



BFD の実装

このモジュールでは、Cisco ASR 9000 シリーズルータでの双方向フォワーディング検出 (BFD) の設定について説明します。

双方向フォワーディング検出 (BFD) では、隣接する転送エンジン間のパスにおける障害を低オーバーヘッド、短時間で検出できます。BFD では、あらゆるメディアおよびあらゆるプロトコルレイヤでの障害検出に単一のメカニズムを使用でき、広範な検出時間とオーバーヘッドに対応できます。障害の迅速な検出が可能のため、リンクやネイバーの障害発生時にもただちに障害に対応することができます。

双方向フォワーディング検出の実装の機能履歴

リリース	変更内容
リリース 3.7.2	BFD が導入されました。
リリース 3.9.0	<ul style="list-style-type: none">• BFD での次のアプリケーションのサポートが追加されました。<ul style="list-style-type: none">• Hot Standby Router Protocol (HSRP)• Virtual Router Redundancy Protocol (VRRP)• BFD セッションのフラッピングとセッションの開始遅延を最小化するために、dampening コマンドが追加されました。• 送信元 IP アドレスを指定してデフォルトを上書きするために、echo ipv4 source コマンドが追加されました。• IPv6 UDP チェックサムの計算および BFD インターフェイス コンフィギュレーション モードを有効および無効にするように、ipv6 checksum コマンドが追加されました。

リリース 4.0.0	<p>次の BFD 機能のサポートが追加されました。</p> <ul style="list-style-type: none"> • OSPFv3 用 BFD • IPv6 用 BFD <p>BFD のサポートは、次の SPA に追加されました。</p> <ul style="list-style-type: none"> • 1 ポート OC-192c/STM-64 POS/RPR XFP SPA • 2 ポート OC-48c/STM-16 POS/RPR SPA • 8 ポート OC-12c/STM-4 POS SPA
リリース 4.0.1	<p>次の BFD 機能のサポートが追加されました。</p> <ul style="list-style-type: none"> • リンクバンドルのメンバリンク単位の BFD のサポートが追加されました。 • 非バンドルインターフェイスの BFD エコーパケットに対する遅延検出を有効にするために、echo latency detect コマンドが追加されました。 • 非バンドルインターフェイスの BFD セッションを開始する前にエコーパスを検証するために、echo startup validate コマンドが追加されました。
リリース 4.2.0	<p>次の BFD 機能のサポートが追加されました。</p> <ul style="list-style-type: none"> • BFD マルチホップグローバル TTL チェック。 • BGP の BFD マルチホップ サポート、および • IPv4 トラフィックの BFD マルチホップ サポート。 • マルチホップセッション用のパケットのドロップを開始するための TTL 値を指定するために、multihop ttl-drop-threshold コマンドが追加されました。
リリース 4.2.1	ASR9K-SIP-700 ラインカードでの BFD マルチホップ機能のサポートが追加されました。

リリース 4.2.3	論理バンドル上の BFD 機能のサポートが追加されました。
リリース 4.3.0	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • GRE を介した BFD • BFD IPv6 マルチホップ • 論理バンドル上の BFD
リリース 4.3.1	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • MPLS トラフィック エンジニアリング LSP を介した BFD • 疑似回線ヘッドエンドを介した BFD • サテライトインターフェイスを介した BFD
リリース 5.2.4	バンドル CISCO/IETF モードを介した BFD のバンドル単位のサポートが追加されました。

- [BFD の実装の前提条件 \(3 ページ\)](#)
- [BFD の実装の制約事項 \(4 ページ\)](#)
- [BFD に関する情報 \(6 ページ\)](#)
- [BFD の設定方法 \(33 ページ\)](#)
- [BFD を設定するための設定例 \(69 ページ\)](#)
- [次の作業 \(79 ページ\)](#)
- [その他の参考資料 \(79 ページ\)](#)

BFD の実装の前提条件

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれません。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

次に、BFD を実装するための前提条件を示します。

- マルチプロトコルラベルスイッチング (MPLS) で BFD を有効にする場合は、MPLS パッケージを含んだインストール済みの複合 PIE ファイル、または複合パッケージイメージが必要です。ボーダーゲートウェイプロトコル (BGP)、Intermediate System-to-Intermediate System (IS-IS)、スタティック、Open Shortest Path First (OSPF) の場合は、インストール済みの Cisco IOS XR IP Unicast Routing Core Bundle イメージが必要です。
- IS-IS または OSPF を使用している場合、ルータで内部ゲートウェイプロトコル (IGP) がアクティブになっていること。

- Cisco ASR 9000 シリーズ ルータでは、BFD をサポートしている各ラインカードが次のタスクを実行できる必要があります。
 - エコー パケットを 50ms * 3 ごとに送信（通常の状態の最小値として）。
 - 制御パケットを 150ms * 3 ごとに送信（負荷のある状態の最小値として）。
 - 最大 9600 pps のユーザ データグラム プロトコル (UDP) を送受信。これにより、15 ms エコー間隔で 144 セッション（または 150 ms エコー間隔で 1440 セッション）を維持します。
- ネイバーの BFD を有効にするには、その隣接ルータが BFD をサポートしている必要があります。
- リリース 3.9.0 よりも前の Cisco IOS XR リリースでは、BFD セッションを設定する前に、グローバル コンフィギュレーション モードで **router-id** コマンドを使用して、ローカル ルータ ID を設定することを推奨していました。ローカル ルータ ID を設定しなかった場合、デフォルトで BFD エコーモードでの IP パケットの送信元アドレスが、出カインターフェイスの IP アドレスとなります。Cisco IOS XR Release 3.9.0 以降では、**echo ipv4 source** コマンドを使用して、送信元アドレスとして使用する IP アドレスを指定できます。
- バンドル メンバリンクでの BFD をサポートするには、次の要件が満たされていることを確認してください。
 - バンドルの両端にあるルータが、間にレイヤ 2 スイッチを使用せずにバックツーバックで接続されている。
 - BFD セッションを開始する場合、次のいずれかの設定または状態がバンドル メンバに存在する。
 - リンク集約制御プロトコル (LACP) 分散状態に到達している、または EtherChannel または POS チャネルが設定されている、または
 - ホットスタンバイおよび LACP 収集状態に到達している。

BFDの実装の制約事項

BFD には、次の制約事項が適用されます。

- Cisco IOS XR ソフトウェアではデマンド モードはサポートされません。
- 次の機能では、BFD エコー モードはサポートされません。
 - バンドル VLAN での IPv4 用 BFD
 - IPv6 用 BFD（グローバルおよびリンクローカルアドレッシング）
 - uRPF での BFD（IPv4 または IPv6）

- BFD バンドル インターフェイスに複数のラックにまたがるメンバリンクがある場合の、ラック リロードおよび活性挿抜 (OIR)
 - マルチホップパスの BFD
- IPv6 用 BFD には、次の制約事項があります。
- IPv6 用 BFD は、バンドル VLAN インターフェイスではサポートされません。
 - IPv6 用 BFD スタティック ルート、OSPFv3、および BGP は、クライアントでサポートされます。
 - ネクストホップとしてリンクローカルアドレスを持つ IPv6 用 BFD スタティック ルートはサポートされません。
- バンドル メンバリンクでの BFD の場合は、IPv4 アドレッシング タイプについてのみ、バンドル メンバリンクごとに 1 つの BFD セッションだけが作成、モニタ、および保持されます。バンドルの IPv6 および VLAN リンクに関する制約事項は、次のとおりです。
- IPv6 の状態はバンドル メンバで明示的にモニタされず、そのメンバ インターフェイスの IPv4 BFD セッションの状態を継承します。
 - バンドル メンバの VLAN サブインターフェイスはまた、そのメンバ インターフェイスの IPv4 BFD セッションから BFD 状態を継承します。VLAN サブインターフェイスはバンドル メンバで明示的にモニタされません。
- エコー遅延検出およびエコー検証は、バンドル インターフェイスではサポートされません。
- BFD マルチホップはデフォルト以外の任意の VRF で実行できますが、選択的 VRF ダウンロードが無効になっている必要があります。選択的 VRF ダウンロードのための設定およびコマンドの詳細については、*Routing Configuration Guide for Cisco ASR 9000 Series Routers* および *Routing Command Reference for Cisco ASR 9000 Series Routers* を参照してください。
- GRE 上の BFD 機能は、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 ではサポートされません。
- BFD IPv6 マルチホップ機能は、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 ではサポートされません。
- 論理バンドル上の BFD 機能は、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 ではサポートされません。
- イーサネットラインカードでは、BFD MH と BLB のみがサポートされています。このラインカードでは、BFD_oTE、BFD_oIRB、BFD_oGRE などの BFD マルチパスセッションはサポートされていません。
- サテライトセッションを介した BFD は、ASR 9000 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。また、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 でもサポートされていません。

- バンドルインターフェイスに明示的なバンドルハッシュが設定されている場合、バンドルマネージャは送信元または宛先の IP アドレスに基づいてハッシュを実行します。これにより、すべてのエコーパケットがメンバーリンクのいずれかでのみ送信され、他のリンクはフラッピングを開始します。

BFD エコーには送信元ポートに基づくハッシュが必要なため、IP ベースのハッシュではメンバーリンク間でエコーパケットが配信されません。

どちらも相互運用できないため、設定されたバンドルの IP ベースのハッシュを回避するか、またはエコーモードを無効にします。

IP ベースのハッシュを削除するには、次の手順を実行します。

```
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 1
RP/0/RSP0/CPU0:router(config)# no bundle load-balancing hash dst-ip
```

```
/* or */
```

```
RP/0/RSP0/CPU0:router(config)# no bundle load-balancing hash src-ip
```

設定されたバンドルのエコーを無効にするには、次の手順を実行します。**echo disable** コマンドは、グローバルモードまたはインターフェイス コンフィギュレーション モードのいずれかで実行されます。

```
RP/0/RSP0/CPU0:router(config)# bfd
RP/0/RSP0/CPU0:router(config)# interface bundle-ether 1
RP/0/RSP0/CPU0:router(config-if)# echo disable
```

```
*/ or */
```

```
RP/0/RSP0/CPU0:router(config)# bfd echo disable
```

BFDに関する情報

Cisco IOS XR ソフトウェアと Cisco IOS ソフトウェアでの BFD の違い

すでに Cisco IOS ソフトウェアでの BFD の設定に精通している場合は、Cisco IOS XR ソフトウェア実装での BFD の設定に関する次の違いについて必ず考慮します。

- Cisco IOS XR ソフトウェアでは、BFD は OSPF や BGP インスタンスなどのダイナミックルーティングプロトコルの下で設定されたアプリケーションです。これは、BFD がインターフェイスでのみ設定される Cisco IOS ソフトウェアでの BFD には当てはまりません。
- Cisco IOS XR ソフトウェアでは、BFD ネイバーはルーティングを介して確立されます。Cisco IOS **bfd neighbor** インターフェイス コンフィギュレーション コマンドは、Cisco IOS XR ソフトウェアではサポートされていません。
- ダイナミックルーティングプロトコルを使用して BFD ネイバーを確立する代わりに、そのパスを定義するためのスタティックルーティングの方法を使用して、Cisco IOS XR ソフトウェアで BFD 応答のための特定の BFD ピアまたはネイバーを確立することができま

す。実際には、Cisco IOS XR ソフトウェアでダイナミック ルーティング プロトコルの下で BFD を設定しない場合は、BFD のスタティック ルートを設定する必要があります。

- Cisco IOS ソフトウェアで BFD を実行しているルータは、**bfd neighbor** コマンドを使用してピアとして Cisco IOS XR ソフトウェアで BFD を実行するルータを指定できます。Cisco IOS XR ルータは、ピア関係を確立するために Cisco IOS ルータに戻るダイナミックルーティングまたは静的ルートを使用する必要があります。[Cisco IOS および Cisco IOS XR ソフトウェアを実行しているルータの BFD ピア](#)：例を参照してください。

nV エッジシステムでの BFD マルチパスセッションのサポート

nV エッジシステムでは、次の BFD マルチパスセッションがサポートされています。

- GRE を介した BFD
- 論理バンドル上の BFD
- IRB を介した BFD
- BFD マルチホップ (5.2.2 以降でのみサポート)
- MPLS TE を介した BFD
- サテライト経由の BFD

BFD の動作モード

Cisco IOS XR ソフトウェアは、エコー パケットを使用するか否かにかかわらず、非同期動作モードだけをサポートします。エコーなしの非同期モードでは、ローカルおよびリモートシステム上のパケット スイッチング パスのさまざまな部分に関与します。ただし、エコーありの非同期モードは通常、若干広いテストカバレッジを提供すると認識されています。これは、エコーパケットがリモートシステムの通常のトラフィックと同じパケット スイッチング パスを通過する自分宛てのパケットであるためです。

BFD エコーモードは、次のインターフェイスではデフォルトで有効になっています。

- BFD バンドル インターフェイスのメンバリンク上の IPv4 の場合。
- 最小間隔が 2 秒未満である他の物理インターフェイス上の IPv4 の場合。

BFD がエコーパケットなしで非同期で実行されている場合 (図 35) は、次のようになります。

- 各システムが相互に定期的に BFD 制御パケットを送信します。BFD ルータの「ピア A」によって BFD ルータの「ピア B」に送信されたパケットは、ピア A からの送信元アドレスおよびピア B の宛先アドレスを保持します。
- 制御パケット ストリームは互いに独立していて、要求/応答モデルで動作しません。
- 連続する多数のパケットが別のシステムによって受信されない場合、セッションがダウンしたと宣言されます。

図 1: エコー パケットなしの BFD 非同期モード



BFD がエコーパケットありで非同期で実行されている場合 (図 36) は、次のようになります。

- BFD エコー パケットは、BFD ピアのための転送パス経路でループバックされ、どのプロトコルスタックでも処理されません。そのため、BFD ルータの「ピア A」によって送信されたパケットは、ピア A の送信元アドレスと宛先アドレスの両方を使用して送信できます。
- BFD 制御パケットに加えて、BFD エコー パケットが送信されます。

図 2: エコー パケットありの BFD 非同期モード



非同期モードでの制御およびエコーパケットの間隔の詳細については、[BFD パケット間隔と障害検出](#)を参照してください。

BFD パケット情報

BFD の送信元および宛先ポート

BFD ペイロード制御パケットは、宛先ポート 3784 および送信元ポート 49152 を使用して、UDP パケットにカプセル化されます。イーサネットのような共有型メディアでも、BFD 制御パケットは常にユニキャストパケットとして BFD ピアに送信されます。

エコーパケットも、宛先ポート 3785 および送信元ポート 3785 を使用して、UDP パケットにカプセル化されます。

バンドルメンバを介した BFD 機能は、送信ごとにエコーパケットの UDP 送信元ポートの各バイトを増分します。UDP 送信元ポートの範囲は 0xC0C0 から 0xFFFF です。次に例を示します。

1 番目のエコーパケット : 0xC0C0

2 番目のエコーパケット : 0xC1C1

3 番目のエコーパケット : 0xC2C2

UDP 送信元ポートは、連続したエコーパケットが逸脱しているバンドルメンバにハッシュされるように増分されます。

BFD パケット間隔と障害検出

BFD は、設定可能な間隔と係数を使用して、非同期モードで制御およびエコー パケットが送信される期間と、それらに対応する障害検出を指定します。

物理インターフェイスで実行されている BFD セッション、およびバンドル メンバリンクの BFD セッションに対するこれらの間隔と障害検出時間の実装方法には違いがあります。

物理インターフェイスでの BFD パケット間隔

BFD が物理インターフェイス経由で実行されている場合、エコー モードは、設定された間隔が 2 秒未満である場合にのみ使用されます。

エコーモードが有効になっているときに物理インターフェイス経由で実行されている BFD セッションは、2 秒ごとの遅いレートで BFD 制御パケットを送信します。BFD エコーパケットはすでに高速で送信されており、エコーパケットがエコー障害検出時間内に受信されないときはリンク障害が検出されるため、高速で制御パケット障害検出を複製する必要はありません。

バンドルメンバリンクの BFD パケット間隔

各バンドルメンバインターフェイスでは、エコーモードが実行されている場合でも、BFD 非同期モード制御パケットはユーザ設定可能な間隔および係数値で動作します。

ただし、バンドルメンバインターフェイスでエコーモードが有効になっているとき、BFD 非同期モードは高速レートで実行し続ける必要があります。これは、BFD エコーモードを有効にする要件の 1 つとして、バンドルメンバインターフェイスが BFD 非同期モードで使用できることがあるためです。

バンドルメンバリンクの BFD の最大エコーパケット間隔は、30 秒または非同期制御パケット障害検出時間のいずれかの最小値です。

エコーモードが無効になっている場合、セッションが設定されたレートで BFD 制御パケットを交換する物理インターフェイスでの BFD と動作は同じになります。

非同期モードでの制御パケット障害検出

エコーなしの非同期モードでの制御パケット障害検出は、最小間隔（非バンドルインターフェイスでは `bfd minimum-interval`、バンドルインターフェイスでは `bfd address-family ipv4 minimum-interval`）および係数（非バンドルインターフェイスでは `bfd multiplier`、バンドルインターフェイスでは `bfd address-family ipv4 multiplier`）コマンドの値を使用して実行されます。

制御パケット障害検出の場合は、ローカルの係数値がネイバーに送信されます。障害検出タイマーは、 $(I \times M)$ に基づいて開始されます。ここで、 I はネゴシエートされた間隔で、 M はリモートエンドによって提供された係数です。

有効な制御パケットがネイバーから受信されるたびに、障害検出タイマーはリセットされます。有効な制御パケットが期間 $(I \times M)$ 内にネイバーから受信されない場合は、障害検出タイマーがトリガーされ、ネイバーがダウンしたと宣言されます。

非同期モードでのエコーパケット障害検出

標準のエコー障害検出方式は、非バンドルインターフェイスでは **bfd multiplier** コマンドの値、バンドルインターフェイスでは **bfd address-family ipv4 multiplier** コマンドの値に基づいたカウンタを通して実行されます。

このカウンタは、エコーパケットがエコーパケットストリームに送信された順序にかかわらず、システムがエコーパケットを送信するたびに増分され、何らかのエコーパケットが受信されるたびにゼロにリセットされます。

つまり、理想的な条件下では、BFD は一般に、バンドルインターフェイスでは期間 ($I \times M$) または ($I \times M \times M$) を超えるエコー障害を検出します。ここで、各値は次のとおりです。

- I : 最小間隔の値 (非バンドルインターフェイスでは **bfd minimum-interval**、バンドルインターフェイスでは **bfd address-family ipv4 minimum-interval**)。
- M : 乗数 (非バンドルインターフェイスでは **bfd multiplier**、バンドルインターフェイスでは **bfd address-family ipv4 multiplier**) コマンドの値。

そのため、システムがエコーパケットをまったく受信せずに係数カウントを超えて追加のエコーパケットを1つ送信した場合は、エコー障害が検出され、ネイバーがダウンしたと宣言されます (例 2) を参照)。

ただし、この標準のエコー障害検出では、BFD セッション中に ($I \times M$) を超えて増加する可能性がある特定のエコーパケットの送信と受信の間の遅延には対処できません。この場合は、係数の期間内にいずれかのエコーパケットが引き続き受信され、カウンタがゼロにリセットされる限り、BFD はネイバーのダウンを宣言しません。Cisco IOS XR 4.0.1 以降では、非バンドルインターフェイスでこの遅延を測定するように BFD を設定できます。詳細については、例 3 および [エコーパケットの遅延](#) を参照してください。

エコー障害検出の例

ここでは、非バンドルインターフェイスでの、遅延検出の設定を行わない標準のエコーパケット処理および障害検出のいくつかのシナリオの例について説明します。これらの例では、間隔は 50 ms、また係数は 3 とします。



- (注) バンドルインターフェイスにもエコー障害検出に対する同じ間隔と乗数カウンタ方式が使用されますが、これらの値は **bfd address-family ipv4 multiplier** と **bfd address-family ipv4 minimum-interval commands** によって決定され、エコーパケットの受信がないことを検出するために ($I \times M \times M$) の期間を使用します。

例 1

次に、次のエコーが送信される前に各エコーパケットが返される理想的なケースの例を示します。この場合、カウンタは 1 に増分され、次のエコーが送信される前に 0 に戻されます。エコー障害は発生しません。セッション内のエコーパケットのラウンドトリップ遅延が最小間隔より短い限り、このシナリオが発生します。

```
Time (T): Echo#1 TX (count = 1)
T + 1 ms: Echo#1 RX (count = 0)
T + 50 ms: Echo#2 TX (count = 1)
T + 51 ms: Echo#2 RX (count = 0)
T + 100 ms: Echo#3 TX (count = 1)
T + 101 ms: Echo#3 RX (count = 0)
T + 150 ms: Echo#4 TX (count = 1)
T + 151 ms: Echo#4 RX (count = 0)
```

例 2

エコーパッケージが一切戻らない例を次に示します。4 番目のエコーパッケージの送信後、カウンタが係数値 3 を超えてエコー障害が検出されます。この場合、エコー障害検出は、150 ms ($I \times M$) 期間で発生します。

```
Time (T): Echo#1 TX (count = 1)
T + 50 ms: Echo#2 TX (count = 2)
T + 100 ms: Echo#3 TX (count = 3)
T + 150 ms: Echo#4 TX (count = 4 -> echo failure)
```

例 3

次に、標準のエコー障害検出を使用しているときに、BFDセッション中に特定のエコーパッケージについてラウンドトリップ遅延が ($I \times M$) を超えて増加する可能性があるが、セッション内の全体的なエコーパッケージの戻りの間の遅延は ($I \times M$) の期間を超えず、またカウンタも乗数を超えないため、ネイバーはダウンしたと宣言されることのない例を示します。



- (注) Cisco IOS XR 4.0.1 以降では、**echo latency detect** コマンドを使用して、非バンドルインターフェイスのラウンドトリップ遅延を検出するように BFD を設定できます。

```
Time (T): Echo#1 TX (count = 1)
T + 1 ms: Echo#1 RX (count = 0)
T + 50 ms: Echo#2 TX (count = 1)
T + 51 ms: Echo#2 RX (count = 0)
T + 100 ms: Echo#3 TX (count = 1)
T + 150 ms: Echo#4 TX (count = 2)
T + 151 ms: Echo#3 RX (count = 0; ~50 ms roundtrip latency)
T + 200 ms: Echo#5 TX (count = 1)
T + 250 ms: Echo#6 TX (count = 2)
T + 251 ms: Echo#4 RX (count = 0; ~100 ms roundtrip latency)
T + 300 ms: Echo#7 TX (count = 1)
T + 350 ms: Echo#8 TX (count = 2)
T + 351 ms: Echo#5 RX (count = 0; ~150 ms roundtrip latency)
T + 451 ms: Echo#6 RX (count = 0; ~200 ms roundtrip latency; no failure detection)
T + 501 ms: Echo#7 RX (count = 0; ~200 ms roundtrip latency; no failure detection)
T + 551 ms: Echo#8 RX (count = 0; ~200 ms roundtrip latency; no failure detection)
```

BFDセッションでのエコーパッケージの受信の間の遅延を見て、どの遅延も ($I \times M$) の期間を超えていないことに注目してください。

```
Echo#1 RX - Echo#2 RX: 50 ms
```

バンドルインターフェイスでの BFD のパケット間隔と障害検出時間の概要

```

Echo#2 RX - Echo#3 RX: 100ms
Echo#3 RX - Echo#4 RX: 100ms
Echo#4 RX - Echo#5 RX: 100ms
Echo#5 RX - Echo#6 RX: 100ms
Echo#6 RX - Echo#7 RX: 50ms
Echo#7 RX - Echo#8 RX: 50ms

```

バンドルインターフェイスでの BFD のパケット間隔と障害検出時間の概要

セッション間隔 I および乗数 M のバンドルインターフェイスの BFD の場合、次のパケット間隔および障害検出時間が BFD 非同期モードに適用されます (表 1: バンドルインターフェイスでの BFD パケット間隔および障害検出時間の例)。

- I の値: BFD 制御パケットを送信する最小間隔。
- $I \times M$ の値
 - BFD 制御パケット障害検出時間。
 - BFD エコーパケットを送信する最小間隔。

BFD 制御パケット障害検出時間は、BFD セッションのダウンが宣言されるまでに BFD 制御パケットを受信せずに経過できる最大時間です。

- $(I \times M) \times M$ の値: BFD エコーパケット障害検出時間。これは、BFD セッションのダウンが宣言されるまでに (非同期モードでのエコーパケット障害検出で説明されている標準の係数カウンタ方式を使用して) BFD エコーパケットを受信せずに経過できる最大時間です。

表 1: バンドルインターフェイスでの BFD パケット間隔および障害検出時間の例

設定された非同期制御パケット間隔 (ms) (bfd address-family ipv4 minimum-interval)	設定された係数 (bfd address-family ipv4 multiplier)	非同期制御パケット障害検出時間 (ms) (間隔 x 係数)	エコーパケット間隔 (非同期制御パケット障害検出時間)	エコーパケット障害検出時間 (エコー間隔 x 係数)
50	3	150	150	450
75	4	300	300	1200
200	2	400	400	800
2000	3	6000	6000	18000
15000	3	45000	30000 ¹	90000

¹ バンドルメンバリンクの BFD の最大エコーパケット間隔は、30 秒または非同期制御パケット障害検出時間のいずれかの最小値です。

エコーパケットの遅延

Cisco IOS XR 4.0.1 よりも前の Cisco IOS XR ソフトウェア リリースでは、BFD は特定のエコーパケットの TX/RX に対する特定の遅延ではなく、エコーパケットの受信がないことだけを検出します。場合によっては、BFD エコーパケットの受信が全体として、障害検出およびパケット送信の全体的な許容値内に収まることもあります。エコーパケットの特定のラウンドトリップについて時間とともに遅延が増加する可能性があります (例 3)。

Cisco IOS XR リリース 4.0.1 以降、ルータを設定して、非バンドルインターフェイスでエコーパケットの送受信間の実際の遅延を検出でき、また遅延がそのラウンドトリップ遅延に設定されたしきい値を超えるとときにセッションをダウンできます。詳細については、[エコー遅延検出に基づいた BFD セッションティアダウンの設定](#)を参照してください。

また、BFD セッションを開始する前に、エコーパケットパスが指定された遅延許容値内にあることも検証できます。エコー起動検証では、BFD セッションの状態変更を可能にする前に設定済みの遅延内に送信が成功するかどうかを確認するために、リンクがダウンしている間、そのリンク上でエコーパケットが定期的に送信されます。詳細については、[エコーパスと遅延の検証までの BFD セッション開始の遅延](#)を参照してください。

BFD パケットのプライオリティの設定

オーバーサブスクリプションの状態にあるすべてのインターフェイスについて、リモート BFD エコーパケットに内部プライオリティを割り当てることにより、これらの BFD パケットが他のデータパケットによって過負荷状態にならないようにする必要があります。さらに、中間スイッチの場合に、リモート BFD エコーパケットの戻りの応答がスイッチ内のその他のすべてのパケットから保護されるように、CoS 値を適切に設定する必要があります。

イーサネット ヘッダーに設定された CoS 値はエコーメッセージ内に保持されない可能性があるため、適切な出力 QoS サービス ポリシーで CoS 値を明示的に設定する必要があります。set cos コマンドを使用して、トラフィック クラスに付加された BFD パケットの CoS 値を設定できます。クラスベースの無条件パケットマーキングの設定の詳細については、*Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers*の「Configuring Modular QoS Packet Classification」を参照してください。

IPv4 用 BFD

Cisco IOS XR ソフトウェアは、IPv4 と IPv6 の両方での双方向フォワーディング検出 (BFD) のシングルホップおよびマルチホップをサポートします。

IPv4 用 BFD のシングルホップ接続では、Cisco IOS XR ソフトウェアは、番号付けされた物理 Packet-over-SONET/SDH (POS) およびギガビットイーサネットリンクでの非同期モードとエコーモードの両方を次のようにサポートします。

- エコーモードは、BFD 制御パケットを使用してセッションが確立された後にはのみ開始されます。BFD バンドルメンバインターフェイスでは、エコーモードは常に有効になっています。物理インターフェイスの場合は、エコーパケットをサポートするために、BFD 最小間隔も 2 秒未満である必要があります。

- BFD エコー パケットは、送信元および宛先ポート 3785 を使用して、UDP/IPv4 で転送されます。IP パケットの送信元アドレスは出力インターフェイスの IP アドレス（デフォルト）か、または設定されている場合は **router-id** コマンドで指定されたアドレスか、**echo ipv4 source** コマンドで指定されたアドレスであり、宛先アドレスはローカルインターフェイスアドレスです。
- BFD 非同期パケットは、送信元ポート 49152 および宛先ポート 3784 を使用して、UDP および IPv4 で転送されます。非同期モードの場合、IP パケットの送信元アドレスはローカルインターフェイスアドレス、宛先アドレスはリモートインターフェイスアドレスとなります。



(注) BFD マルチホップは、エコー モードをサポートしません。

Cisco IOS XR ソフトウェアで BFD を設定する場合は、次の注意事項を考慮してください。

- BFD は固定長の hello プロトコルで、接続の各終端で転送パスを通じてパケットを定期的 に転送します。Cisco IOS XR ソフトウェアは、BFD 適応型検出時間をサポートします。
- BFD は、次のアプリケーションと併用することができます。
 - BGP
 - IS-IS
 - EIGRP
 - OSPF
および OSPFv3
 - MPLS トラフィック エンジニアリング (MPLS-TE)
 - 静的ルート (IPv4 および IPv6)
 - Protocol Independent Multicast (PIM)
 - Hot Standby Router Protocol (HSRP)
 - Virtual Router Redundancy Protocol (VRRP)



(注) 複数のアプリケーションが同じ BFD セッションを共有するとき、最も強力なタイマーのあるアプリケーションがローカルで優先されます。その結果は、次にピアルータとネゴシエートされます。

- BFD は、次のインターフェイス タイプでの接続でサポートされます。
 - ギガビット イーサネット (GigE)
 - 10 ギガビット イーサネット (TenGigE)

- Packet-over-SONET/SDH (POS)
- シリアル (Serial)
- 仮想 LAN (VLAN)
- Bridge Group Virtual Interface (BVI)
- サテライトインターフェイス
- バンドル、GRE、PWHE などの論理インターフェイス



(注) BFDは上のインターフェイスタイプでサポートされ、特に説明されていない限り、論理インターフェイスではサポートされません。

- Cisco IOS XR ソフトウェアは、BFD バージョン 0 およびバージョン 1 をサポートします。BFD セッションは、ネイバーに応じていずれかのバージョンを使用して確立されます。BFD バージョン 1 はデフォルトバージョンであり、セッション確立において最初に試行されます。

IPv6 用 BFD

Cisco IOS XR ソフトウェアは、IPv4 と IPv6 の両方での双方向フォワーディング検出 (BFD) をサポートします。IPv6 での双方向フォワーディング検出 (BFD) では、IPv6 アドレスを使用するインターフェイスでの稼働中の接続の確認をサポートします。

稼働中の接続の確認は、IPv4 と IPv6 の両方のインターフェイスについて、同じサービスとプロセスによって実行されます。同一ラインカード上で、IPv4 と IPv6 の両方の BFD セッションを同時に実行することができます。

IPv4 用 BFD でサポートされるものと同じ機能と設定が IPv6 用 BFD でもサポートされます。

バンドル VLAN での BFD

バンドル VLAN 上の IPv4 用 BFD は、スタティックルーティング、IS-IS、および OSPF を使用してサポートされます。バンドル VLAN インターフェイスで BFD セッションを実行すると、VLAN バンドルがアップ状態である限り BFD セッションはアクティブな状態となります。

VLAN バンドルがアクティブであれば、次に示すイベントによって BFD セッションが失敗することはありません。

- コンポーネント リンクの障害。
- 1 つ以上のコンポーネント リンクをホストするラインカードの活性挿抜 (OIR) 。
- バンドルへのコンポーネント リンクの追加 (設定による) 。

- バンドルからのコンポーネントリンクの削除（設定による）。
- コンポーネントリンクのシャットダウン。
- RP スイッチオーバー。



(注) VLAN バンドルの設定の詳細については、「*Configuring Link Bundling on the Cisco ASR 9000 Series Router*」のモジュールを参照してください。

バンドル VLAN で BFD を設定する場合には、次の事項に注意する必要があります。

- RP スイッチオーバーの場合、設定されているネクストホップは Routing Information Base (RIB) に登録されます。
- BFD 再起動の場合、スタティックルートは RIB に残ります。BFD セッションは、BFD の再起動時に再確立されます。

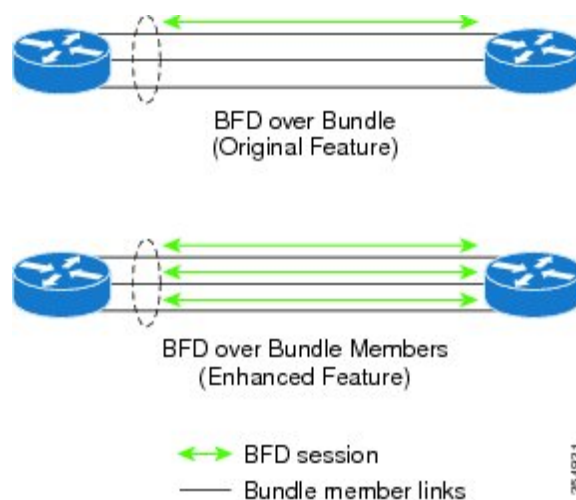


(注) スタティック BFD セッションは、ネクストホップがルータに直接接続されているアドレスプレフィックスを持つピアでサポートされます。

リンクバンドルのメンバリンク上の BFD

以前のリリースのように単一のバンドルメンバのみではなく、BFD ではリンク上のレイヤ 3 接続をモニタする個々の物理バンドルメンバリンクで BFD セッションをサポートしています (図 37)。

図 3: バンドル上の元の BFD およびバンドルメンバリンク アーキテクチャ上の拡張 BFD における BFD セッション



リンクバンドルで BFD を実行する場合は、そのバンドルの一部である基盤となる各物理インターフェイスで、独立した BFD セッションを実行できます。

BFD がリンクバンドルメンバで実行されているとき、接続の次のレイヤは BFD のインターフェイス状態モニタリングの一部として実質上テストされます。

- レイヤ 1 の物理状態
- レイヤ 2 のリンクアクセスコントロールプロトコル (LACP) 状態
- レイヤ 3 の BFD 状態

各バンドルメンバリンクの BFD エージェントはリンクの状態変更をモニタリングします。バンドルメンバリンクで実行されているセッションの BFD エージェントはバンドルマネージャと通信します。バンドルマネージャは、メンバリンクの状態とバンドル全体のアベイラビリティを特定します。メンバリンクの状態は、そのバンドル用に設定された最小アクティブリンクまたは最小アクティブ帯域幅のしきい値に基づいて、バンドル全体の状態に影響を及ぼします。

メンバリンクおよびバンドルステータスでの BFD 状態変更動作の概要

ここでは、バンドルメンバリンクの状態がいつアクティブまたはダウンとして特徴づけられるか、およびそれらの全体的なバンドルステータスへの影響について説明します。

- すでにアクティブであるか、または非アクティブであるバンドルメンバインターフェイスで BFD を設定できます。インターフェイスで LACP を使用してアップになる BFD セッションの場合は、LACP が配布状態に達している必要があります。

リンクが LACP 分散状態にあり、BFD セッションがアップである場合、BFD メンバリンクは「IIR Active」です。

- BFD セッションがダウンである場合は、LACP 状態遷移が受信されない限り、BFD メンバリンクは「IIR Attached」です。
- リンクバンドル BFD セッションのダウンを宣言する前に、ピアからの BFD 状態変更通知 (SCN) の受信遅延を許可するように最大 3600 秒 (1 時間) のタイマーを設定できます。設定可能なタイマーは、次の状況に適用されます。
 - BFD セッションの開始 (`bfd address-family ipv4 timers start` コマンド) : セッションのアップを宣言するために BFD ピアからの予測される通知が受信されるように、BFD メンバリンクセッションの開始後に見越しておく秒数。その期間の後に SCN が受信されない場合は、BFD セッションのダウンが宣言されます。
 - ネイバーによる BFD 設定の削除の通知 (`bfd address-family ipv4 timers nbr-unconfig` コマンド) : BFD ピア間の設定の不一致をすべて解決できるように、BFD 設定が BFD ネイバーによって削除されたことの通知の受信後に見越しておく秒数。指定されたタイマーに達する前に BFD 設定の問題が解決されない場合、BFD セッションのダウンが宣言されます。
- BFD セッションは、次のいずれかが発生すると DOWN 通知を送信します。

- ローカル メンバリンクで BFD 設定が削除される。

BFD システムは、設定が削除されたことを隣接ルータのピアに通知します。BFD セッションは、他のバンドルメンバインターフェイスまたは全体的なバンドル状態に影響を与えることなく、バンドルマネージャから削除されます。

- メンバリンクがバンドルから削除される。

バンドルからのメンバリンクの削除によって、バンドルメンバは強制的に削除されます。BFD セッションは削除され、隣接ルータ上の BFD がそのセッションを NBR_CONFIG_DOWN ではなく、DOWN とマークします。

- 次の場合、DOWN 通知は送信されませんが、内部インフラストラクチャは DOWN が発生したかのようにイベントを処理します。

- 隣接ルータ上で BFD 設定が削除され、ネイバー設定解除タイマー（設定されている場合）の期限が切れる。

BFD システムは BFD 設定が隣接ルータから削除されたことをバンドルマネージャに通知し、**bfd timers nbr-unconfig** がリンクで設定されている場合は、タイマーを開始します。タイマーの期限が切れる前にローカルルータ上で BFD 設定が削除された場合は、タイマーは停止し、ローカルルータ上の BFD 設定を削除した場合と同じ動作になります。

タイマーが切れた場合、動作は BFD セッション DOWN 通知の場合と同じです。

- BFD ピアからの通知が受信される前に、セッション開始タイマーの期限が切れる。

- バンドルメンバの BFD セッションがバンドルマネージャに BFD 状態変更通知を送信します。バンドルメンバインターフェイスの BFD 状態変更通知がバンドルマネージャによって受信されると、バンドルマネージャは、対応するバンドルインターフェイスが使用可能かどうかを判断します。

- バンドルのアクティブメンバリンクの最小数のしきい値は、メンバリンクの状態に基づいてバンドルがアクティブなままか、ダウンであるかを判断するためにバンドルマネージャによって使用されます。すでにアクティブであるバンドルで BFD が開始された場合、そのバンドルの BFD 状態は、既存のすべてのアクティブメンバの BFD 状態が既知であるときに宣言されます。

メンバの状態が変更されるたびに、バンドルマネージャは、アクティブメンバの数がアクティブリンクのしきい値の最小数より小さいかどうかを判断します。その場合は、バンドルが DOWN 状態になるか、または DOWN 状態のままになります。アクティブリンクの数が最小しきい値に達すると、バンドルは UP 状態に戻ります。

- バンドルで別のしきい値を設定できます。そのしきい値は、バンドルマネージャによって使用され、バンドルが DOWN 状態になる前に使用できるアクティブな帯域幅の最小値が決定されます。これを設定するには、**bundle minimum-active bandwidth** コマンドを使用します。

- BFD サーバは、バンドル インターフェイスの状態変更に関するバンドル マネージャからの情報に応答し、そのインターフェイス上のアプリケーションに通知するとともに、システム メッセージや MIB トラップも送信します。

BFD マルチパス セッション

BFD は、GRE トンネル インターフェイスや PWHE インターフェイスなどの仮想 インターフェイス経由で、または「[マルチホップパスの BFD](#)」の項で説明されているようにマルチホップ離れた インターフェイス間で適用できます。これらのタイプの BFD セッションは、BFD マルチパス セッションと呼ばれます。

宛先への 1 つのパスがアクティブである限り、次のイベントによって BFD マルチパス セッションが失敗する場合も、失敗しない場合もあります。それは、ネゴシエートされた間隔と、フローディング プレーンの更新に必要なコンバージェンス時間の関係に依存するためです。

- パスの障害
- 1 つ以上のパスをホストするラインカードのオンライン挿入または削除 (OIR)
- パスを構成するリンクの削除 (設定による)
- パスを構成するリンクのシャットダウン

マルチパスセッションのパケットを送受信するために使用できる基盤となるメカニズムに対して少なくとも 1 枚のラインカードを有効にするには、**bfd multipath include location location-id** コマンドを設定する必要があります。

BFD マルチパス セッションが、**bfd multipath include** の設定から削除されるか、オンラインで削除されるか、またはメンテナンスモードにされようとしているラインカードでホストされている場合、BFD は、そのラインカードでホストされているすべての BFD マルチパス セッションを別のラインカードに移行しようとします。その場合は、RIB からスタティックルートが削除されてから、BFD セッションが再度確立され、RIB に含まれます。

BFD マルチパスセッションの場合、入力インターフェイスと出力インターフェイスは、ルーティングテーブルの更新に基づいて変更されることがあります。マルチパスセッション BFD パケットを優先的に処理する必要がある場合は、ルータの考えられる入出力インターフェイスを含めて、パス全体の QoS ポリシーを設定する必要があります。

QoS ポリシーは、入力および出力の BFD パケットを優先度レベル 1 のキューまたは優先度レベル 2 のキューに分類する必要があります。同様のアプローチは、BVI での BFD セッションと「バンドル上での VLAN を介した BFD」(つまり、BLB) に適用されます。

例:

```
ipv4 access-list BFD
5 permit udp any any eq 4784
!
class-map match-any BFDCLASS
match access-group ipv4 BFD
!
policy-map BFD
class BFDCLASS
```

```

priority level 1
  police rate 10 kbps
!
interface GigabitEthernet0/2/0/1
service-policy output BFD
service-policy input BFD

```

PW ヘッドエンドとその設定の詳細については、の「*Implementing Virtual Private LAN Services*」モジュールを参照してください。GREの詳細については、の「*Implementing MPLS Layer 2 VPNs*」モジュールを参照してください。

マルチホップパスのBFD

BFD マルチホップ (BFD-MH) は、同じサブネット上にない2つのアドレス間のBFDセッションです。BFD-MH の例には、PE および CE ループバック アドレス間のBFDセッションや、数TTL ホップ離れたルータ間のBFDセッションがあります。BFD マルチホップをサポートするアプリケーションには、外部BGPと内部BGPがあります。BFD マルチホップは、複数のネットワーク ホップにまたがる場合もある任意のパス上のBFDをサポートします。

BFD マルチホップ機能では、複数ホップ (最大255ホップ) 離れた宛先に対する1秒未満の転送障害検出が可能になります。**bfd multihop ttl-drop-threshold** コマンドを使用すると、特定のホップ数を超えるネイバーから送信されたBFDパケットをドロップできます。BFD マルチホップは、BFD シングルホップで現在サポートされているすべてのメディアタイプでサポートされます。

BFD マルチホップの設定

BFD マルチホップセッションは、クライアントによって指定された送信元アドレスと宛先アドレスの一意のペア間で設定されます。IP接続された2つのエンドポイント間でセッションを設定できます。BFD マルチホップでは、グローバルルーティングテーブルとVRFの両方にあるIPv4アドレスがサポートされます。

BFDをBGPとともに使用すると、BFDセッションタイプ (シングルホップまたはマルチホップ) がBGP設定に基づいて設定されます。**eBGP-multihop** キーワードを設定すると、BFDセッションもマルチホップモードで実行されます。それ以外の場合、セッションはシングルホップモードで実行されます。

MPLS トラフィック エンジニアリング LSP を介した BFD

Cisco IOS XR ソフトウェアのMPLS トラフィック エンジニアリング ラベル スイッチドパス (LSP) 機能を介した双方向フォワーディング検出 (BFD) は、MPLS ラベルスイッチドパス LSP データプレーンの障害を検出します。BFD制御パケットに必要なコントロールプレーン処理は、LSP ping メッセージに必要な処理よりも比較的小さいため、BFDを展開すると多数のLSPのデータプレーン障害をより迅速に検出できます。

Cisco IOS XR ソフトウェアでのMPLS TE LSPを介したBFD実装は、*RFC 5884 : MPLS ラベル スイッチドパス (LSP) での Bidirectional Forwarding Detection (BFD)* に基づいています。LSP ping は、MPLS データプレーンの障害を検出し、コントロールプレーンと照合してMPLS LSP データプレーンを確認するための既存のメカニズムです。BFDは、MPLS データプレーンでの

障害の検出に使用できますが、コントロールプレーンと照合する MPLS LSP データプレーンの確認には使用できません。LSP ping と BFD を組み合わせると、多数の LSP 上でデータプレーン障害を迅速に検出できます。

BFD を高速障害検出トラフィックのブラックホールとして使用することでネットワークの信頼性と稼働時間を引き上げるため、MPLS TE LSP を介した BFD は MPLS をマルチサービス トランスポートとして展開し、BFD を高速障害検出メカニズムとして使用するネットワークに使用します。

MPLS TE LSP を介した BFD のサポート：

- BFD 非同期モード (BFD エコーモードはサポートされていません)
- IPv4 のみ (MPLS コアは IPv4 であるため)
- BFD パケットで IP DSCP 6 を伝送 (インターネット制御)
- TE トンネルの起動、再最適化、およびパスの保護のための BFD の使用 (スタンバイおよび FRR)
- 最速の検出時間 (100 ms x 3 = 300 ms)
- BFD セッションが起動した後の任意の定期的な LSP ping の検証
- 保留 BFD 障害パスオプションへのダンプニング
- テールエンドからヘッドエンドへの BFD パケットは、次の 2 つの方法で使用されます。
 - テールエンドからヘッドエンドへの BFD パケットは、IP ルーティングされる (IPv4 マルチホップ：ポート番号 4784)。
 - テールエンドからヘッドエンドへの BFD パケットは、テールエンドからヘッドエンドへのラベルパスを使用して MPLS LDP がコアで使用できる場合は、ラベルが切り替わる (ポート番号 3784)。

バンドルインターフェイス上での BFD 用のエコータイマーの設定

エコータイマーの設定では、バンドルメンバリンク上の IPv4 BFD セッションでのエコーパケットの最小間隔を指定できます。エコータイマー値をグローバルに設定するには、**bfd echo ipv4 bundle-per-member minimum-interval** コマンドを使用します。バンドルイーサネットインターフェイスの最小間隔値をローカルに設定するには、**bfd address-family ipv4 echo minimum-interval** を使用します。



(注) この機能は、メンバリンク単位のバンドルを介したシスコの標準的な BFD モードにのみ適用できます。

これらのコマンドの詳細については、『Cisco ASR 9000 Series Router module of Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference』の「BFD Commands」を参照してください。

次の表に、グローバルおよびローカルのエコ設定の組み合わせによるエコタイマーの動作を示します。

表 2: グローバルおよびローカルのエコ設定を使用したエコタイマーの動作

グローバルエコ最小間隔値 コマンド: bfd echo ipv4 bundle-per-member minimum-interval	ローカルバンドルイーサネット インターフェイス固有のエコ 最小間隔値 コマンド: bfd address-family ipv4 echo minimum-interval	グローバルおよびローカルの 設定に基づいて BoB セッション で使用されるエコ値
未設定	未設定	非同期 * 乗数
グローバル値が非同期 * 乗数 より小さい	未設定	非同期 * 乗数
グローバル値が非同期 * 乗数 を超えている	未設定	グローバル
未設定	ローカル値が非同期 * 乗数 を超えている	ローカル
Not configured	ローカル値が非同期 * 乗数 より小さい	非同期 * 乗数
グローバルが設定されている (任意の値)	ローカル値が非同期 * 乗数 を超えている	ローカル
グローバルが設定されている (任意の値)	ローカル値が非同期 * 乗数 より小さい	非同期 * 乗数



- (注)
- テーブル内の乗数は、リモートの乗数値を示します。
 - 非同期は、ネゴシエートされた非同期の最小間隔値を示します。

R5.3.0 デバイスで、R5.3.0 よりも前のバージョンで実行されているデバイスとの BoB セッションがある場合は、デフォルトのエコタイマー値を保持するか、両方のデバイスで同じ値を設定することをお勧めします。

論理バンドルを介した双方向転送検出

論理バンドル上の双方向フォワーディング検出 (BFD) 機能では、RFC 5880 に基づいて、バンドルインターフェイスを介して BFD を実装および配置します。論理バンドル上の BFD (BLB) 機能は BVLAN 機能を置き換え、純粋な RFC5880 の方法でバンドルインターフェイス上で BFD を実行する他のプラットフォームとの相互運用性に関する特定の問題を解決します。これらのプラットフォームには、Cisco IOS または Cisco Nexus OS ソフトウェアを実行している他のシスコ製品だけでなく、他のベンダーの製品が含まれています。

BLB は、マルチパス (MP) シングルホップセッションです。BLB では、セッションが実行されているバンドルインターフェイスに関する限られた知識しか必要としません。これは、BFD がバンドルを1つの大きなパイプとして処理するためです。BLB を機能させるには、バンドルインターフェイスの IP アドレス、インターフェイス タイプ、および制限に関する情報だけが必要です。バンドルメンバのリスト、メンバの状態、設定されている最小または最大のバンドルリンクなどの情報は必要ありません。

BLB は、IPv4 アドレス、IPv6 グローバルアドレス、および IPv6 リンクローカルアドレスでサポートされます。ソフトウェアの現在のバージョンは、ラインカードごとに合計 200 のセッションをサポートしています (物理および論理のサブインターフェイスの BFD シングルホップ、バンドルを介した BFD (BoB) および BLB を含む)。ラインカードごとの BFD 制御パケットの最大処理能力も、7000 pps (1 秒あたりのパケット数) へと強化されています。



(注) ISSU は、論理バンドルを介した BFD 機能ではサポートされていません。

論理バンドル上の BFD 機能は、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 ではサポートされません。

総称ルーティングカプセル化を介した双方向フォワーディング検出

Generic Routing Encapsulation (GRE) 機能を介して Bidirectional Forwarding Detection (BFD) を使用すると、既存の GRE キープアライブメカニズムよりも迅速にネットワーク障害を検出できます。BFD は、エンドポイントが BFD ピアである GRE トンネルを介してセッションを確立します。BFD は障害検出時にトンネルを停止させますが、障害が解消されると、トンネル キープアライブメカニズムによってトンネルを回復させることができます。BFD は、IPv4 GRE トンネルモードでのみサポートされています。

BFD セッションの送信元と宛先は、GRE トンネルの IPv4 アドレスと同じになります。

トンネルキープアライブが有効になっている場合、GRE トンネルで BFD を有効にすることも、その逆もできません。

GRE トンネリングプロトコルは、さまざまなプロトコルパケットタイプを IP トンネルの内部にカプセル化し、IP インターネットワーク上のリモートポイントにある 2 台のルータ間に仮想ポイントツーポイントリンクを作成します。GRE を使用すると、自身のコア ネットワーク内で MPLS を実行していないサービス プロバイダーが VPN サービスを提供できるようになります。

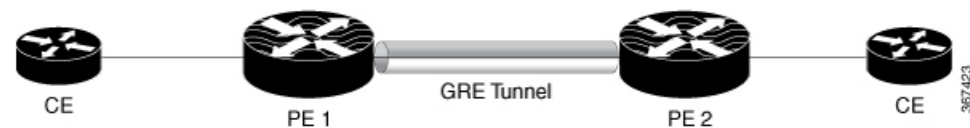
GRE 上の BFD 機能は、Cisco ASR 9000 シリーズ SPA インターフェイスプロセッサ 700 ではサポートされません。

BFD は、RFC5880 に従った、GRE 番号付きインターフェイス上の IPv4 シングルホップバージョン 1 非同期モードを提供します。

Generic Routing Encapsulation を介した双方向フォワーディング検出の設定

次の項では、Generic Routing Encapsulation (GRE) を介した双方向フォワーディング検出 (BFD) の設定方法を示します。

図 4: GRE を介した BFD



設定例

PE1 ルータで次のステップを設定します。

```
Router# configure
Router(config)# bfd
Router(config-bfd)# multipath include location 0/0/CPU0
Router(config-bfd)# exit
Router(config)# interface tunnel-ip 100
Router(config-if)# ipv4 address 10.0.0.1 255.255.255.252
Router(config-if)# tunnel source Loopback 100
Router(config-if)# tunnel destination 10.2.2.2
Router(config-if)# tunnel bfd destination 10.0.0.2
Router(config-if)# tunnel bfd minimum-interval 300
Router(config-if)# tunnel bfd multiplier 5
Router(config-if)# tunnel bfd period 5
Router(config-if)# tunnel bfd retry 2
Router(config-if)# commit
```

PE2 ルータで次のステップを設定します。

```
Router# configure
Router(config)# bfd
Router(config-bfd)# multipath include location 0/0/CPU0
Router(config-bfd)# exit
Router(config)# interface tunnel-ip 100
Router(config-if)# ipv4 address 10.0.0.2 255.255.255.252
Router(config-if)# tunnel source Loopback 100
Router(config-if)# tunnel destination 10.1.1.1
Router(config-if)# tunnel bfd destination 10.0.0.1
Router(config-if)# tunnel bfd minimum-interval 300
Router(config-if)# tunnel bfd multiplier 5
Router(config-if)# tunnel bfd period 5
Router(config-if)# tunnel bfd retry 2
Router(config-if)# commit
```

実行コンフィギュレーション

/* The following is the running configuration from PE1 Router */


```
bfd
 multipath include location 0/0/CPU0
!
interface tunnel-ip 100
 ipv4 address 100.0.0.1 255.255.255.252
 tunnel source Loopback 100
 tunnel destination 10.2.2.2
 tunnel bfd destination 10.0.0.2
 tunnel bfd minimum-interval 300
 tunnel bfd multiplier 5
 tunnel bfd period 5
 tunnel bfd retry 2

/* The following is the running configuration from PE2 Router */

bfd
 multipath include location 0/0/CPU0
!
interface tunnel-ip 100
 ipv4 address 100.0.0.2 255.255.255.252
 tunnel source Loopback 100
 tunnel destination 10.1.1.1
 tunnel bfd destination 10.0.0.1
 tunnel bfd minimum-interval 300
 tunnel bfd multiplier 5
 tunnel bfd period 5
 tunnel bfd retry 2
```

確認

```
Router# show interfaces tunnel-ip 1
Mon Jul  9 10:54:06.952 IST
tunnel-ipl is up, line protocol is up
  Interface state transitions: 1
  Hardware is Tunnel
  Internet address is 20.1.1.2/24
  MTU 1500 bytes, BW 100 Kbit (Max: 100 Kbit)
    reliability 255/255, txload 2/255, rxload 2/255
  Encapsulation TUNNEL_IP, loopback not set,
  Last link flapped 00:03:54
  Tunnel TOS 0
  Tunnel mode GRE IPV4
  Keepalive is enabled, interval 10 seconds, maximum retry 3
  Tunnel source 10.0.0.2, destination 10.1.1.1/32
  Tunnel TTL 255
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 1000 bits/sec, 3 packets/sec
  5 minute output rate 1000 bits/sec, 3 packets/sec
    999 packets input, 75088 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
  Received 0 broadcast packets, 0 multicast packets
  1001 packets output, 51380 bytes, 0 total output drops
  Output 0 broadcast packets, 0 multicast packets

Router# show bfd session interface tenGigE 0/1/1/0.200 detail

I/f: TenGigE0/1/1/0.200, Location: 0/0/CPU0
Dest: 10.1.1.2
Src: 10.0.0.2
State: UP for 0d:0h:6m:9s, number of times UP: 1
Session type: PR/V4/SH
Received parameters:
```

```

Version: 1, desired tx interval: 300 ms, required rx interval: 300 ms
Required echo rx interval: 0 ms, multiplier: 3, diag: None
My discr: 2148532226, your discr: 2148335671, state UP, D/F/P/C/A: 0/0/0/1/0
Transmitted parameters:
Version: 1, desired tx interval: 15 ms, required rx interval: 15 ms
Required echo rx interval: 0 ms, multiplier: 3, diag: None
My discr: 2148335671, your discr: 2148532226, state UP, D/F/P/C/A: 0/1/0/1/0
Timer Values:
Local negotiated async tx interval: 300 ms
Remote negotiated async tx interval: 300 ms
Desired echo tx interval: 0 s, local negotiated echo tx interval: 0 ms
Echo detection time: 0 ms(0 ms*3), async detection time: 900 ms(300 ms*3)
Local Stats:
Intervals between async packets:
  Tx: Number of intervals=4, min=1 ms, max=346 s, avg=88 s
      Last packet transmitted 23 s ago
  Rx: Number of intervals=11, min=1 ms, max=346 s, avg=32 s
      Last packet received 23 s ago
Intervals between echo packets:
  Tx: Number of intervals=0, min=0 s, max=0 s, avg=0 s
      Last packet transmitted 0 s ago
  Rx: Number of intervals=0, min=0 s, max=0 s, avg=0 s
      Last packet received 0 s ago
Latency of echo packets (time between tx and rx):
  Number of packets: 0, min=0 ms, max=0 ms, avg=0 ms
Session owner information:

```

Client	Interval	Desired Multiplier	Interval	Adjusted Multiplier
tunl_gre_ma	15 ms	3	15 ms	3

```
Router# show bfd client
```

```

Mon Jul  9 10:55:16.025 IST
Name                Node                Num sessions
-----
L2VPN_ATOM          0/0/CPU0           0
bundlemgr_distrib   0/0/CPU0           0
object_tracking     0/0/CPU0           0
pim6                 0/0/CPU0           0
pim                  0/0/CPU0           0
tunl_gre_ma         0/0/CPU0           1

```

```
Router# show tunnel ip keepalive
```

```

Mon Jul  9 10:54:30.005 IST

---- Tunnel GRE Keepalive Database ----

interface tunnel-ip1
 tunnel interface/basecaps state UP/UP
 tunnel ifhandle 0x90
 tunnel source 10.0.0.2
 tunnel destination 10.1.1.1
 tunnel transport vrf id 0x60000000
 tunnel transport vrf table id 0xe0000000
 tunnel ttl 255
 tunnel flags 0x1400
 tunnel keepalive max retries 3
 tunnel keepalive period 10
 tunnel keepalive state 0x2
 tunnel keepalive fail count 0
 tunnel keepalive packets sent 27

```

```
Timestamp of last KA sent Mon Jul 9 10:54:21 2018
tunnel keepalive packets received 24
Timestamp of last KA received Mon Jul 9 10:54:21 2018
```

関連コマンド

- **bfd minimum-interval**
- **bfd multiplier**
- **tunnel bfd**

双方向フォワーディング検出 IPv6 マルチホップ

双方向フォワーディング検出 (BFD) IPv6 マルチホップ機能では、BFD ネイバーを物理的または論理的に複数ホップ離れた場所に配置できる IPv6 マルチホップ BFD セッションが可能になります。BFD ネイバーに到達するために、複数のパスを使用できます。BFD パケットは、対応する BFD セッションをホストしている可能性のあるラインカードで受信されます。あるラインカード内の BFD エージェントが、別のラインカード上の出力インターフェイスから BFD パケットを送信することが必要になる場合があります。

IPv6 マルチホップに対する BFD のサポートは、BFD IPv4 マルチホップと同様です。BFD IPv6 マルチホップは、ASR 9000 イーサネット ラインカードおよび ASR 9000 拡張イーサネット ラインカードでサポートされます。

BFD IPv6 マルチホップ機能は、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 ではサポートされません。

BFD IPv6 マルチホップでは、BFD ネイバーが常に 1 ホップ離れていて、ラインカード内の BFD エージェントが常に同じラインカード上のローカルインターフェイス経由で BFD パケットを受信または送信する、単一パス IPv6 BFD セッションの制約事項が解消されます。

IPv6 マルチホップリンクの BFD スイッチングメカニズムは、BFD パケットがあるエンドポイント ノードから他のエンドポイント ノードに送信されたときに使用されます。BFD パンティングメカニズムは、BFD パケットがリモートエンドポイント ノードで受信されたときに使用されます。

疑似回線ヘッドエンドを介した BFD

疑似回線ヘッドエンド (BFD_oPWHE) を介した Bidirectional Forwarding Detection 機能により、カスタマーエッジ (CE) から疑似回線ヘッドエンド (S-PE) のリンクを介した BFD サポートが可能になり、eBGP ネイバー間のパスに沿って迅速に障害を検出できます。

PWHE を介した BFD は、ASR 9000 拡張イーサネットラインカードでのみサポートされています。

PWHE を介した BFD は次をサポートしています。

- CE と PWHE PE 間のエンドツーエンドの障害検出のための疑似回線単位の BFD セッション

- BFDv4 for IPv4 と BFDv6 for IPv6 (スタティックと BGP)
- PWHE を介した BFD 非同期モード
- 擬似回線 VC タイプ 4 およびタイプ 5

PWHEを動作させるには、PWHE 汎用インターフェイスリストに含まれているラインカードのいずれかで BFD エージェントをホストする必要があります。BFD マルチパスは、汎用インターフェイスリストに含まれているラインカード用に設定する必要があります。

BFD マルチパスセッションをホストして、PWHE を介した BFD を有効にするために特定のラインカードを含めるには、`bfd multipath include location node-id` コマンドを使用します。

サテライトインターフェイスを介した BFD

サテライトインターフェイスを介した双方向フォワーディング検出 (BFD) 機能は、サテライトラインカード上で BFD をサポートします。サテライトインターフェイスは、仮想 (バンドル) インターフェイスと呼ばれています。BFD はマルチパス インフラストラクチャを使用して、サテライトラインカード上の BFD をサポートします。サテライトを介した BFD はマルチパス (MP) シングルホップセッションであり、IPv4 アドレス、IPv6 グローバルアドレス、および IPv6 リンクローカルアドレスでサポートされています。サテライトを介した BFD は、ASR 9000 拡張イーサネットラインカードでのみサポートされており、また、非同期モードでサポートされています。エコーモードでは、サテライトを介した BFD はサポートされていません。



- (注)
- `bfd multipath include location node-id` コマンドは ASR 9000 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。したがって、サテライトインターフェイスを介した BFD 機能は、ASR 9000 イーサネットラインカードでは動作しません。
 - サテライトインターフェイスを介した BFD は、nV エッジシステムではサポートされていません。
 - nV サテライトのアクセスポートバンドルは、シャーシ間リンク (ICL) がバンドル (バンドルトポロジを介したバンドル) でもある場合、バンドルを介した BFD (BoB) をサポートしません。

IRB を介した BFD

VLAN でルータを使用するには、ルータが VLAN ヘッダーを維持した状態で、あるインターフェイスから別のインターフェイスにフレームを転送可能である必要があります。レイヤ 3 (ネットワーク層) プロトコルをルーティングするようにルータを設定する場合は、フレームを受信するインターフェイスで VLAN と MAC レイヤが終端します。MAC 層のヘッダーは、ルータがネットワーク層プロトコルをブリッジングする場合に維持できます。ただし、通常のブリッジングでも VLAN ヘッダーは終端されます。

Cisco IOS XR ソフトウェア リリース 5.1.0 以降の Integrated Routing Bridging (IRB) 機能を使用すると、同じインターフェイス上の同じネットワーク層プロトコルをルーティングし、ブリッジングするようにルータを設定できます。これにより、VLAN ヘッダーは、あるインターフェイスから別のインターフェイスへのルータを通過する間、フレームで維持されるようになります。IRB は、ブリッジグループ仮想インターフェイス (BVI) により、ブリッジドメインとルーテッドドメイン間でルーティングする機能を提供します。BVI は、ルータ内の仮想インターフェイスであり、ブリッジングをサポートしないが、ルータ内のルーテッドインターフェイスに相当するブリッジグループを代表する、正常なルーテッドインターフェイスのように動作します。BVI のインターフェイス番号は、仮想インターフェイスが代表するブリッジグループの番号です。この番号が BVI とブリッジグループ間のリンクになります。

BVI はルーテッドインターフェイスとしてブリッジグループを代表するため、ネットワーク層アドレスのようなレイヤ 3 (L3) 特性のみにより設定する必要があります。同様に、プロトコルのブリッジングのために設定されたインターフェイスは、どのような L3 特性によっても設定してはなりません。

IRB を介した BFD はマルチパスのシングルホップセッションです。BFD マルチパスセッションでは、BFD を仮想インターフェイス上か、または複数ホップ離れたインターフェイス間に適用できます。Cisco IOS XR ソフトウェアの BFD マルチホップは、「RFC 5883: マルチホップパスの双方向転送検出 (BFD) (RFC 5883—*Bidirectional Forwarding Detection (BFD) for Multihop Paths*)」に基づいています。IRB を介した BFD は、IPv4 アドレス、IPv6 グローバルアドレス、および IPv6 リンクローカルアドレスでサポートされています。IRB を介した BFD は非同期モードでのみサポートされており、エコーモードはサポートされていません。IRB を介した BFD 機能は、ASR 9000 拡張イーサネットラインカードでのみサポートされています。

メンバリンク単位のバンドルを介した BFD

メンバリンク単位のバンドルを介した BFD (BoB) モードは、異なるプラットフォーム間で相互運用可能なリンク集約 (LAG) メンバリンクの標準ベースの高速障害検出機能です。これにより、Cisco または IETF 標準のいずれかを使用するためのメンバリンク単位のモードを選択するオプションが提供されます。この機能は、Cisco ASR 9000 拡張イーサネットラインカードでのみサポートされています。



- (注)
- システム内のすべてのバンドルは、任意の単一時点で複数のモードに属することができます。
 - バンドルを介した BoB を設定するためのグローバルコマンドは、リリース 5.3.0 までのみ使用できます。5.3.1 以降のリリースでは、バンドル単位でバンドルを介した BFD の CISCO/IETF モードのサポートを設定するオプションが提供されています。
 - Cisco モードでは CDP MAC を使用しますが、IETF モードでは IANA によって割り当てられた MAC が使用されます。
 - バンドルを介した Cisco BFD セッションでは宛先 UDP ポートとして 3784 が使用され、バンドルを介した IETF BFD セッションでは宛先 UDP ポートとして 6784 が使用されます。

制限事項

次の制限は、メンバリンク単位のバンドルを介した BFD モード機能に適用されます。

- Cisco ASR 9000 拡張イーサネットラインカードでのみサポートされます。
- BFD エコーモードはサポートされていません。
- IPv6 は IETF モードでサポートされており、シスコモードではサポートされていません。
- モードの変更は、新しいセッションにのみ適用されます。既存のセッションに対してモードの変更を適用するには、セッションを削除してから再作成します。
- メンバインターフェイス上の BFD セッションは、1つのモード（Cisco モードまたは IETF モード）にのみ属することができます。同じバンドル内でのモードの混在はサポートされていません。

バンドルを介した BFD の CISCO/IETF モードのバンドル単位でのサポート

BFD over Bundle (BoB) モードは、異なるプラットフォーム間で相互運用可能なリンクアグリゲーション (LAG) メンバリンクの標準ベースの高速障害検出です。バンドルごとの BoB サポートでは、さまざまなシステムでリロードやプロセスの再起動を必要とせずに、バンドルごとに Cisco または IETF 標準を選択するオプションが提供されます。デフォルトは Cisco モードです。



(注) バンドルを介した CISCO/IETF BoB を設定するための以前のリリースで使用可能なグローバルレベルのコマンドはリリース 5.3.1 以降、廃止されています。スムーズにアップグレードできるようにするため、バンドルをインターフェイスレベルで設定することをお勧めします。

- Cisco モードでは CDP MAC を使用しますが、IETF モードでは IANA によって割り当てられた MAC が使用されます。
- バンドルを介した Cisco BFD セッションでは宛先 UDP ポートとして 3784 が使用され、バンドルを介した IETF BFD セッションでは宛先 UDP ポートとして 6784 が使用されます。

制約事項

次の制限はバンドルを介した BFD モード機能に適用されます。

- Cisco ASR 9000 拡張イーサネットラインカードでのみサポートされます。
- BFD モードの変更（Cisco から IETF およびその逆）は、バンドルの BFD 状態が「ダウン (down)」または「動作不能 (nonoperational)」の場合にのみ実行されます。



(注) BoB を動作不能にするには、**no bfd address-family ipv4 fast-detect** コマンドを使用します。また、特定のバンドルでシャットダウンを設定することによっても、バンドルを「ダウン」状態に設定できます。

- バンドルが新しい BFD モードの変更を受け入れるようにするには、既存の BFD セッションをダウンさせてから、再作成する必要があります。
- BFD エコーモードは、バンドルを介した IETF BFD (BoB) セッションではサポートされていません。

BFD ダンプニング

双方向フォワーディング検出 (BFD) は、ネイバーに対する到達可能性の障害を迅速に認識して通知するために、ルーティングプロトコルで使用されているメカニズムです。BFD でクライアントの到達可能性ステータスの変更が検出されると、そのネイバーがすぐに通知を受けます。小さい障害であってもコンバージェンスに影響を与えないよう、ルーティングテーブルの変更を最小限にすることが重要になる場合があります。過剰にフラップが発生する不安定なリンクは、ネットワークの他のデバイスにかなりの処理リソースを消費させ、ルーティングプロトコルでフラッピングリンクの状態との同期が失われる原因になる可能性があります。

BFD ダンプニング機能によって、設定可能な指数的遅延メカニズムが導入されます。このメカニズムは、BFD でのリモートノードの到達可能性イベントのフラッピングによる過度な影響を抑えるように設計されています。BFD ダンプニング機能を使用して、ネットワークオペレータは自動的に特定の BFD セッションをダンプニングして BFD クライアントへの過剰な通知を防ぐことができ、このようにして、ネットワークが不必要に不安定にならないようにします。BFD クライアントへの通知のダンプニングにより、モニタリング中のセッションがフラッピングを停止して安定するまで BFD の通知を抑制します。

BFD ダンプニング機能を、特に高速インターフェイスでルーティング クライアントとともに設定すると、ネットワーク全体のコンバージェンス時間と安定性が向上します。BFD ダンプニングは、IPv4/シングルホップ/マルチホップ、Multiprotocol Label Switching-Transport Profile (MPLS-TP)、Pseudo Wire (PW) Virtual Circuit Connection Verification (VCCV) を含む、BFD セッションのすべてのタイプに適用できます。

BFD セッションダンプニング

BFD テンプレート レベル (シングルホップとマルチホップの両方のテンプレート) で BFD ダンプニング機能を設定できます。ダンプニングは、BFD テンプレートを使用するすべてのセッションに適用されます。セッションをダンプニングする場合は、新しいセッションに対してダンプニングしない新しい BFD テンプレートを使用する必要があります。デフォルトでは、テンプレートのダンプニング機能は有効になっていません。

BFD ハードウェアオフロード

双方向フォワーディング検出 (BFD) ハードウェアオフロード機能を使用すると、ASR 9000 拡張イーサネットラインカードのネットワーク処理ユニットに対する非同期 BFD 送信 (Tx) と受信 (Rx) をオフロードできます。BFD ハードウェアオフロードにより拡張性が改善し、ルーティングテーブル再計算のために迅速な障害検出パケット (メッセージ) をルーティングプロトコルに送信することで、全体的なネットワーク コンバージェンス時間が短縮されます。

次の非同期 BFD セッションは、ASR 9000 拡張イーサネットラインカード上のネットワーク処理ユニットにオフロードされます。

- 物理インターフェイスと VLAN インターフェイスを介した BFD IPv4 セッション。
- 物理インターフェイスと VLAN インターフェイスを介した BFD IPv6 セッション。
- MPLS TP LSP シングルパス (SP) セッションを介した BFD。

BFD ハードウェア オフロード モードは、**hw-module bfd-hw-offload enable** コマンドを使用して ASR 9000 拡張イーサネットラインカードで有効になります。cXR デバイスの管理モードと、eXR デバイスのグローバルコンフィギュレーションモードで **hw-module bfd-hw-offload enable** コマンドを設定します。設定を有効にするには、コマンドを実行した後にラインカードをリロードします。



(注) BFD ハードウェアオフロードモードを有効にした後は、ASR 9000 拡張イーサネットラインカードをリロードする必要があります。

BFD ハードウェアオフロードは、BFD セッションの 7 つのタイマー間隔をサポートしています。サポートされる最小タイマー間隔は 3.3 ミリ秒、最大タイマー間隔は 30 秒です。次の表に、タイマー間隔によって異なる、サポート対象 BFD セッション数の詳細を示します。

BFD セッション	タイマー間隔	ラインカードでサポートされているセッション数	ネットワーク処理ユニットでサポートされているセッション
IPv4、IPv6、MPLS-TP	3.3 ミリ秒	600	300
IPv4、IPv6	15 ミリ秒	2000	1000
IPv4、IPv6	50 ミリ秒	8000	3000
IPv4、IPv6	300 ミリ秒	8000	3000
IPv4、IPv6	1 秒	8000	3000
IPv4、IPv6	2 秒	8000	3000
IPv4、IPv6	30 秒	8000	3000

制約事項

- ハードウェアオフロードされたセッションは、エコーモードをサポートしていません。
- BFD セッションがサポートしているタイマー間隔は7つのみです。
- In-Service Software Upgrade (ISSU) は、BFD ハードウェアオフロードされたセッションをサポートしていません。
- バンドルメンバリンクを介してハードウェアオフロードされた BFD は、Cisco モードをサポートしていません。

BFD オブジェクトトラッキング

オブジェクトトラッキングは、リモート IP アドレスの到達可能性を追跡する BFD をサポートするように拡張されました。これにより、BFD は数ミリ秒程度で検出を実行できるため、完全な検出と HSRP スイッチオーバーを 1 秒未満の時間内で実行できます。

BFD の設定方法

BFD 設定時の注意事項

BFD を設定する前に、次の注意事項を考慮してください。

- BFD を使用した FRR/TE、FRR/IP、および FRR/LDP は、POS インターフェイスおよびイーサネット インターフェイスでサポートされます。
- Cisco IOS XR ソフトウェアで BFD ネイバーを確立するには、BFD をダイナミック ルーティング プロトコルの下で、またはスタティック ルートを使用して設定する必要があります。
- BFD セッションの 1 秒当たりのパケット数 (pps) での最大レートはラインカードに依存します。BFD をサポートする複数のラインカードがある場合、システム単位の BFD セッションの最大レートは、サポートされるラインカードレートにラインカードの数を掛けた値です。
BFD スケール値を確認するには、**show bfd summary** コマンドを使用します。
- バンドル内のメンバの最大数は 64 です。
- BFD を OSPF とともに使用する場合は、次の注意事項を考慮してください。
 - BFD がネイバーから指定ルータ (DR) またはバックアップ DR (BDR) へのセッションを確立するのは、ネイバーの状態がフルである場合だけです。
 - BFD は、DR 以外のネイバー間にセッションを確立しません (たとえば、その OSPF 状態がどちらも双方向である場合)。



注意 特定のインターフェイスで BFD を Unicast Reverse Path Forwarding (uRPF) と併用している場合は、**echo disable** コマンドを使用して、そのインターフェイスでのエコーモードを無効にする必要があります。そうしないと、エコーパケットは拒否されます。詳細については、「[エコーモードの無効化](#)」の項を参照してください。IPv4 インターフェイスでの IPv4 uRPF のチェックを有効または無効にするには、インターフェイス コンフィギュレーション モードで **[no] ipv4 verify unicast source reachable-via** コマンドを使用します。



(注) **echo disable** コマンドは、論理バンドル (BLB) を介した BFD ではサポートされていません。

ダイナミックルーティングプロトコルの下での、またはスタティックルートを使用した BFD の設定

BGP ネイバーでの BFD のイネーブル化

BFD は、ネイバー単位またはインターフェイス単位でイネーブルにすることができます。このタスクでは、隣接ルータで BGP の BFD をイネーブルにする方法について説明します。インターフェイスごとに BFD を有効にするには、「[インターフェイスでの OSPF への BFD の有効化](#)」の項にある手順を使用します。



(注) BFD 近接ルータの設定は、BGP でのみサポートされます。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **bfd minimum-interval** *milliseconds*
4. **bfd multiplier** *multiplier*
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **bfd fast-detect**
8. **commit**

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 <i>autonomous-system-number</i> 例 : RP/0/RSP0/cpu 0: router(config)# router bgp 120	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の設定を行えます。 現在のルータの <i>autonomous-system-number</i> を取得するには、EXEC モードで show bgp コマンドを使用します。
ステップ 3	bfd minimum-interval <i>milliseconds</i> 例 : RP/0/RSP0/cpu 0: router(config-bgp)# bfd minimum-interval 6500	BFD の最小間隔を設定します。有効値の範囲は 15 ~ 30000 ミリ秒です。
ステップ 4	bfd multiplier <i>multiplier</i> 例 : RP/0/RSP0/cpu 0: router(config-bgp)# bfd multiplier 7	BFD 係数を設定します。
ステップ 5	neighbor <i>ip-address</i> 例 : RP/0/RSP0/cpu 0: router(config-bgp)# neighbor 172.168.40.24	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。 この例では、IP アドレス 172.168.40.24 を BGP ピアとして設定しています。
ステップ 6	remote-as <i>autonomous-system-number</i> 例 : RP/0/RSP0/cpu 0: router(config-bgp-nbr)# remote-as 2002	ネイバーを作成し、そのネイバーをリモート自律システムに割り当てます。 この例では、設定されるリモート自律システムは 2002 です。
ステップ 7	bfd fast-detect 例 : RP/0/RSP0/cpu 0: router(config-bgp-nbr)# bfd fast-detect	ローカルネットワーク装置と、ステップ 5 で IP アドレスを BGP ピアとして設定したネイバー間での BFD を有効にします。 ステップ 5 の例では、IP アドレス 172.168.40.24 が BGP ピアとして設定されています。この例では、ローカルネットワーク装置とネイバー 172.168.40.24 間での BFD が有効になります。
ステップ 8	commit	

インターフェイスでの OSPF への BFD の有効化

次に、Open Shortest Path First (OSPF) での BFD を特定のインターフェイスで設定する手順について説明します。この方法の手順は、コマンドモードが異なる点を除き、IS-IS および MPLS-TE での BFD を設定する手順と共通です。



(注) インターフェイス単位での BFD の設定は、OSPF、OSPFv3、IS-IS、MPLS-TE でのみサポートされます。OSPFv3 インターフェイスでの BFD の設定については、[特定インターフェイスでの OSPFv3 の BFD の有効化](#)を参照してください。

手順の概要

1. **configure**
2. **bfd multipath include locationnode-id**
3. **router ospf process-name**
4. **bfd minimum-interval milliseconds**
5. **bfd multiplier multiplier**
6. **area area-id**
7. **interface type interface-path-id**
8. **bfd fast-detect**
9. **commit**
10. **show run router ospf**

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	bfd multipath include locationnode-id 例： <pre>RP/0/RSP0/cpu 0: router(config)# bfd multipath include location 0/0/CPU0</pre>	(任意) インターフェイス上の指定されたバンドルに BFD マルチパスを有効にします。この手順は、バンドルインターフェイスに必要です。 (注) <ul style="list-style-type: none"> • この手順は、バンドルインターフェイスにメンバリンクがあるすべてのラインカードに対して繰り返す必要があります。
ステップ 3	router ospf process-name 例： <pre>RP/0/RSP0/cpu 0: router(config)# router ospf 0</pre>	OSPF 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、OSPF ルーティングプロセスの設定を行えます。 現在のルータの process-name を取得するには、EXEC コンフィギュレーション モードで show ospf コマンドを使用します。

	コマンドまたはアクション	目的
		(注) <ul style="list-style-type: none"> IS-IS または MPLS-TE での BFD を設定するには、対応するコンフィギュレーションモードを開始します。たとえば、MPLS-TE の場合は、MPLS-TE コンフィギュレーションモードを開始します。
ステップ 4	bfd minimum-interval <i>milliseconds</i> 例 : RP/0/RSP0/cpu 0: router(config-ospf)# bfd minimum-interval 6500	BFD の最小間隔を設定します。有効値の範囲は 15 ~ 30000 ミリ秒です。 この例では、BFD の最小間隔を 6500 ミリ秒に設定しています。
ステップ 5	bfd multiplier <i>multiplier</i> 例 : RP/0/RSP0/cpu 0: router(config-ospf)# bfd multiplier 7	BFD 係数を設定します。 この例では、BFD 係数を 7 に設定しています。
ステップ 6	area <i>area-id</i> 例 : RP/0/RSP0/cpu 0: router(config-ospf)# area 0	Open Shortest Path First (OSPF) 領域を設定します。 <i>area-id</i> を OSPF エリア識別子に置き換えます。
ステップ 7	interface <i>type interface-path-id</i> 例 : RP/0/RSP0/cpu 0: router(config-ospf-ar)# interface gigabitEthernet 0/3/0/1	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て、インターフェイス名と <i>rack/slot/module/port</i> 表記を指定します。 <ul style="list-style-type: none"> この例では、モジュラサービスカードスロット 3 にあるギガビットイーサネットインターフェイスを示しています。
ステップ 8	bfd fast-detect 例 : RP/0/RSP0/cpu 0: router(config-ospf-ar-if)# bfd fast-detect	隣接する転送エンジン間のパスで障害を検出するために、BFD をイネーブルにします。
ステップ 9	commit	
ステップ 10	show run router ospf 例 : RP/0/RSP0/cpu 0: router(config-ospf-ar-if)# show run router ospf	適切なインターフェイスで BFD がイネーブルになっていることを確認します。

特定インターフェイスでの OSPFv3 の BFD の有効化

次に、OSPFv3 での BFD を特定のインターフェイスで設定する手順について説明します。この方法の手順は、コマンドモードが異なる点を除き、IS-IS および MPLS-TE での BFD を設定する手順と共通です。



(注) インターフェイス単位での BFD の設定は、OSPF、OSPFv3、IS-IS、MPLS-TE でのみサポートされます。OSPF インターフェイスでの BFD の設定については、[インターフェイスでの OSPF への BFD の有効化](#)を参照してください。

手順の概要

1. **configure**
2. **router ospfv3 process-name**
3. **bfd minimum-interval milliseconds**
4. **bfd multiplier multiplier**
5. **area area-id**
6. **interface type interface-path-id**
7. **bfd fast-detect**
8. **commit**
9. **show run router ospfv3**

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 ospfv3 process-name 例 : <pre>RP/0/RSP0/cpu 0: routerconfig)# router ospfv3 0</pre>	OSPFv3 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、OSPFv3 ルーティングプロセスの設定を行えます。 現在のルータの process name を取得するには、EXEC モードで show ospfv3 コマンドを使用します。 (注) <ul style="list-style-type: none"> • IS-IS または MPLS-TE での BFD を設定するには、対応するコンフィギュレーションモードを開始します。たとえば、MPLS-TE の場合は、MPLS-TE 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	bfd minimum-interval milliseconds 例 :	BFD の最小間隔を設定します。有効値の範囲は 15 ~ 30000 ミリ秒です。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config-ospfv3)# bfd minimum-interval 6500	この例では、BFD の最小間隔を 6500 ミリ秒に設定しています。
ステップ 4	bfd multiplier multiplier 例： RP/0/RSP0/cpu 0: router(config-ospfv3)# bfd multiplier 7	BFD 係数を設定します。 この例では、BFD 係数を 7 に設定しています。
ステップ 5	area area-id 例： RP/0/RSP0/CPU0:router(config-ospfv3)# area 0	OSPFv3 領域を設定します。 <i>area-id</i> は、OSPFv3 エリア識別子に置き換えます。
ステップ 6	interface type interface-path-id 例： RP/0/RSP0/cpu 0: router(config-ospfv3-ar)# interface gigabitEthernet 0/1/5/0	インターフェイス コンフィギュレーション モードを開始して、インターフェイス名と <i>rack/slot/module/port</i> 表記を指定します。 <ul style="list-style-type: none">この例では、モジュラ サービス カード スロット 1 にあるギガビットイーサネット インターフェイスを示しています。
ステップ 7	bfd fast-detect 例： RP/0/RSP0/cpu 0: router(config-ospfv3-ar-if)# bfd fast-detect	隣接する転送エンジン間のパスで障害を検出するために、BFD をイネーブルにします。
ステップ 8	commit	
ステップ 9	show run router ospfv3 例： RP/0/RSP0/cpu 0: router(config-ospfv3-ar-if)# show run router ospfv3	適切なインターフェイスで BFD が有効になっていることを確認します。

スタティック ルートでの BFD のイネーブル化

次に、スタティック ルートでの BFD をイネーブルにする手順について説明します。



(注) バンドル VLAN セッションは、間隔 250 ms、係数 3 の場合のみに制限されます。これよりも強力なパラメータは使用できません。

手順の概要

1. **configure**
2. **router static**
3. **address-family ipv4 unicast address nexthop bfd fast-detect [minimum-interval interval] [multiplier multiplier]**
4. **vrf vrf-name**
5. **address-family ipv4 unicast address nexthop bfd fast-detect**
6. **commit**

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 static 例： RP/0/RSP0/cpu 0: router(config)# router static	スタティック ルート 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、スタティック ルーティングの設定を行えます。
ステップ 3	address-family ipv4 unicast address nexthop bfd fast-detect [minimum-interval interval] [multiplier multiplier] 例： RP/0/RSP0/cpu 0: router(config-static)# address-family ipv4 unicast 0.0.0.0/0 2.6.0.1 bfd fast-detect minimum-interval 1000 multiplier 5	<p>指定の IPV4 ユニキャスト宛先アドレスプレフィックスおよびフォワーディング ネクストホップアドレスで BFD 高速検出を有効にします。</p> <ul style="list-style-type: none"> • ネクストホップが確実に同じ hello 間隔で割り当てられるようにするには、オプションの minimum-interval キーワードと引数を含めません。<i>interval</i> 引数は、間隔をミリ秒単位で指定する数字に置き換えてください。有効値の範囲は 10 ~ 10,000 です。 • ネクストホップが確実に同じ検出乗数で割り当てられるようにするには、オプションの multiplier キーワード引数を含めません。<i>multiplier</i> 引数は、検出係数を指定する数字に置き換えてください。有効値の範囲は 1 ~ 10 です。 <p>(注) バンドル VLAN セッションは、間隔 250 ms、係数 3 の場合のみに制限されます。これよりも強力なパラメータは使用できません。</p>
ステップ 4	vrf vrf-name 例： RP/0/RSP0/cpu 0: router(config-static)# vrf vrf1	VPN ルーティングおよび転送 (VRF) インスタンスを指定して、その VRF に対するスタティック ルート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	address-family ipv4 unicast address nexthop bfd fast-detect 例 : RP/0/RSP0/cpu 0: router(config-static-vrf)# address-family ipv4 unicast 0.0.0.0/0 2.6.0.2	指定の IPv4 ユニキャスト宛先アドレスプレフィックスおよびフォワーディングネクストホップアドレスで BFD 高速検出を有効にします。
ステップ 6	commit	

IPv6 静的ルートでの BFD の有効化

次に、IPv6 静的ルートでの BFD の有効化を説明する設定例を示します。

```
RP/0/RSP0/cpu 0: router# configure
RP/0/RSP0/cpu 0: router(config)# router static
RP/0/RSP0/cpu 0: router(config-static)# address-family ipv6 unicast 1011:17e4::1/128
ab11:15d2::2 bfd fast-detect minimum-interval 50 multiplier 3
RP/0/RSP0/cpu 0: router(config-static)# commit
```

バンドルメンバリンクでの BFD の設定

バンドルメンバリンクで BFD を設定するための前提条件

バンドルメンバである物理インターフェイスは、間にスイッチを使用せずにピアルータ間で直接接続している必要があります。

バンドルの BFD 宛先アドレスの指定

バンドルの BFD 宛先アドレスを指定するには、次の手順を実行します。

手順の詳細

手順の概要

1. **configure**
2. **interface Bundle-Ether | Bundle-POS] bundle-id**
3. **bfd address-family ipv4 destinationip-address**
4. **commit**

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	interface Bundle-Ether Bundle-POS] bundle-id 例 :	指定したバンドル ID のインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	
ステップ 3	bfd address-family ipv4 destination <i>ip-address</i> 例： RP/0/RSP0/cpu 0: router(config-if)# bfd address-family ipv4 destination 10.20.20.1	接続されたリモートシステムでバンドルインターフェイスに割り当てられたプライマリ IPv4 アドレスを指定します。ここで、 <i>ip-address</i> はドット区切りの 10 進数形式 (A.B.C.D) の 32 ビットの IP アドレスです。
ステップ 4	commit	

バンドルメンバのBFDセッションのイネーブル化

バンドルメンバーリンクでBFDセッションをイネーブルにするには、次の手順を実行します。

手順の概要

1. **configure**
2. **interface Bundle-Ether | Bundle-POS] *bundle-id***
3. **bfd address-family ipv4 fast-detect**
4. **commit**

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	interface Bundle-Ether Bundle-POS] <i>bundle-id</i> 例： RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	指定したバンドル ID のインターフェイス 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	bfd address-family ipv4 fast-detect 例： RP/0/RSP0/cpu 0: router(config-if)# bfd address-family ipv4 fast-detect	バンドルメンバーリンクでIPv4 BFDセッションをイネーブルにします。
ステップ 4	commit	

アクティブバンドルを維持するための最小しきい値の設定

バンドルマネージャは、メンバーリンクの状態に基づいて、バンドルが始動できるまたはアップのまま維持できる、またはダウンしているかどうかを判断するために2つの設定可能な最小しきい値を使用します。

- アクティブリンクの最小数
- 使用可能な最小アクティブ帯域幅

メンバの状態が変更されるたびに、バンドルマネージャは、アクティブメンバの数または使用可能な帯域幅が最小値より小さいかどうかを判断します。その場合は、バンドルがDOWN状態になるか、またはDOWN状態のままになります。アクティブリンクの数または使用可能な帯域幅がいずれかの最小しきい値に達すると、バンドルはUP状態に戻ります。

最小バンドルしきい値を設定するには、次の手順を実行します。

手順の概要

1. **configure**
2. **interface Bundle-Ether *bundle-id***
3. **bundle minimum-active bandwidth *kbps***
4. **bundle minimum-active links *links***
5. **commit**

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	interface Bundle-Ether <i>bundle-id</i> 例 : RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	指定したバンドル ID のインターフェイス 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	bundle minimum-active bandwidth <i>kbps</i> 例 : RP/0/RSP0/cpu 0: router(config-if)# bundle minimum-active bandwidth 580000	バンドルを始動またはアップのままにできるようにする前に必要な最小帯域幅を設定します。範囲は 1 から、プラットフォームやバンドルタイプによって異なる数値までです。
ステップ 4	bundle minimum-active links <i>links</i> 例 : RP/0/RSP0/cpu 0: router(config-if)# bundle minimum-active links 2	バンドルを始動またはアップのままにできるようにする前に必要なアクティブリンク数を設定します。指定できる範囲は 1 ~ 32 です。

	コマンドまたはアクション	目的
		(注) <ul style="list-style-type: none"> すでにアクティブであるバンドルでBFDが開始された場合、そのバンドルのBFD状態は、既存のすべてのアクティブメンバのBFD状態が既知であるときに宣言されます。
ステップ 5	commit	

バンドルのBFDパケット送信間隔と障害検出時間の設定

バンドルメンバーリンク上のBFDセッションのBFD非同期パケット間隔と障害検出時間は、バンドル上の **bfd address-family ipv4 minimum-interval** および **bfd address-family ipv4 multiplier** インターフェイス設定コマンドの組み合わせを使用して設定されます。

BFD制御パケット間隔は、**bfd address-family ipv4 minimum-interval** コマンドを使用して直接設定されます。BFDエコーパケット間隔およびすべての障害検出時間は、これらのコマンドの間隔および係数の値を組み合わせで決定されます。詳細については、[BFDパケット間隔と障害検出](#)を参照してください。

バンドルメンバリンクでBFD非同期モード制御およびエコーパケットの最小送信間隔と障害検出時間を設定するには、次の手順を実行します。

手順の詳細

手順の概要

1. **configure**
2. **interface Bundle-Ether | Bundle-POS] bundle-id**
3. **bfd address-family ipv4 minimum-interval milliseconds**
4. **bfd address-family ipv4 multiplier multiplier**
5. **commit**

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	interface Bundle-Ether Bundle-POS] bundle-id 例： RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	指定したバンドル ID のインターフェイス 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	bfd address-family ipv4 minimum-interval milliseconds 例：	

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config-if)#bfd address-family ipv4 minimum-interval 2000 (注) <ul style="list-style-type: none"> バンドル メンバー リンクで IPv4 BFD セッションの非同期モード制御パケットの最小間隔（ミリ秒単位）を指定します。範囲は 15 ～ 30000 です。このコマンドでは 15 ミリの最小値を設定できますが、Cisco ASR 9000 シリーズ ルーターでサポートされる最小値は 50 ミリ秒です。 	
ステップ 4	bfd address-family ipv4 multiplier multiplier 例 : RP/0/RSP0/cpu 0: router(config-if)#bfd address-family ipv4 multiplier 30	バンドル メンバ リンクの IPv4 BFD セッションの BFD 制御、エコー パケット障害検出時間およびエコーパケットの送信間隔を決定するために、最小間隔とともに係数として使用する値を指定します。範囲は 2 ～ 50 です。デフォルトは 3 です。 (注) <ul style="list-style-type: none"> このコマンドでは 2 の最小値を設定できますが、サポートされる最小値は 3 です。
ステップ 5	commit	

バンドルのタイマーを使用した BFD 状態変更通知の許容可能な遅延の設定

リンク バンドル メンバの BFD セッションのダウンを宣言する前に、ピアからの BFD SCN の受信の遅延を許可するために次の 2 つの設定可能なタイマーが BFD システムによってサポートされています。

- BFD セッションの開始
- ネイバーによる BFD 設定の削除

これらのタイマーの動作方法やその他の BFD 状態変更動作の詳細については、[メンバリンク](#) および [バンドル ステータスでの BFD 状態変更動作の概要](#) を参照してください。

ピアからの BFD SCN の受信の遅延を許可するタイマーを設定するには、次の手順を実行します。

手順の概要

1. **configure**
2. **interface Bundle-Ether | Bundle-POS] bundle-id**
3. **bfd address-family ipv4 timers start seconds**
4. **bfd address-family ipv4 timers nbr-unconfig seconds**

5. commit

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	interface Bundle-Ether Bundle-POS] bundle-id 例 : RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	指定したバンドル ID のインターフェイス 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	bfd address-family ipv4 timers start seconds 例 : RP/0/RSP0/cpu 0: router(config-if)#	セッションのアップを宣言できるように、BFD メンバリンク セッションの開始後、BFD ピアからの予測される通知が受信されるのを待つ秒数を指定します。その期間の後に SCN が受信されない場合は、BFD セッションのダウンが宣言されます。範囲は 60 ~ 3600 です。(Cisco IOS XR Release 4.0 および 4.0.1 では、使用可能な最小値は 30 ですが、これはお勧めできません)。
ステップ 4	bfd address-family ipv4 timers nbr-unconfig seconds 例 : RP/0/RSP0/cpu 0: router(config-if)#	BFD ピア間の設定の不一致を解決できるように、BFD 設定が BFD ネイバーによって削除されたことの通知の受信後に待機する秒数を指定します。指定されたタイマーに達する前に BFD 設定の問題が解決されない場合、BFD セッションのダウンが宣言されます。範囲は 30 ~ 3600 です。
ステップ 5	commit	

バンドル単位のバンドル CISCO/IETF モードを介した BFD のサポートの設定

バンドル CISCO/IETF モードを介した BFD のサポートをバンドル単位で設定するには、次の手順を実行します。

始める前に

BFD モードの変更 (Cisco から IETF およびその逆) は、バンドルが新たに作成されるか、またはバンドルの BFD 状態が「ダウン (down)」または「BoB 動作不能 (BoB nonoperational)」の場合にのみ実行されます。



(注) この手順は、リリース 5.3.1 以降に適用されます。

手順の概要

1. **configure**
2. **interface Bundle-Ether *bundle-id***
3. **no bfd address-family ipv4 fast-detect**
4. **commit**
5. **bfd mode { cisco | ietf }**
6. **bfd address-family ipv4 fast-detect**
7. **commit**
8. **show bundle bundle-ether *bundle-id***

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	interface Bundle-Ether <i>bundle-id</i> 例 : RP/0/RSP0/cpu 0: router(config)# interface Bundle-Ether 1	指定したバンドル ID のインターフェイス 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	no bfd address-family ipv4 fast-detect 例 : RP/0/RSP0/cpu 0: router(config-if)# no bfd address-family ipv4 fast-detect	指定したバンドルで IPv4 BFD セッションを無効にします。
ステップ 4	commit	
ステップ 5	bfd mode { cisco ietf } 例 : RP/0/RSP0/cpu 0: router(config-if)# bfd mode ietf	指定したバンドルのバンドルを介した BFD に Cisco モードまたは IETF モードを有効にします。デフォルトは cisco です。
ステップ 6	bfd address-family ipv4 fast-detect 例 : RP/0/RSP0/cpu 0: router(config-if)# bfd address-family ipv4 fast-detect	指定したバンドルで IPv4 BFD セッションを有効にします。
ステップ 7	commit	
ステップ 8	show bundle bundle-ether <i>bundle-id</i>	選択されたバンドル モードが表示されます。

モードを確認するための show コマンドの出力例

次に、バンドルモードが選択された **show bundle bundle-ether** コマンドの出力例を示します。

```
RP/0/RP0/CPU0:R3-PE3#sh bundle bundle-ether 4301

Bundle-Ether4301
  Status:                               Up
  Local links {active/standby/configured}: 2 / 0 / 2
  Local bandwidth {effective/available}:   20000000 (20000000) kbps
  MAC address (source):                   0014.1c00.0003 (Chassis pool)
  Inter-chassis link:                     No
  Minimum active links / bandwidth:       1 / 1 kbps
  Maximum active links:                   64
  Wait while timer:                       2000 ms
  Load balancing:                          Default
  LACP:                                    Operational
    Flap suppression timer:               Off
    Cisco extensions:                      Disabled
  mLACP:                                    Not configured
  IPv4 BFD:                                Operational
    State:                                 Up
  Mode:                                     ietf #####----- this is the
mode cisco/ietf .
  Fast detect:                             Enabled
  Start timer:                             60 s
  Neighbor-unconfigured timer:              60 s
  Preferred min interval:                   150 ms
  Preferred multiple:                       3
  Destination address:                      101.43.1.1

Port          Device          State          Port ID          B/W, kbps
-----
Te0/5/0/4    Local          Active         0x8000, 0x0012  10000000
  Link is Active
Te0/7/0/8    Local          Active         0x8000, 0x0006  10000000
  Link is Active
```

次のタスク

バンドルが新しい BFD モードの変更を受け入れるようにするには、既存の BFD セッションをダウンさせてから、再作成する必要があります。

BFD ピアへの転送パスをテストするためのエコモードの有効化

BFD エコモードは、次のインターフェイスではデフォルトで有効になっています。

- BFD バンドル インターフェイスのメンバリンク上の IPv4 の場合。
- 最小間隔が 2 秒未満である他の物理インターフェイス上の IPv4 の場合。



(注) **bfd minimum-interval** コマンドを使用して物理インターフェイスで2秒より長いBFD最小間隔を設定した場合、エコーモードをサポートして有効にするには、この間隔を2秒未満に変更する必要があります。これは、エコーモードを常にサポートするバンドルメンバリンクには適用されません。

デフォルトのエコー パケット送信元アドレスの上書き

エコーパケット送信元アドレスを指定しないと、BFD はエコーパケットのデフォルト送信元アドレスとして出力インターフェイスの IP アドレスを使用します。

3.9.0 よりも前の Cisco IOS XR リリースでは、エコーパケット送信元アドレスのデフォルト IP アドレスをルータ ID として指定されたアドレスに変更するために、**router-id** コマンドを使用してローカルルータ ID を設定することを推奨します。

Cisco IOS XR Release 3.9.0 以降では、BFD で **echo ipv4 source** コマンドを使用するか、インターフェイス BFD コンフィギュレーションモードを使用して、エコーパケット送信元アドレスとして使用する IP アドレスを指定できます。

ルータ全体で、または特定のインターフェイスについて、BFD のエコーパケットのデフォルト IP 送信元アドレスを上書きできます。

BFD に対するグローバルでのエコー パケット送信元アドレスの指定

ルータの BFD に対してグローバルにエコーパケット送信元 IP アドレスを指定するには、次の手順を実行します。

手順の概要

1. **configure**
2. **bfd**
3. **echo ipv4 source ip-address**
4. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)# bfd	BFD コンフィギュレーションモードを開始します。

個々のインターフェイスまたはバンドルのエコーパケット送信元アドレスの指定

	コマンドまたはアクション	目的
ステップ 3	echo ipv4 source ip-address 例： RP/0/RSP0/cpu 0: router(config-bfd)# echo ipv4 source 10.10.10.1	BFD エコーパケットで送信元アドレスとして使用される IPv4 アドレスを指定します。ここで、 <i>ip-address</i> はドット区切りの 10 進数形式 (A.B.C.D) の 32 ビットの IP アドレスです。
ステップ 4	commit	

個々のインターフェイスまたはバンドルのエコーパケット送信元アドレスの指定

個々の BFD インターフェイスまたはバンドルのエコーパケット送信元 IP アドレスを指定するには、次の手順を実行します。

手順の概要

1. **configure**
2. **bfd**
3. **interface type interface-path-id**
4. **echo ipv4 source ip-address**
5. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	interface type interface-path-id 例： RP/0/RSP0/cpu 0: router(config-bfd)# interface gigabitEthernet 0/1/5/0	特定のインターフェイスまたはバンドルに対して BFD 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。BFD インターフェイス コンフィギュレーションモードでは、個別のインターフェイスまたはバンドルで IPv4 アドレスを指定できます。
ステップ 4	echo ipv4 source ip-address 例： RP/0/RSP0/cpu 0: router(config-bfd)# echo ipv4 source 10.10.10.1	BFD エコーパケットで送信元アドレスとして使用される IPv4 アドレスを指定します。ここで、 <i>ip-address</i> はドット区切りの 10 進数形式 (A.B.C.D) の 32 ビットの IP アドレスです。
ステップ 5	commit	

エコー遅延検出に基づいた BFD セッションティアダウンの設定

Cisco IOS XR 4.0.1 以降では、設定されたエコー遅延許容値を超えた BFD セッションを停止するように非バンドルインターフェイスの BFD セッションを設定できます。

エコー遅延検出を使用して BFD セッションティアダウンを設定するには、次の手順を実行します。

エコー遅延検出を有効にする前に、BFD 設定でエコーモードがサポートされていることを確認してください。

エコー遅延検出はバンドル インターフェイスではサポートされません。

手順の詳細

手順の概要

1. **configure**
2. **bfd**
3. **echo latency detect [percentage percent-value [count packet-count]**
4. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	echo latency detect [percentage percent-value [count packet-count] 例： RP/0/RSP0/cpu 0: router(config-bfd)# echo latency detect	BFD セッション中のエコーパケットの遅延検出を有効にします。ここで、各値は次のとおりです。 <ul style="list-style-type: none"> • percentage percent-value : 不正遅延として検出するエコー障害検出時間のパーセンテージを指定します。範囲は 100 ~ 250 です。デフォルトは 100 です。 • count packet-count : BFD セッションをダウンさせる、不正遅延で受信される連続したパケットの数を指定します。指定できる範囲は 1 ~ 10 です。デフォルトは 1 です。
ステップ 4	commit	

エコーパスと遅延の検証までのBFDセッション開始の遅延

Cisco IOS XR Release 4.0.1以降、非バンドルインターフェイスのBFDセッションを開始する前に、エコーパケットパスが動作していて、設定された遅延しきい値内であることを確認できます。



(注) エコー起動検証は、バンドルインターフェイスではサポートされません。

BFDのエコー起動検証を設定するには、次の手順を実行します。

始める前に

エコー起動検証を有効にする前に、BFD設定でエコーモードがサポートされていることを確認してください。

手順の概要

1. **configure**
2. **bfd**
3. **echo startup validate [force]**
4. **commit**

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	bfd 例： RP/0/0RP0RSP0/CPU0:router(config)# bfd	BFD 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	echo startup validate [force] 例： RP/0/0RP0RSP0/CPU0:router(config-bfd)# echo startup validate	BFDセッションを開始する前に、エコーパケットパスの検証を有効にします。その場合、BFDセッションの状態変更を可能にする前に設定済みの遅延内に送信が成功するかどうかを確認するために、リンク上でエコーパケットが定期的に送信されます。 force キーワードが設定されていない場合、ローカルシステムは、次の条件が満たされた場合にエコー起動検証を実行します。 <ul style="list-style-type: none"> • ローカルルータは、エコーを実行できます（このセッションでは、エコーが有効になっています）。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> リモートルータは、エコーを実行できます（リモートシステムから受信された制御パケットには、ゼロ以外の「Required Min Echo RX Interval」値が含まれています）。 <p>force キーワードが設定されている場合、ローカルシステムは、次の条件を満たす場合にエコー起動検証を実行します。</p> <ul style="list-style-type: none"> ローカルルータは、エコーを実行できます（このセッションでは、エコーが有効になっています）。 リモートルータのエコー機能は考慮されません（リモートシステムから受信された制御パケットには、ゼロまたはゼロ以外の「Required Min Echo RX Interval」値が含まれています）。
ステップ 4	commit	

エコーモードの無効化

BFD は、特定の環境ではエコーモードでの非同期動作をサポートしません。BFD を次のアプリケーションまたは条件で使用する場合、エコーモードを無効にする必要があります。

- uRPF での BFD (IPv4)
- BFD バンドル インターフェイスに複数のラックにまたがるメンバリンクがある場合の、ラック リロードおよび活性挿抜 (OIR) をサポートするため。



(注) 最小間隔が 2 秒より長い場合、BFD エコーモードは、物理インターフェイスの BFD に対して自動的に無効になります。最小間隔は、BFD バンドル メンバリンクのエコーモードには影響を与えません。BFD エコーモードはまた、バンドル VLAN および IPv6 の BFD に対しても自動的に無効になります（グローバルおよびリンクローカルアドレッシング）。

ルータ全体で、または特定のインターフェイスについて、BFD のエコーモードを無効にすることができます。

ルータでのエコーモードの無効化

ルータでエコーモードをグローバルに無効にするには、次の手順を実行します。

個々のインターフェイスまたはバンドルでのエコーモードの無効化

手順の詳細

手順の概要

1. **configure**
2. **bfd**
3. **echo disable**
4. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	echo disable 例： RP/0/RSP0/cpu 0: router(config-bfd)# echo disable	ルータでエコーモードを無効にします。
ステップ 4	commit	

個々のインターフェイスまたはバンドルでのエコーモードの無効化

次に、インターフェイスまたはバンドルでエコーモードを無効にする手順について説明します。

手順の概要

1. **configure**
2. **bfd**
3. **interface type interface-path-id**
4. **echo disable**
5. **commit**

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	bfd 例：	BFD コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config)# bfd	
ステップ 3	interface type interface-path-id 例 : RP/0/RSP0/cpu 0: router(config-bfd)# interface gigabitEthernet 0/1/5/0	特定のインターフェイスまたはバンドルに対して BFD 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。BFD インターフェイスコンフィギュレーションモードでは、個別のインターフェイスまたはバンドルでエコーモードを無効にすることができます。
ステップ 4	echo disable 例 : RP/0/RSP0/cpu 0: router(config-bfd-if)# echo disable	指定された個別のインターフェイスまたはバンドルでエコーモードを無効にします。
ステップ 5	commit	

BFD ダンプニングを使用した BFD セッションフラッピングの最小化

BFD セッションフラッピングを制御するために BFD ダンプニングを設定するには、次の手順を実行します。

手順の概要

1. **configure**
2. **bfd**
3. **dampening [bundle-member] {initial-wait | maximum-wait | secondary-wait} milliseconds**
4. **commit**

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	bfd 例 : RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	dampening [bundle-member] {initial-wait maximum-wait secondary-wait} milliseconds 例 : RP/0/RSP0/cpu 0: router(config-bfd)# dampening initial-wait 30000	フラッピングを制御するための BFD セッション開始の遅延（ミリ秒単位）を指定します。 maximum-wait の値は、 initial-wait の値よりも大きい値にする必要があります。

	コマンドまたはアクション	目的
		ダンプニング値は、バンドル メンバ インターフェイスおよび非バンドル インターフェイスに対して定義できます。
ステップ 4	<code>commit</code>	

IPv6 チェックサムサポートの有効化および無効化

デフォルトでは、UDP パケットの IPv6 チェックサム計算はルータの BFD に対して有効になっています。

ルータ全体で、または特定のインターフェイスのどちらかの BFD の IPv6 チェックサムサポートを無効にすることができます。IPv6 チェックサムサポートが一方のルータでは有効になっているが、もう一方のルータでは無効になっている場合は、不良構成が発生する可能性があります。そのため、両方のルータで IPv6 チェックサムサポートを有効または無効にする必要があります。

ここでは、次のことについて説明します。



- (注) コマンドラインインターフェイス (CLI) は、BFD 設定と BFD インターフェイス コンフィギュレーションでは若干異なります。BFD 設定の場合、**disable** キーワードはオプションではありません。そのため、そのモードで BFD 設定を有効にするには、コマンドの **no** 形式を使用する必要があります。

ルータでの BFD の IPv6 チェックサム計算の有効化および無効化

ルータで IPv6 チェックサム計算をグローバルに有効または無効にするには、次の手順を実行します。

手順の概要

1. `configure`
2. `bfd`
3. `ipv6 checksum [disable]`
4. `commit`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure</code>	
ステップ 2	<code>bfd</code> 例 :	BFD コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config)# bfd	
ステップ 3	ipv6 checksum [disable] 例 : RP/0/RSP0/cpu 0: router(config-bfd-if)# ipv6 checksum disable	インターフェイスでの IPv6 チェックサムサポートを有効にします。無効にするには、 disable キーワードを使用します。
ステップ 4	commit	

個々のインターフェイスまたはバンドルの BFD の IPv6 チェックサム計算の有効化と無効化

次に、インターフェイスまたはバンドルで IPv6 チェックサム計算を有効または無効にする手順について説明します。

手順の詳細

手順の概要

1. **configure**
2. **bfd**
3. **interface type interface-path-id**
4. **ipv6 checksum [disable]**
5. **commit**

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	bfd 例 : RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	interface type interface-path-id 例 : RP/0/RSP0/cpu 0: router(config-bfd)# interface gigabitEthernet 0/1/5/0	特定のインターフェイスまたはバンドルに対して BFD 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。

	コマンドまたはアクション	目的
ステップ 4	ipv6 checksum [disable] 例： RP/0/RSP0/cpu 0: router(config-bfd-if)# ipv6 checksum	インターフェイスでのIPv6チェックサムサポートを有効にします。無効にするには、 disable キーワードを使用します。
ステップ 5	commit	

BFD カウンタのクリアおよび無効化

次に、BFD パケット カウンタの表示およびクリアの手順について説明します。特定ノードまたは特定インターフェイスでホストされている BFD セッションのパケット カウンタをクリアすることができます。

手順の概要

1. **show bfd counters [ipv4 | all] packet interface type interface-path-id location node-id**
2. **clear bfd counters [ipv4 | ipv6 | all] packet [interface type interface-path-id] location node-id**
3. **show bfd counters [[ipv4 | ipv6 | all] packet [interface type interface-path-id] location node-id**

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 bfd counters [ipv4 all] packet interface type interface-path-id location node-id 例： RP/0/RSP0/cpu 0: router#show bfd counters all packet location 0/3/cpu0	IPv4 パケット、IPv6 パケット、またはすべてのパケットの BFD カウンタを表示します。
ステップ 2	clear bfd counters [ipv4 ipv6 all] packet [interface type interface-path-id] location node-id 例： RP/0/RSP0/cpu 0: router# clear bfd counters all packet location 0/3/cpu0	IPv4 パケット、IPv6 パケット、またはすべてのパケットの BFD カウンタをクリアします。
ステップ 3	show bfd counters [[ipv4 ipv6 all] packet [interface type interface-path-id] location node-id 例： RP/0/RSP0/cpu 0: router# show bfd counters all packet location 0/3/cpu0	IPv4 パケット、IPv6 パケット、またはすべてのパケットの BFD カウンタがクリアされていることを確認します。

バンドル上の BFD (BoB) と論理バンドル上の BFD (BLB) の間の共存設定

BoB と BLB の間の共存メカニズムを設定するには、次のタスクを実行します。

始める前に

MP BFD セッションのホストを許可するには、1 つ以上のラインカードを設定する必要があります。ラインカードが搭載されていない場合、ラインカードグループは形成されず、その結果、BFD MP セッションは作成されません。グループサイズと番号のデフォルト設定では、2 行以上の **bfd multiple-paths include location node-id** コマンドと有効なラインカードを、グループの形成と BFD MP セッションの確立を開始するためのアルゴリズムの設定に追加する必要があります。

次に、設定例を示します。

```
(config)#bfd multipath include location 0/0/CPU0
(config)#bfd multipath include location 0/1/CPU0
```

手順の概要

1. **configure**
2. **bfd**
3. 次のいずれかのコマンドを使用します。
 - **bundle coexistence bob-blb inherit**
 - **bundle coexistence bob-blb logical**
4. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)#bfd	双方向フォワーディング検出 (BFD) を設定し、グローバル BFD 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	次のいずれかのコマンドを使用します。 <ul style="list-style-type: none"> • bundle coexistence bob-blb inherit • bundle coexistence bob-blb logical 例： RP/0/RSP0/cpu 0: router(config-bfd)#bundle coexistence bob-blb inherit または RP/0/RSP0/cpu 0: router(config-bfd)#bundle coexistence bob-blb logical	BoB と BLB の間の共存メカニズムを設定します。 <ul style="list-style-type: none"> • inherit : 「継承された」共存モードを設定するには、inherit キーワードを使用します。 • logical : 「論理的な」共存モードを設定するには、logical キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 4	commit	

BFD IPv6 マルチホップの設定

eBGP ネイバーの BFD IPv6 マルチホップの設定

eBGP ネイバーの BFD IPv6 マルチホップを設定するには、次のタスクを実行します。

手順の概要

1. **configure**
2. **bfd multipath include location *node-id***
3. **router bgp *as-number***
4. **neighbor *ip-address* ebgp-multihop *ttl-value***
5. **neighbor *ip-address* bfd fast-detect**
6. **commit**

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	bfd multipath include location <i>node-id</i> 例： RP/0/RSP0/cpu 0: router(config)#bfd multipath include location 0/7/CPU0	BFD マルチホップセッションをホストするための指定されたラインカードを含めます。
ステップ 3	router bgp <i>as-number</i> 例： RP/0/RSP0/cpu 0: router(config)# router bgp 65001	BGP コンフィギュレーションモードを開始します。
ステップ 4	neighbor <i>ip-address</i> ebgp-multihop <i>ttl-value</i> 例： RP/0/RSP0/cpu 0: router(config-bgp)#neighbor 21:1:1:1:1:1:2 ebgp-multihop 255	外部 BGP (eBGP) ネイバーとのマルチホップ ピアリングを有効にします。
ステップ 5	neighbor <i>ip-address</i> bfd fast-detect 例： RP/0/RSP0/cpu 0: router(config-bgp)#neighbor 21:1:1:1:1:1:2 bfd fast-detect	eBGP ネイバーの IP アドレスを指定し、BFD の迅速な検出を有効にします。
ステップ 6	commit	

iBGP ネイバーの BFD IPv6 マルチホップの設定

iBGP ネイバーの BFD IPv6 マルチホップを設定するには、次のタスクを実行します。

手順の概要

1. **configure**
2. **bfd multipath include location node-id**
3. **router bgp as-number**
4. **neighbor ip-address bfd fast-detect**
5. **commit**

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	bfd multipath include location node-id 例： RP/0/RSP0/cpu 0: router(config)#bfd multipath include location 0/7/CPU0	BFD マルチホップセッションをホストするための指定されたラインカードを含めます。
ステップ 3	router bgp as-number 例： RP/0/RSP0/cpu 0: router(config)#router bgp 65001	BGP コンフィギュレーションモードを開始します。
ステップ 4	neighbor ip-address bfd fast-detect 例： RP/0/RSP0/cpu 0: router(config-bgp)#neighbor 21:1:1:1:1:1:2	iBGP ネイバーの IP アドレスを指定し、BFD の迅速な検出を有効にします。
ステップ 5	commit	

MPLS トラフィック エンジニアリング LSP を介した BFD の設定

TE トンネルを介した BFD に対する BFD パラメータの有効化

TE トンネルの BFD は、トンネルで BFD パラメータを設定することにより、ヘッドエンドで有効になります。すでに起動しているトンネルで BFD が有効になっている場合、TE は、トンネルをダウンさせる前に、起動タイムアウトを待機します。デフォルトでは、TE トンネル上で BFD は無効になっています。BFD パラメータを設定し、TE トンネルを介した BFD を有効にするには、次のタスクを実行します。



- (注) BFD は、CPU 使用率の変動を避けるために LSP ping メッセージを 50 PPS 未満に制限することで、BFD セッションの作成ペースを調整します。

手順の概要

1. **configure**
2. **interface tunnel-te interface-number**
3. **bfd fast-detect**
4. **bfd minimum-interval milliseconds**
5. **bfd multiplier number**
6. **commit**

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	interface tunnel-te interface-number 例： RP/0/RSP0/cpu 0: router(config)#interface tunnel-te 65535	MPLS トラフィック エンジニアリング (MPLS TE) トンネルインターフェイスを設定し、MPLS TE トンネル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	bfd fast-detect 例： RP/0/RSP0/cpu 0: router(config-if)#bfd fast-detect	BFD 高速検出を有効にします。
ステップ 4	bfd minimum-interval milliseconds 例： RP/0/RSP0/cpu 0: router(config-if)#bfd minimum-interval 2000	hello 間隔をミリ秒単位で設定します。 hello 間隔の範囲は 100 ~ 30000 ミリ秒です。デフォルトの hello 間隔は 100 ミリ秒です。
ステップ 5	bfd multiplier number 例： RP/0/RSP0/cpu 0: router(config-if)#bfd multiplier 5	BFD 乗数検出を設定します。 BFD 乗数の範囲は 3 ~ 10 です。デフォルトの BFD 乗数は 3 です。
ステップ 6	commit	

次のタスク

BFD の起動タイムアウト間隔を設定します。

LSP がシグナリングされ、BFD セッションが作成されると、TE は BFD セッションが起動するまでの時間を指定できるようになります。BFD セッションがタイムアウト内に起動しない場合、LSP は切断されます。そのため、BFD 起動タイムアウトを設定する必要があります

BFD 起動タイムアウトの設定

BFD 起動タイムアウト間隔を設定するには、次の手順を実行します。デフォルトの起動タイムアウト間隔は 60 秒です。

始める前に

BFD は、MPLS TE トンネルインターフェイスで有効にする必要があります。

手順の概要

1. **configure**
2. **interface tunnel-te interface-number**
3. **bfd bringup-timeout seconds**
4. **commit**

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	interface tunnel-te interface-number 例： RP/0/RSP0/cpu 0: router(config)#interface tunnel-te 65535	MPLS トラフィック エンジニアリング (MPLS TE) トンネルインターフェイスを設定し、MPLS TE トンネル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	bfd bringup-timeout seconds 例： RP/0/RSP0/cpu 0: router(config-if)#bfd bringup-timeout 2400	BFD セッションが起動するのを待機する時間間隔 (秒単位) を有効にします。 起動タイムアウトの範囲は 6 ~ 3600 秒です。デフォルトの起動タイムアウト間隔は 60 秒です。
ステップ 4	commit	

次のタスク

BFD ダンプニングパラメータを設定して、TE トンネルを起動し、ネットワーク内のシグナリングの変化を回避します。

TE トンネルの BFD ダンプニングの設定

BFD セッションの起動に失敗すると、TE は失敗したパスオプションを使用してすぐにオフに戻り、ネットワーク内でのシグナリングの変化を回避します。

ダンプニング間隔を設定して TE トンネルを起動するには、次の手順を実行します。

始める前に

- BFD は、MPLS TE トンネルインターフェイスで有効にする必要があります。

- BFD 起動タイムアウト間隔は、**bfd bringup-timeout** コマンドを使用して設定する必要があります。

手順の概要

1. **configure**
2. **interface tunnel-te interface-number**
3. **bfd dampening initial-wait milliseconds**
4. **bfd dampening maximum-wait milliseconds**
5. **bfd dampening secondary-wait milliseconds**
6. **commit**

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	interface tunnel-te interface-number 例： RP/0/RSP0/cpu 0: router(config)#interface tunnel-te 65535	MPLS トラフィック エンジニアリング (MPLS TE) トンネルインターフェイスを設定し、MPLS TE トンネル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	bfd dampening initial-wait milliseconds 例： RP/0/RSP0/cpu 0: router(config-if)#bfd dampening initial-wait 360000	トンネルが起動するまでの初期遅延間隔を設定します。 初期起動待機遅延間隔の範囲は 1 ~ 518400000 ミリ秒です。デフォルトの初期待機間隔は 16000 ミリ秒です。 (注) このオプションを使用すると、以前にシグナリングされた帯域幅を持つ TE トンネルが起動します。
ステップ 4	bfd dampening maximum-wait milliseconds 例： RP/0/RSP0/cpu 0: router(config-if)#bfd dampening maximum-wait 700000	トンネルが起動するまでの最大遅延間隔を設定します。 最大起動待機遅延の時間間隔の範囲は 1 ~ 518400000 ミリ秒です。デフォルトの初期待機間隔は 600000 ミリ秒です。 (注) このオプションを使用すると、設定された帯域幅を持つ TE トンネルが起動します。
ステップ 5	bfd dampening secondary-wait milliseconds 例：	トンネルを起動するまでのセカンダリ遅延間隔を設定します。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config-if)#bfd dampening secondary-wait 30000	セカンダリ起動待機遅延時間間隔の範囲は 1 ~ 518400000 ミリ秒です。デフォルトのセカンダリ待機間隔は 20000 ミリ秒です。
ステップ 6	commit	

次のタスク

定期的な LSP ping オプションを設定します。

定期的な LSP ping 要求の設定

BFD セッションが起動した後、BFD TLV で定期的な LSP ping 要求を送信するように設定するには、次のタスクを実行します。

始める前に

BFD は、MPLS TE トンネルインターフェイスで有効にする必要があります。

手順の概要

1. **configure**
2. **interface tunnel-te interface-number**
3. 次のいずれかのコマンドを使用します。
 - **bfd lsp-ping interval 300**
4. **commit**

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	interface tunnel-te interface-number 例： RP/0/RSP0/cpu 0: router(config)#interface tunnel-te 65535	MPLS トラフィック エンジニアリング (MPLS TE) トンネルインターフェイスを設定し、MPLS TE トンネルインターフェイス 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	次のいずれかのコマンドを使用します。 • bfd lsp-ping interval 300 例： RP/0/RSP0/cpu 0: router(config-if)#bfd lsp-ping interval 300 または	LSP ping 要求の定期的な間隔を設定するか、または LSP ping 要求を無効にします。 • interval seconds : 定期的な LSP ping 要求の間隔を秒単位で設定します。間隔の範囲は 60 ~ 3600 秒です。デフォルトの間隔は 120 秒です。 • disable : 定期的な LSP ping 要求を無効にします。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: router(config-if)#bfd lsp-ping disable	定期的な LSP ping 要求は、デフォルトで有効になっています。ping 要求のデフォルトの間隔は 120 秒です。BFD は LSP ping を 1 秒あたり 50 ping (PPS) に調整します。そのため、ping 間隔は受け入れられません。ただし、60～3600 秒の間隔を設定しない限り、これは保証されません。
ステップ 4	commit	

次のタスク

テールエンドで BFD を設定します。

テールエンドでの BFD の設定

LSP セッションを介したすべての BFD に BFD 最小間隔と BFD 乗数パラメータを設定するには、テールエンド グローバルコンフィギュレーション コマンドを使用します。範囲とデフォルト値は、BFD ヘッドエンド設定値と同じです。BFD は、ヘッドエンドの最小間隔とテールエンドの最小間隔の間で設定された最大値を使用します。

テールエンドで BFD を設定するには、次のタスクを実行します。

手順の概要

1. **configure**
2. **mpls traffic-eng bfd lsp tailminimum-interval *milliseconds***
3. **mpls traffic-eng bfd lsp tailmultiplier *number***
4. **commit**

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	mpls traffic-eng bfd lsp tailminimum-interval <i>milliseconds</i> 例： RP/0/RSP0/cpu 0: router(config)#mpls traffic-eng bfd lsp tail minimum-interval 20000	hello 間隔をミリ秒単位で設定します。 hello 間隔の範囲は 100～30000 ミリ秒です。デフォルトの hello 間隔は 100 ミリ秒です。
ステップ 3	mpls traffic-eng bfd lsp tailmultiplier <i>number</i> 例： RP/0/RSP0/cpu 0: router(config)#mpls traffic-eng bfd lsp tail multiplier 5	BFD 乗数検出を設定します。 BFD 乗数検出の範囲は 3～10 です。デフォルトの BFD 乗数は 3 です。
ステップ 4	commit	

次のタスク

BFD マルチパスセッションをホストするように指定されたラインカードを含めるように **bfd multipath include location node-id** コマンドを設定します。

ラインカードでの LSP セッションを介した BFD の設定

フロントエンドとテールエンドの両方での LSP セッションを介した BFD は、次の設定が有効になっているラインカード上でホストされます。

手順の概要

1. **configure**
2. **bfd**
3. **multipath include location node-id**
4. **commit**

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	bfd 例： RP/0/RSP0/cpu 0: router(config)# bfd	BFD 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	multipath include location node-id 例： RP/0/RSP0/cpu 0: router(config-bfd)# multipath include location 0/1/CPU0	特定のラインカードに BFD マルチパスを設定します。 bfd multipath include を使用して、1 枚以上のラインカードを設定する必要があります。次に例を示します。 bfd multipath include location 0/1/CPU0 multipath include location 0/2/CPU0 ヘッドエンドとテールエンドの両方での LSP セッションを介した BFD は、ラインカード上でホストされます。ヘッドエンドとテールエンドの両方での LSP セッションを介した BFD は、内部選択メカニズムに従ってラインカード 0/1/CPU0 と 0/2/CPU0 に配信されます。
ステップ 4	commit	

BFD オブジェクト トラッキングの設定

手順の概要

1. **configure**
2. **track** *track-name*
3. **type bfdtrtr rate** *tx-rate*
4. **debouncedebounce**
5. **interface** *if-name*
6. **destaddress** *dest_addr*
7. **commit**

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	track <i>track-name</i> 例： RP/0/RSP0/cpu 0: router(config)# track track1	トラック コンフィギュレーション モードを開始します。 • <i>track-name</i> : トラッキングの対象となるオブジェクト名を指定します。
ステップ 3	type bfdtrtr rate <i>tx-rate</i> 例： RP/0/RSP0/cpu 0: router(config-track)# type bfdtrtr rate 4	<i>tx_rate</i> : BFD がリモート エンティティをプローブする時間 (ミリ秒)
ステップ 4	debouncedebounce 例： RP/0/RSP0/cpu 0: router(config-if)# debounce 10	<i>debounce</i> : BFD が OT に通知するまでにステータスが一致しなければならない連続する BFD プローブの数
ステップ 5	interface <i>if-name</i> 例： RP/0/RSP0/cpu 0: router(config-track-line-prot)# interface atm 0/2/0/0.1	<i>if_name</i> : BFD がリモート BFD のステータスをチェックするために使用する送信元のインターフェイス名。
ステップ 6	destaddress <i>dest_addr</i> 例： RP/0/RSP0/cpu 0: router(config-if)#destaddress 1.2.3.4	<i>dest_addr</i> : トラッキングされるリモート BFD エンティティの IPV4 アドレス。
ステップ 7	commit	

BFD を設定するための設定例

BGP を介した BFD : 例

次に、自律システム 65000 とネイバー 192.168.70.24 間での BFD を設定する例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router bgp 65000
RP/0/RSP0/cpu 0: router(config-bgp)#bfd multiplier 2
RP/0/RSP0/cpu 0: router(config-bgp)#bfd minimum-interval 20
RP/0/RSP0/cpu 0: router(config-bgp)#neighbor 192.168.70.24
RP/0/RSP0/cpu 0: router(config-bgp-nbr)#remote-as 2
RP/0/RSP0/cpu 0: router(config-bgp-nbr)#bfd fast-detect
RP/0/RSP0/cpu 0: router(config-bgp-nbr)#commit
RP/0/RSP0/cpu 0: router(config-bgp-nbr)#end
RP/0/RSP0/cpu 0: router#show run router bgp
```

OSPF を介した BFD : 例

次に、ギガビットイーサネットインターフェイスで OSPF での BFD を有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router ospf 0
RP/0/RSP0/cpu 0: router(config-ospf)#area 0
RP/0/RSP0/cpu 0: router(config-ospf-ar)#interface GigabitEthernet 0/3/0/1
RP/0/RSP0/cpu 0: router(config-ospf-ar-if)#bfd fast-detect
RP/0/RSP0/cpu 0: router(config-ospf-ar-if)#commit
RP/0/RSP0/cpu 0: router(config-ospf-ar-if)#end

RP/0/RSP0/cpu 0: router#show run router ospf

router ospf 0
area 0
interface GigabitEthernet0/3/0/1
bfd fast-detect
```

次に、ギガビットイーサネットインターフェイスで OSPFv3 での BFD を有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router ospfv3 0
RP/0/RSP0/cpu 0: router(config-ospfv3)#bfd minimum-interval 6500
RP/0/RSP0/cpu 0: router(config-ospfv3)#bfd multiplier 7
RP/0/RSP0/cpu 0: router(config-ospfv3-ar)#area 0
RP/0/RSP0/cpu 0: router(config-ospfv3-ar)#interface gigabitEthernet 0/1/5/0
RP/0/RSP0/cpu 0: router(config-ospfv3-ar-if)#bfd fast-detect
RP/0/RSP0/cpu 0: router(config-ospfv3-ar-if)#commit
RP/0/RSP0/cpu 0: router(config-ospfv3-ar-if)#end

RP/0/RSP0/cpu 0: router#show run router ospfv3
router ospfv3
```

```

area 0
interface GigabitEthernet0/1/5/0
bfd fast-detect

```

静的ルートを介した BFD : 例

次に、IPv4 静的ルートでの BFD を有効にする例を示します。この例では、BFD セッションは、ネクストホップ 10.3.3.3 が到達可能になると、このネクストホップで確立されます。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router static
RP/0/RSP0/cpu 0: router(config-static)#address-family ipv4 unicast
RP/0/RSP0/cpu 0: router(config-static)#10.2.2.0/24 10.3.3.3 bfd fast-detect
RP/0/RSP0/cpu 0: router(config-static)#end

```

次に、IPv6 静的ルートでの BFD を有効にする例を示します。この例では、BFD セッションは、ネクストホップ 2001:0DB8:D987:398:AE3:B39:333:783 が到達可能になると、このネクストホップで確立されます。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router static
RP/0/RSP0/cpu 0: router(config-static)#address-family ipv6 unicast
RP/0/RSP0/cpu 0: router(config-static)#2001:0DB8:C18:2:1::F/64
2001:0DB8:D987:398:AE3:B39:333:783 bfd fast-detect minimum-interval 150 multiplier 4
RP/0/RSP0/cpu 0: router(config-static)#end

RP/0/RSP0/cpu 0: router#show run router static address-family ipv6 unicast

```

バンドル VLAN での BFD : 例

次に、バンドル VLAN で BFD を設定する例を示します。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#multipath include location 0/0/CPU0
RP/0/RSP0/cpu 0: router(config-bfd)#exit

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#interface Bundle-ether 1
RP/0/RSP0/cpu 0: router(config-if)#bundle maximum-active links 1
RP/0/RSP0/cpu 0: router(config-if)#exit
!
RP/0/RSP0/cpu 0: router(config)#interface TenGigE 0/1/0/1
RP/0/RSP0/cpu 0: router(config-if)#bundle id 1 mode active
RP/0/RSP0/cpu 0: router(config-if)#exit
!
RP/0/RSP0/cpu 0: router(config)#interface TenGigE 0/2/0/1
RP/0/RSP0/cpu 0: router(config-if)#bundle id 1 mode active
RP/0/RSP0/cpu 0: router(config-if)#exit
!
RP/0/RSP0/cpu 0: router(config)#interface Bundle-Ether1.2
RP/0/RSP0/cpu 0: router(config-if)#ipv4 address 172.16.2.1 255.255.255.0
RP/0/RSP0/cpu 0: router(config-if)#encapsulation dot1q 2

```

```

RP/0/RSP0/cpu 0: router(config-if)#exit
!
RP/0/RSP0/cpu 0: router(config)#interface Bundle-Ether1.1
RP/0/RSP0/cpu 0: router(config-if)#ipv4 address 172.16.1.1 255.255.255.0
RP/0/RSP0/cpu 0: router(config-if)#encapsulation dot1q 1
!
RP/0/RSP0/cpu 0: router(config)#router static
RP/0/RSP0/cpu 0: router(config-static)#address-family ipv4 unicast
RP/0/RSP0/cpu 0: router(config-static-afi)#10.2.1.0/24 172.16.1.2 bfd fast-detect
minimum-interval 250
RP/0/RSP0/cpu 0: router(config-static-afi)#10.2.2.0/24 172.16.2.2 bfd fast-detect
minimum-interval 250
RP/0/RSP0/cpu 0: router(config-static-afi)#10.2.3.0/24 172.16.3.2 bfd fast-detect
minimum-interval 250
RP/0/RSP0/cpu 0: router(config-static-afi)#exit
RP/0/RSP0/cpu 0: router(config-static)#exit
!

```

ブリッジグループ仮想インターフェイスを介した BFD : 例

次に、ピアノードと uut ノードの設定の例を示します。BVI インターフェイスがデフォルトテーブルではなく VRF にあることがわかります。

```

interface BVI100
vrf cctv1 <<<<<<<<<

```

次に、ピアノードの例を示します。

```

l2vpn
bridge group bg
  bridge-domain bd
  interface Bundle-Ether1.100
  !
  routed interface BVI100
  !
  !
  !
router vrrp
interface BVI100
  bfd minimum-interval 15
  address-family ipv4
  vrrp 100
  address 192.168.1.254
  bfd fast-detect peer ipv4 192.168.1.2
  !
  !
  !
router ospf 100
vrf cctv1
  router-id 192.168.1.1
  area 0
  interface BVI100
  !
  !
  !
interface BVI100

```

```

vrf cctv1
ipv4 address 192.168.1.1 255.255.255.0
!
interface GigE0/1/0/10
bundle id 1 mode active
no shut
!
interface Bundle-Ether1
no shut
!
interface Bundle-Ether1.100 l2transport
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric

!
bfd multipath include loc 0/1/cpu0

interface MgmtEth0/RSP1/CPU0/0
ipv4 address 7.37.19.20 255.255.0.0
no shutdown
!
router static
address-family ipv4 unicast
0.0.0.0/0 7.37.0.1

```

次に、uut ノードの例を示します。

```

l2vpn
bridge group bg
bridge-domain bd
interface Bundle-Ether1.100
!
routed interface BVI100
!
!
!
router vrrp
interface BVI100
bfd minimum-interval 15
address-family ipv4
vrrp 100
address 192.168.1.254
bfd fast-detect peer ipv4 192.168.1.1
!
!
!
router ospf 100
vrf cctv1
router-id 192.168.1.2
area 0
interface BVI100
!
!
!
interface BVI100
vrf cctv1
ipv4 address 192.168.1.2 255.255.255.0
!

```



```
interface GigE0/1/0/0
  bundle id 1 mode active
  no shut
  !
  interface Bundle-Ether1
  no shut
  !
  interface Bundle-Ether1.100 l2transport
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  !
bfd multipath include location 0/1/CPU0
```

バンドルメンバリンクでの BFD : 例

次に、イーサネットバンドルインターフェイスのメンバリンクで BFD を設定する例を示します。

```
bfd
  interface Bundle-Ether4
  echo disable
  !
  interface GigabitEthernet0/0/0/2.3
  echo disable
  !
  !
  interface GigabitEthernet0/0/0/3 bundle id 1 mode active
  interface GigabitEthernet0/0/0/4 bundle id 2 mode active
  interface GigabitEthernet0/1/0/2 bundle id 3 mode active
  interface GigabitEthernet0/1/0/3 bundle id 4 mode active
  interface Bundle-Ether1
  ipv4 address 192.168.1.1/30
  bundle minimum-active links 1
  !
  interface Bundle-Ether1.1
  ipv4 address 192.168.100.1/30
  encapsulation dot1q 1001
  !
  interface Bundle-Ether2
  bfd address-family ipv4 destination 192.168.2.2
  bfd address-family ipv4 fast-detect
  bfd address-family ipv4 min 83
  bfd address-family ipv4 mul 3
  ipv4 address 192.168.2.1/30
  bundle minimum-active links 1
  !
  interface Bundle-Ether3
  bfd address-family ipv4 destination 192.168.3.2
  bfd address-family ipv4 fast-detect
  bfd address-family ipv4 min 83
  bfd address-family ipv4 mul 3
  ipv4 address 192.168.3.1/30
  bundle minimum-active links 1
  !
  interface Bundle-Ether4
  bfd address-family ipv4 destination 192.168.4.2
  bfd address-family ipv4 fast-detect
  bfd address-family ipv4 min 83
  bfd address-family ipv4 mul 3
```

```

ipv4 address 192.168.4.1/30
bundle minimum-active links 1
!
interface GigabitEthernet 0/0/0/2
  ipv4 address 192.168.10.1/30
!
interface GigabitEthernet 0/0/0/2.1
  ipv4 address 192.168.11.1/30
  ipv6 address beef:cafe::1/64
  encapsulation dot1q 2001
!
interface GigabitEthernet 0/0/0/2.2
  ipv4 address 192.168.12.1/30
  encapsulation dot1q 2002
!
interface GigabitEthernet 0/0/0/2.3
  ipv4 address 192.168.13.1/30
  encapsulation dot1q 2003
!
router static
  address-family ipv4 unicast
    10.10.11.2/32 192.168.11.2 bfd fast-detect minimum-interval 250 multiplier 3
    10.10.12.2/32 192.168.12.2 bfd fast-detect minimum-interval 250 multiplier 3
    10.10.13.2/32 192.168.13.2 bfd fast-detect minimum-interval 250 multiplier 3
    10.10.100.2/32 192.168.100.2 bfd fast-detect minimum-interval 250 multiplier 3
!
  address-family ipv6 unicast
    babe:cace::2/128 beef:cafe::2 bfd fast-detect minimum-interval 250 multiplier 3
!

```

エコーパケット送信元アドレス：例

次に、ルータ上のすべてのBFDセッションのBFDエコーパケットの送信元アドレスとしてIPアドレス10.10.10.1を指定する例を示します。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo ipv4 source 10.10.10.1

```

次に、個々のギガビットイーサネットインターフェイス上のBFDエコーパケットの送信元アドレスとしてIPアドレス10.10.10.1を指定する例を示します。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#interface gigabitethernet 0/1/0/0
RP/0/RSP0/cpu 0: router(config-bfd-if)#echo ipv4 source 10.10.10.1

```

次に、個々のPacket-over-SONET (POS) インターフェイスのBFDエコーパケットの送信元アドレスとして、IPアドレス10.10.10.1を指定する例を示します。

```

RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#interface pos 0/1/0/0
RP/0/RSP0/cpu 0: router(config-bfd-if)#echo ipv4 source 10.10.10.1

```

エコー遅延検出 : 例

次の例では、BFD 最小間隔は 50 ms、また BFD セッションの係数は 3 とします。

次に、1 のパケットカウントに対するエコー障害期間 (I x M) の 100% のデフォルト値を使用してエコー遅延検出を有効にする例を示します。この例では、ラウンドトリップ遅延が 150 ms を超える 1 つのエコー パケットが検出されると、セッションはダウンします。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo latency detect
```

次に、1 のパケットカウントに対するエコー障害期間の 200% (2 倍) に基づいてエコー遅延検出を有効にする例を示します。この例では、ラウンドトリップ遅延が 300 ms を超える 1 つのパケットを検出すると、セッションはダウンします。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo latency detect percentage 200
```

次に、3 のパケットカウントに対するエコー障害期間の 100% に基づいてエコー遅延検出を有効にする例を示します。この例では、ラウンドトリップ遅延が 150 ms を超える 3 つの連続したエコー パケットが検出されると、セッションはダウンします。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo latency detect percentage 100 count 3
```

エコー起動検証 : 例

次に、最後に受信された制御パケットにゼロ以外の「Required Min Echo RX Interval」値が含まれている場合に、非バンドル インターフェイスの BFD セッションのエコー起動検証を有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo startup validate
```

次に、最後の制御パケット内の「Required Min Echo RX Interval」値には関係なく、非バンドル インターフェイスの BFD セッションのエコー起動検証を有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo startup validate force
```

BFD エコーモードの無効化：例

次に、ルータでエコーモードを無効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#echo disable
```

次に、インターフェイスでエコーモード無効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#interface gigabitethernet 0/1/0/0
RP/0/RSP0/cpu 0: router(config-bfd-if)#echo disable
```

BFD ダンプニング：例

次に、BFD バンドルメンバの BFD セッション開始の初期および最大遅延を設定する例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#dampening bundle-member initial-wait 8000
RP/0/RSP0/cpu 0: router(config-bfd)#dampening bundle-member maximum-wait 15000
```

次に、非バンドルインターフェイスの BFD に対するデフォルトの initial-wait を変更する例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#dampening initial-wait 30000
RP/0/RSP0/cpu 0: router(config-bfd)#dampening maximum-wait 35000
```

BFD IPv6 チェックサム：例

次に、ルータのすべての BFD セッションの UDP パケットの IPv6 チェックサム計算を無効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#ipv6 checksum disable
```

次に、ルータのすべての BFD セッションの UDP パケットの IPv6 チェックサム計算を再び有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#no ipv6 checksum disable
```

次に、個々のインターフェイスの BFD セッションのエコーモードを有効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#interface gigabitethernet 0/1/0/0
RP/0/RSP0/cpu 0: router(config-bfd-if)#ipv6 checksum
```

次に、個々のインターフェイスの BFD セッションのエコーモードを無効にする例を示します。

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#bfd
RP/0/RSP0/cpu 0: router(config-bfd)#interface gigabitethernet 0/1/0/0
RP/0/RSP0/cpu 0: router(config-bfd-if)#ipv6 checksum disable
```

Cisco IOS および Cisco IOS XR ソフトウェアを実行しているルータの BFD ピア : 例

次に、Cisco IOS ソフトウェアを実行しているルータ 1 のルータインターフェイスで BFD を設定し、**bfd neighbor** コマンドを使用してインターフェイスの IP アドレス 192.0.2.1 をルータ 2 の BFD ピアとして指定する例を示します。ルータ 2 は、Cisco IOS XR ソフトウェアを実行していて、**router static** コマンドと **address-family ipv4 unicast** コマンドを使用して、IP アドレス 192.0.2.2 でルータ 1 のインターフェイスに戻るパスを指定します。

ルータ 1 (Cisco IOS ソフトウェア)

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#interface GigabitEthernet8/1/0
RP/0/RSP0/cpu 0: router(config-if)#description to-TestBed1 G0/0/0/0
RP/0/RSP0/cpu 0: router(config-if)#ip address 192.0.2.2 255.255.255.0
RP/0/RSP0/cpu 0: router(config-if)#bfd interval 100 min_rx 100 multiplier 3
RP/0/RSP0/cpu 0: router(config-if)#bfd neighbor 192.0.2.1
```

ルータ 2 (Cisco IOS XR ソフトウェア)

```
RP/0/RSP0/cpu 0: router#configure
RP/0/RSP0/cpu 0: router(config)#router static
RP/0/RSP0/cpu 0: router(config-static)#address-family ipv4 unicast
RP/0/RSP0/cpu 0: router(config-static-afi)#10.10.10.10/32 192.0.2.2 bfd fast-detect
RP/0/RSP0/cpu 0: router(config-static-afi)#exit
RP/0/RSP0/cpu 0: router(config-static)#exit
RP/0/RSP0/cpu 0: router(config)#interface GigabitEthernet0/0/0/0
RP/0/RSP0/cpu 0: router(config-if)#ipv4 address 192.0.2.1 255.255.255.0
```

BFD IPv6 マルチホップの設定 : 例

eBGP ネイバーの BFD IPv6 マルチホップの設定 : 例

次に、eBGP ネイバーの BFD IPv6 マルチホップを設定する例を示します。

```

bfd
 multipath include location 0//CPU0
!
router bgp 65001
 neighbor 21:1:1:1:1:1:2
  bfd fast-detect
  ebgp-multihop 255

```

iBGP ネイバーの BFD IPv6 マルチホップの設定 : 例

次に、iBGP ネイバーの BFD IPv6 マルチホップを設定する例を示します。

```

bfd
 multipath include location 0/7/CPU0
!
router bgp 65001
 neighbor 21:1:1:1:1:1:2
  bfd fast-detect

```

MPLS TE LSP を介した BFD : 例

次に、MPLS TE LSP を介した BFD の設定方法の例を示します。

MPLS TE トンネルヘッドエンド設定を介した BFD : 例

次に、ヘッドエンドで MPLS TE トンネルを介した BFD を設定する例を示します。

```

bfd multipath include loc 0/1/CPU0
mpls oam
interface tunnel-te 1 bfd fast-detect
interface tunnel-te 1
  bfd minimum-interval
  bfd multiplier
  bfd bringup-timeout
  bfd lsp-ping interval 60
  bfd lsp-ping disable
  bfd dampening initial-wait (default 16000 ms)
  bfd dampening maximum-wait (default 600000 ms)
  bfd dampening secondary-wait (default 20000 ms)
logging events bfd-status

```

MPLS TE トンネルテールエンド設定を介した BFD : 例

次に、テールエンドで MPLS TE トンネルを介した BFD を設定する例を示します。

```

bfd multipath include loc 0/1/CPU0
mpls oam
mpls traffic-eng bfd lsp tail multiplier 3
mpls traffic-eng bfd lsp tail minimum-interval 100

```

次の作業

BFDは、複数のプラットフォームでサポートされます。これらのコマンドの詳細については、プラットフォームに対応する『Cisco IOS XR Routing Command Reference』および『Cisco IOS XR MPLS Command Reference』の関連の章を参照してください。

http://www.cisco.com/en/US/products/ps5845/prod_command_reference_list.html

- 『BGP Commands on Cisco IOS XR Software』
- 『IS-IS Commands on Cisco IOS XR Software』
- 『OSPF Commands on Cisco IOS XR Software』
- 『Static Routing Commands on Cisco IOS XR Software』
- 『MPLS Traffic Engineering Commands on Cisco IOS XR Software』

その他の参考資料

ここでは、Cisco IOS XR ソフトウェアの BFD 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
BFD コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、例	<i>Routing Command Reference for Cisco ASR 9000 Series Routers</i>
QoS パケット分類の設定	<i>Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers</i>

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

RFC

RFC	タイトル
rfc5880_bfd_base	『 <i>Bidirectional Forwarding Detection</i> 』、2010年6月
rfc5881_bfd_ipv4_ipv6	『 <i>BFD for IPv4 and IPv6 (Single Hop)</i> 』、2010年6月
rfc5883_bfd_multihop	『 <i>BFD for Multihop Paths</i> 』、2010年6月

MIB

MIB	MIB のリンク
—	<p>Cisco IOS XR ソフトウェアを使用して MIB の場所を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューからプラットフォームを選択します。</p> <p>https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index</p>

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