IP および MPLS-VPN 向け BGP PIC（プレフィックス独立コンバージェンス）エッジ

IP および MPLS-VPN 向け BGP PIC（プレフィックス独立コンバージェンス）エッジ機能により、ネットワーク障害後の BGP コンバージェンスが向上します。このコンバージェンスは、IP ネットワークと MPLS ネットワークで使用可能であり、コア障害とエッジ障害の両方に適用されます。IP および MPLS-VPN 向け BGP PIC エッジ機能は、ルーティング情報ベース（RIB）、転送情報ベース（FIB）、および Cisco Express Forwarding にバックアップ パスまたは代替パスを作成、保存します。障害の検出時には、バックアップパスまたは代替パスが即座に引き継ぐため、高速なフェールオーバーが実現されます。

（注） このドキュメントでは、IP および MPLS-VPN 向け BGP PIC エッジ機能は短縮名の BGP PIC と呼ばれます。

BGP PIC の前提条件

- 複数のパスによってプロバイダー サイトと接続されている（マルチホーム）カスタマー サイトで、ボーダー ゲートウェイ プロトコル（BGP）および IP またはマルチプロトコル ラベル スイッチング（MPLS）ネットワークが稼働中であることを確認します。

- バックアップ パスまたは代替パスには、最良パスのネクスト ホップと異なる固有のネクスト ホップがあることを確認します。
- 直接接続されたネイバーのリンク障害をすばやく検出できるように、Bidirectional Forwarding Detection（BFD）プロトコルを有効にします。

BGP PIC の制約事項

- グローバル プレフィックスのラベルが付いていない BGP PIC エッジはサポートされません。
- TE、SR、SR-TE、flex-LSP はサポートされません。
- コアとしての BVI はサポートされません。
- プライマリ パスとバックアップ パスはそれぞれ 1 つのみサポートされます。複数のプライマリ パスと 1 つのバックアップ パスはサポートされません。
- PIC エッジは、グローバル IPv4、IPv6（6PE）、および MPLS-VPN プレフィックス（VPNv4 および VPNv6）でサポートされます。

利点

- プライマリ パスが無効になった場合や取り消された場合でも、フェールオーバー用の追加パスにより、接続を迅速に復元できます。
- トラフィック損失の軽減。
- コンバージェンス時間が一定なので、すべてのプレフィックスで切り替え時間が同じ。

BGP コンバージェンス

通常の状況では、BGP はネットワークの変更後に収束するのに数秒から数分かかることがあります。概要としては、BGP は次のプロセスの手順を実行します。

1. BGP は内部ゲートウェイ プロトコル（IGP）または BFD イベント、もしくはインターフェイス イベントを通じて不具合を確認します。
2. BGP はルーティング情報ベース（RIB）からルートを取り消し、RIB は Forwarding Information Base（FIB; 転送情報ベース）および分散 FIB（dFIB）からルートを取り消します。このプロセスにより、障害の影響を受けたプレフィックスへのデータ パスがクリアされます。
3. BGP は取り消しのメッセージをネイバーに送信します。
4. BGP は影響を受けたプレフィックスへの次に適したパスを計算します。

5. BGP は影響を受けたプレフィックスの次に適したパスを RIB に挿入し、RIB はそのパスを FIB および dFIB にインストールします。

このプロセスが完了するまでには数秒から数分かかることがあります。これは、ネットワークの遅延、ネットワーク全体のコンバージェンス時間、およびデバイスでのローカル ロードによって異なります。コントロール プレーンのコンバージェンスが行われて初めて、データ プレーンのコンバージェンスが行われます。

コンバージェンスの改善

BGP PIC 機能は、BGP、RIB、Cisco Express Forwarding、MPLS の追加機能によって実現されます。

- BGP の機能

BGP PIC は、IPv4 および VPNv4 アドレス ファミリのプレフィックスに影響を与えます。これらのプレフィックスについて、BGP は、プライマリ ベスト パスに加え、2 番目に適したパスも計算します（2 番目に適したパスは、バックアップ パスまたは代替パスと呼ばれます）。BGP は、影響を受けたプレフィックスのベスト パスとバックアップ パスまたは代替パスを BGP RIB にインストールします。バックアップ パスまたは代替パスにより、単一のネットワーク障害に対処する高速再ルーティング機能が提供されます。また、BGP は、IP RIB に対するアプリケーション プログラミング インターフェイス（API）に代替パスまたはバックアップ パスを追加します。

- RIB の機能

BGP PIC では、RIB はルートごとに代替パスをインストールします（使用可能な場合）。RIB は、バックアップ パスまたは代替パスを含む BGP ルートを選択した場合、ベスト パスとともにそのバックアップ パスまたは代替パスをインストールします。また、RIB は、この代替パスを FIB との API にも追加します。

- Cisco Express Forwarding 機能

BGP PIC では、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）はプレフィックスごとに代替パスを保存します。プライマリ パスがダウンした場合、Cisco Express Forwarding は、プレフィックスに依存しない方法でバックアップ パスまたは代替パスを検索します。また、シスコ エクスプレス フォワーディングは、局地的な障害を迅速に検出するために、BFD イベントをリッスンします。

- MPLS 機能

MPLS 転送は、プライマリ パスがダウンした場合には代替パスを保存して代替パスに切り替えるという点で、Cisco Express Forwarding と似ています。

BGP PIC 機能が有効な場合、BGP はプレフィックスごとにバックアップ パスまたは代替パスを計算し、BGP RIB、IP RIB、および FIB にインストールします。これにより、ネットワーク

障害後のコンバージェンスが向上します。BGP PIC機能によって検出されるネットワーク障害には、次の 2 種類があります。

- コア ノードまたはリンク障害（内部ボーダー ゲートウェイ プロトコル（iBGP）ノード障害）：PE ノードまたはリンクで障害が発生した場合、IGP コンバージェンスによって障害が検出されます。IGP は、RIB を通じて FIB に障害を伝達します。
- ローカル リンクまたは直近にあるネイバー ノードの障害（外部ボーダー ゲートウェイ プロトコル（eBGP）ノードまたはリンク障害）：ローカル リンク障害または eBGP シングルホップ ピア ノード障害を瞬時に検出するには、BFD を有効にする必要があります。Cisco Express Forwarding は eBGP シングルホップ ピアの障害を検出するために BFD イベントを探します。

データ プレーンでのコンバージェンス

障害を検出すると、Cisco Express Forwarding は、その障害の影響を受けるすべてのプレフィックスに対する代替ネクスト ホップを検出します。データ プレーン コンバージェンスは、BGP PIC の実装がソフトウェアに存在するかハードウェアに存在するかに応じて、瞬時に達成されます。

コントロール プレーンでのコンバージェンス

障害を検出すると、BGP は、IGP コンバージェンスまたは BFD イベントによってその障害を確認し、該当のプレフィックスについて取り消しのメッセージを送信し、ベストパスとバックアップパスまたは代替パスを再計算し、ネットワーク全体で次に適したパスをアドバタイズします。

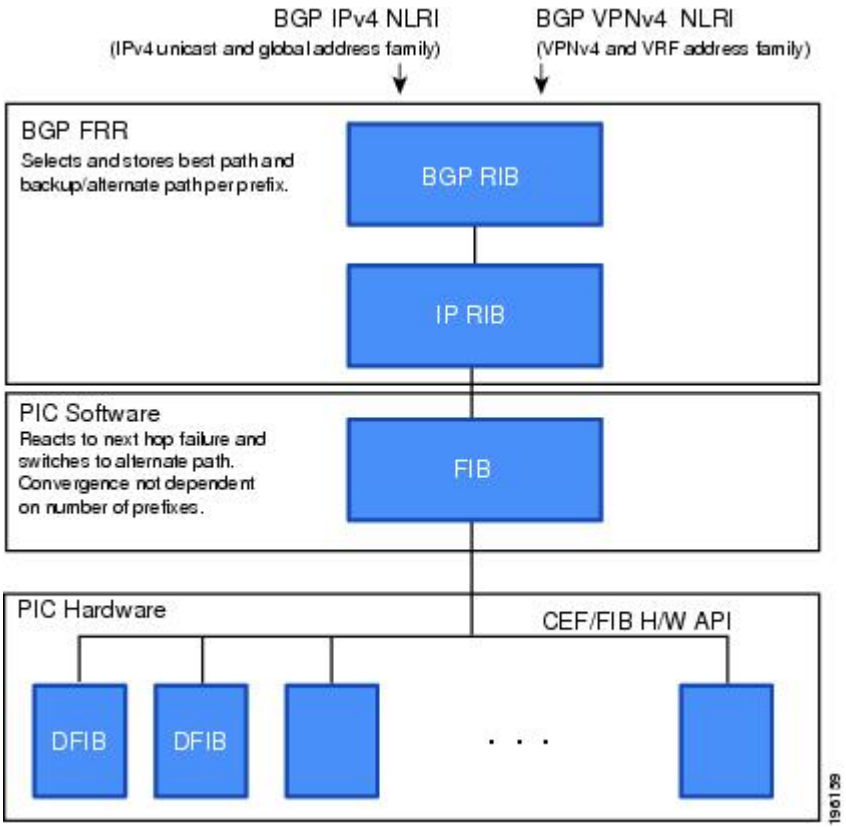
BGP Fast Reroute

BGP Fast Reroute（FRR; 高速再ルーティング）は、BGP、RIB、および Cisco Express Forwarding でのベスト パスとバックアップ パスまたは代替パスを提供します。BGP FRR は、現在のベスト パスが使用できない場合に宛先に到達するためのバックアップ BGP ネクスト ホップに関する高速再ルーティング メカニズムを RIB および Cisco Express Forwarding（CEF）に提供します。

BGP FRR は BGP で次に適したパスを事前に計算し、そのパスをバックアップ パスまたは代替パスとして RIB および Cisco ExpressForwardin に提供し、CEF はそのパスをライン カードにプログラムします。

BGP PIC 機能は、現在のネクスト ホップまたはこのネクスト ホップへのリンクがダウンした場合に CEF でトラフィックを他の出力ポートに迅速に切り替えることができるようにします。

図 *1 : BGP PIC* エッジと *BGP FRR*



障害の検出

IGP は、iBGP（リモート）ピアの障害を検出します。障害が検出されるまでに数秒かかる場合があります。コンバージェンスは、ラインカードでPICがイネーブルにされているかどうかに応じて、瞬時、または数秒以内に行われます。

直接接続されたネイバー（eBGP）で障害が発生した場合や、ネイバーがダウンしたことをBFDを使用して検出する場合。ライン カードで PIC が有効化されているかどうかに応じて、瞬時に検出されることがあり、コンバージェンスも瞬時または数秒以内に行われます。

MPLS VPN–BGP ローカル コンバージェンス

BGP PIC は、MPLS VPN–BGP ローカル コンバージェンス機能を拡張したものです。リンク障害後にベスト パスを再計算するフェールオーバー メカニズムを提供します。その後、新しいパスが転送に組み込まれます。トラフィックの損失を最小限に抑えるために、この機能はローカル ラベルを 5 分間保持して、トラフィックでバックアップ パスまたは代替パスが使用されるようにします。

BGP PIC は、事前にバックアップ パスまたは代替パスを計算して、LoC 時間を 1 秒未満に短縮します。リンク障害が発生すると、トラフィックはバックアップ パスまたは代替パスに送られます。

BGP PIC を設定すると、MPLS VPN--BGP ローカル コンバージェンスの機能がオーバーライドされます。設定から **protection local-prefixes** コマンドを削除しないでください。

BGP PIC の有効化

BGP PIC エッジは、次のアドレス ファミリで有効化できます。

- IPv4
- IPv6
- VPNv4
- VPNv6

BGP PIC シナリオ

BGP PIC 機能を設定して、高速コンバージェンスを実現できます。

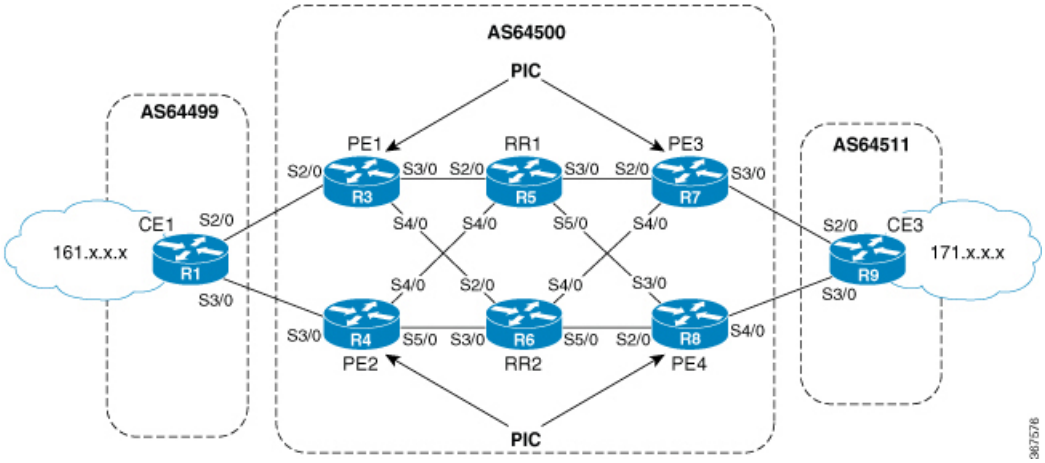
IP PE-CE リンクおよびノード保護

このネットワークは、以下のコンポーネントで構成されています。

- CE1（161.x.x.x）からのトラフィックは、PE1 を使用してルータ CE3 を介してネットワーク 171.x.x.x に到達します。CE1 には次の 2 つのパスがあります。
  - プライマリ パスとしての PE1。
  - バックアップ パスまたは代替パスとしての PE2。

PE1、PE2、PE3、および PE4 には、BGP PIC エッジ機能が設定されています。PE1 は、プレフィックス 161.x.x.x について CE1 から学習します。また、PE1 はルート リフレクタ（RR1 および RR2）から PE2 を介して同じプレフィックスについて学習します。PE1 に、プレフィックス 161.x.x.x のプライマリおよびバックアップが組み込まれます。PE1 と CE1 の間のリンクがダウンすると PE1 で PIC エッジがトリガーされ、BGP PIC エッジがアクティブになり、PE2 を介して CE1 にトラフィックを送信します。これは、PE と CE のリンク障害時の BGP PIC エッジです。

図 *2 : BGP PIC* を使用した *PE-CE* リンクの保護



- 同様に、PE1 にはルータ CE3 を介してネットワーク 171.x.x.x に到達するパスが 2 つあります。
  - プライマリ パスとしての PE3。
  - バックアップ パスまたは代替パスとしての PE4。

PE1 は RR1 および RR2 を介して PE3 と PE4 からプレフィックス 171.x.x.x について学習し、このプレフィックスのプライマリとバックアップを組み込みます。PE3 がダウンすると、PE1 で BGP PIC エッジがトリガーされてトラフィックが PE4 に再ルーティングされます。これは、ノード障害時の BGP PIC エッジです。

BGP PIC の設定

手順

ステップ 1 **cef encap-sharing disable**

例：

```
RP/0/RP0/cpu 0: router(config)# cef encap-sharing disable
```

デフォルトでは、IPv4 グローバル プレフィックスは、プライマリ パスおよびバックアップ パス（使用可能な場合）とともにハードウェアに組み込まれます。IPv6（6 PE）、VPNv4、および VPNv6 プレフィックスの保護をハードウェアに組み込むには、グローバル コンフィギュレーション モードで CLI **cef encap-sharing disable** コマンドを設定する必要があります。

注意 この CLI によって CEF が完全に再プログラミングされ、トラフィックが影響を受けます。これは、メンテナンス期間に実行することをお勧めします。

ステップ 2 **router bgp** *as-number*

例：

```
RP/0/RP0/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 **address-family** {**vpnv4 unicast** | **vpnv6 unicast** | **ipv4 unicast** | **ipv6 unicast**}

例：

```
RP/0/RP0/cpu 0: router(config-bgp)# address-family ipv4 unicast
```

```
address-family ipv4 unicast
  additional-paths receive
  additional-paths selection route-policy backup 1
  allocate-label all
!
```

ステップ 4 **additional-paths selection route-policy** *route-policy-name*

例：

```
RP/0/RP0/cpu 0: router(config-bgp-af)# additional-paths selection route-policy ap1
```

プレフィックスの追加パス選択モードを設定します。

（注） **additional-paths selection** コマンドを適切なルート ポリシーとともに使用して、バックアップ パスを計算し、プレフィックス独立コンバージェンス（PIC）機能を有効にします。

ルートポリシーの設定は、プレフィックスの追加パス選択モードを設定するための前提条件です。追加選択コマンドで使用するルートポリシー設定の例を次に示します。

```
route-policy ap1
    set path-selection backup 1 install
  end-policy
```