようにアクションが定義されています。

リダイレクトトラフィックとレート制限：例

```
class-map type traffic match-all match-src-ipv6-addr
 match source-address ipv6 3110:1::/48
 end-class-map
!
policy-map type pbr test5
 class type traffic match-src-ipv6-addr
  redirect nexthop 3010:10:11::
  police rate 20 mbps
  !
 !
 class type traffic class-default
 !
 end-policy-map
!
```

この例では、特定の送信元 IP アドレス（3110:1::/48）からのすべてのトラフィックをネクストホップアドレスにリダイレクトするために、フロースペックルールにアクションが定義されています。また、この送信元アドレスで着信するすべてのトラフィックについて、送信元アドレスのレート制限は 20 メガビット/秒になります。

グローバルからの VRF（vrf1）へのトラフィックのリダイレクト

次に、トラフィックをグローバル トラフィック リンクから個々の VRF インターフェイスへリダイレクトするための設定例を示します。

```
class-map type traffic match-all match-src-ipv6-addr
 match source-address ipv6 3110:1::/48
 end-class-map
!
policy-map type pbr test4
 class type traffic match-src-ipv6-addr
  redirect nexthop route-target 100:1
 !
 class type traffic class-default
 !
 end-policy-map
```

DSCP のリマーク

次に、set dscp アクションの設定例を示します。

```
class-map type traffic match-all match-dscp-af11
 match dscp 10
 end-class-map
!
policy-map type pbr test6
 class type traffic match-dscp-af11
  set dscp af23
 !
 class type traffic class-default
 !
 end-policy-map
!
```

この例では、トラフィックマーキング拡張コミュニティ（**match dscp**）によって、dscp 10 から dscp af23 へ通過する IP パケットの DSCP ビットを変更または設定するようにシステムに指示します。

BGP フロースペックの追加資料

以降の項では、BGP フロースペックの実装に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
BGP フロースペックコマンド：コマンドシンタックスの詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	*Routing Command Reference for Cisco ASR 9000 Series Routers*

標準

標準	タイトル
draft-ietf-idr-flow-spec-v6-05 draft-ietf-idr-flowspec-redirect-ip-01 draft-simpson-idr-flowspec-redirect-02 draft-ietf-idr-bgp-flowspec-oid-02	『*Dissemination of Flow Specification Rules for IPv6*』、 『BGP Flow-Spec Redirect to IP Action』 『BGP Flow-Spec Extended Community for Traffic Redirect to IP Next Hop』 『Revised Validation Procedure for BGP Flow Specifications』

RFC

RFC	タイトル
RFC 5575	『Dissemination of Flow Specification Rules』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport