IP ルーティング：BFD コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

双方向フォワーディング検出 3

機能情報の確認 3

双方向フォワーディング検出の前提条件 4

双方向フォワーディング検出の制約事項 5

双方向フォワーディング検出について 9

BFD の動作 9

ネイバー関係 9

BFD の障害検出 10

BFD バージョンの相互運用性 11

Cisco 12000 ルータでの BFD サポート 11

RP の BFD プロセス 11

LC の BFD プロセス 12

BFD セッションの制限 12

非ブロードキャスト メディア インターフェイスに対する BFD サポート 12

VPN ルーティングおよび転送インターフェイスに対する BFD サポート 12

ステートフル スイッチオーバーでのノンストップ フォワーディングの BFD サポート 12

ステートフル スイッチオーバーの BFD サポート 13

スタンバイ RP のステートフル BFD 13

スタティック ルーティングの BFD サポート 14

ATM 疑似回線の BFD Control Channel over VCCV のサポート 15

マルチホップでの BFD 16

障害検出に BFD を使用することの利点 16

DMVPN での BFD サポートの利点 17

双方向フォワーディング検出の設定方法 17

インターフェイスでの BFD セッション パラメータの設定 17

ダイナミック ルーティング プロトコルに対する BFD サポートの設定 19
BGP に対する BFD サポートの設定 20
次の作業 21
EIGRP に対する BFD サポートの設定 22
次の作業 24
IS-IS に対する BFD サポートの設定 24
前提条件 25
すべてのインターフェイスの IS-IS に対する BFD サポートの設定 25
次の作業 27
1 つ以上のインターフェイスの IS-IS に対する BFD サポートの設定 27
次の作業 29
OSPF に対する BFD サポートの設定 30
すべてのインターフェイスの OSPF に対する BFD サポートの設定 30
次の作業 33
1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定 33
次の作業 35
HSRP に対する BFD サポートの設定 35
次の作業 37
スタティック ルーティングに対する BFD サポートの設定 37
BFD エコー モードの設定 40
前提条件 41
機能制限 41
BFD 低速タイマーの設定 41
非対称性のない BFD エコー モードのディセーブル化 42
BFD テンプレートの作成と設定 43
シングルホップ テンプレートの設定 43
マルチホップ テンプレートの設定 45
次の作業 46
BFD マップの設定 46
ATM 疑似回線の BFD Control Channel over VCCV サポートの設定 47
DMVPN での BFD サポートの設定 50
BFD のモニタリングとトラブルシューティング 51

Cisco 7600 シリーズ ルータの BFD のモニタリングとトラブルシューティング 51
Cisco 10720 インターネット ルータの BFD のモニタリングとトラブルシューティング 52
Cisco 12000 シリーズ ルータの BFD のモニタリングとトラブルシューティング 53
双方向フォワーディング検出の設定例 55
例：エコーモードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定 55
例：OSPF ネットワークでの BFD の設定 60
例：BGP ネットワークでの BFD の設定 64
例：IS-IS ネットワークでの BFD の設定 66
例：HSRP ネットワークでの BFD の設定 67
例：スタティック ルーティングに対する BFD サポートの設定 69
例：BFD Control Channel over VCCV：ATM 疑似回線サポートの設定 70
例：DMVPN での BFD サポート 71
その他の参考資料 75
双方向フォワーディング検出に関する機能情報 77
IPv6 での BFD に対するスタティック ルート サポート 87
機能情報の確認 87
IPv6 での BFD に対するスタティック ルート サポートに関する情報 87
BFDv6 associated モード 88
BFDv6 unassociated モード 88
IPv6 の双方向フォワーディング検出の設定方法 89
スタティック BFDv6 ネイバーの指定 89
BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け 90
IPv6 での BFD に対するスタティック ルート サポートの設定例 91
例：IPv6 スタティック BFDv6 ネイバーの指定 91
例：BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け 91
その他の参考資料 91
IPv6 での BFD に対するスタティック ルート サポートに関する機能情報 92
OSPFv3 for BFD 95
機能情報の確認 95

OSPFv3 for BFD に関する情報 95
OSPFv3 for BFD の設定方法 96
OSPFv3 に対する BFD サポートの設定 96
インターフェイスの基本 BFD セッション パラメータの設定 96
すべてのインターフェイスの OSPFv3 に対する BFD サポートの設定 97
1 つ以上の OSPFv3 インターフェイスの OSPFv3 に対する BFDv6 サポートの設定 99
モニタリングおよびトラブルシューティングのための BFDv6 情報の取得 101
OSPFv3 for BFD の設定例 102
例：BFD に関する OSPF インターフェイス情報の表示 102
その他の参考資料 102
OSPFv3 for BFD に関する機能情報 104
BDI インターフェイスでの BFD 105
機能情報の確認 105
ブリッジ ドメイン インターフェイスの BFD に関する情報 106
ブリッジ ドメイン インターフェイスの BFD 106
BDI インターフェイスの BFD の設定方法 106
ブリッジ ドメイン インターフェイス上での BFD のイネーブル化 106
ブリッジ ドメインとイーサネット フロー ポイントの関連付け 107
BDI インターフェイスの BFD の設定例 110
BDI インターフェイスの BFD の例 110
その他の参考資料 111
ブリッジ ドメイン インターフェイスの BFD に関する機能情報 113
BFD シングルホップ認証 115
機能情報の確認 115
BFD シングルホップ認証の前提条件 116
BFD シングルホップ認証の制限事項 116
BFD シングルホップ認証に関する情報 116
BFD シングルホップ認証の利点 116
サービス妨害（DoS）攻撃を防ぐ際の BFD シングルホップ認証の役割 117
BFD シングルホップ認証の設定方法 117
キー チェーンの設定 117

認証を使用した BFD テンプレートの設定 118
インターフェイスでのシングルホップ テンプレートの設定 120
BFD シングルホップ認証の確認 121
BFD シングルホップ認証の設定例 121
例：キー チェーンの設定 121
例：認証を使用した BFD テンプレートの設定 121
例：インターフェイスでのシングルホップ テンプレートの設定 122
例：BFD シングルホップ認証の確認 122
その他の参考資料 123
BFD シングルホップ認証に関する機能情報 123
IPv4 スタティック ルートの BFD マルチホップ サポート 125
機能情報の確認 125
IPv4 スタティック ルートの BFD マルチホップ サポートの前提条件 126
IPv4 スタティック ルートの BFD マルチホップ サポートに関する情報 126
BFDv4 associated モード 126
BFDv4 unassociated モード 126
IPv4 スタティック ルートの BFD マルチホップ サポートの設定方法 127
BFD マルチホップ IPv4 スタティック ルートの設定 127
IPv4 スタティック ルートの BFD マルチホップ サポートの確認 128
IPv4 スタティック ルートの BFD マルチホップ サポートの設定例 129
例：associated モードでの IPv4 スタティック ルートの BFD マルチホップの設定 129
例：unassociated モードでの BFD の IPv4 スタティック マルチホップの設定 129
IPv4 スタティック ルートの BFD マルチホップ サポートに関する追加情報 130
IPv4 スタティック ルートの BFD マルチホップ サポートに関する機能情報 131
BFD の IS-IS IPv6 クライアント 133
機能情報の確認 133
BFD の IS-IS IPv6 クライアントの前提条件 133
BFD の IS-IS IPv6 クライアントに関する情報 134
IS-IS BFD トポロジ 134
IS-IS BFD IPv6 セッションの作成 134
IS-IS BFD IPv6 セッションの削除 134
BFD の ISIS IPv6 クライアントの設定方法 135

インターフェイスでの BFD の IS-IS IPv6 クライアント サポートの設定 135
すべてのインターフェイスでの BFD の IS-IS IPv6 クライアント サポートの設定 136
BFD の ISIS IPv6 クライアントの設定例 138
例：単一インターフェイスでの BFD の IS-IS IPv6 クライアント サポート 138
例：すべてのインターフェイスでの BFD の IS-IS IPv6 クライアント サポート 138
その他の参考資料 138
BFD の IS-IS IPv6 クライアントに関する機能情報 139
BFD C ビットの IS-IS クライアント サポート 141
機能情報の確認 141
BFD C ビットの IS-IS クライアント サポートの前提条件 142
BFD C ビットの IS-IS クライアント サポートに関する情報 142
IS-IS の再起動と BFD セッション 142
BFD C ビットの IS-IS クライアント サポートの設定方法 143
BFD C ビットの IS-IS クライアント サポートの設定 143
BFD C ビットの IS-IS クライアント サポートの設定例 144
例：BFD C ビットの IS-IS クライアント サポートの設定 144
その他の参考資料 144
BFD C ビットの IS-IS クライアント サポートに関する機能情報 145
BFD ダンプニング 147
機能情報の確認 147
BFD ダンプニングに関する情報 148
BFD ダンプニングの概要 148
BFD ダンプニングの設定方法 149
BFD ダンプニングの設定 149
BFD ダンプニングの設定例 150
例：BFD ダンプニングの設定 150
BFD ダンプニングに関する追加情報 151
BFD ダンプニングに関する機能情報 151

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

双方向フォワーディング検出

このマニュアルでは、双方向フォワーディング検出（BFD）プロトコルをイネーブルにする方法について説明します。BFDはあらゆるメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。これにはマルチ ホップ BFD セッションの設定方法の説明が含まれます。

BFDは高速転送パス障害検出に加えて、ネットワーク管理者向けの整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、さまざまなルーティング プロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

- 機能情報の確認，3 ページ
- 双方向フォワーディング検出の前提条件，4 ページ
- 双方向フォワーディング検出の制約事項，5 ページ
- 双方向フォワーディング検出について，9 ページ
- 双方向フォワーディング検出の設定方法，17 ページ
- 双方向フォワーディング検出の設定例，55 ページ
- その他の参考資料，75 ページ
- 双方向フォワーディング検出に関する機能情報，77 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

双方向フォワーディング検出の前提条件

- シスコ エクスプレス フォワーディングおよび IP ルーティングが、関連するすべてのルータでイネーブルになっていること。
- BFD が正常に動作するには、Cisco 10720 インターネット ルータで Cisco Parallel eXpress Forwarding（PXF）をイネーブルにしてあること。PXF はデフォルトでイネーブルになり、オフにすることは通常ありません。
- BFD を導入する前に、BFD でサポートされる IP ルーティング プロトコルのいずれかをルータで設定しておくこと。使用しているルーティング プロトコルの高速コンバージェンスを実装する必要があります。高速コンバージェンスの設定については、お使いのバージョンの Cisco IOS ソフトウェアの IP ルーティングのマニュアルを参照してください。Cisco IOS ソフトウェアの BFD ルーティング プロトコルのサポートの詳細については、「双方向フォワーディング検出の制約事項」の項を参照してください。
- 疑似回線で Virtual Circuit Connection Verification（VCCV）BFD を実行する前に、疑似回線がネットワーク上に設定されている必要があります。
- Cisco IOS Release 15.1(2)S 以降のリリースでは、Cisco 7600 シリーズ ルータで ES+ ライン カードに BFD セッションをオフロードするためのサポートの前提条件は次のとおりです。
  - ルータが BFD バージョン 1 を実行していること。
  - BFD セッション タイプは IPv4 シングルホップであること。
  - BFD エコー モードがセッションに対して無効であること。

  ハードウェア オフロードの前提条件の詳細については、『*Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*』の「Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card」の項を参照してください。
- Cisco IOS Release 15.1(3)S 以降のリリースでは、Cisco 7600 シリーズ ルータでマルチホップ BFD セッションのサポートの前提条件は次のとおりです。
  - クライアントがマルチホップをサポートしていること。
  - 有効なマルチホップ テンプレートおよびマップが設定されていること。
  - 各 BFD マルチホップ セッションに送信元アドレスと宛先アドレスの一意のペアが指定されていること。

双方向フォワーディング検出の制約事項

- CSCts32440 の場合、サポートされる VRF 対応 IS-IS BFD セッションの最大数は 28 です。
- Cisco IOS Release 12.2(18)SXE、12.0(31)S、12.4(4)T、12.0(32)S、12.2(33)SRA、および 12.2(33)SRB 用のシスコの BFD 実装では、非同期モードだけがサポートされます。非同期モードでは、どちらの BFD ピアも BFD セッションを開始できます。
- Cisco IOS Release 12.2(33)SRC、12.2(33)SXH、および 12.2(33)SXI では、デフォルトがエコーモードです。
- Cisco IOS ソフトウェアでは、仮想テンプレートおよびダイヤラ インターフェイスで BFD を誤って設定する可能性がありますが、仮想テンプレートおよびダイヤラインターフェイスで BFD 機能はサポートされません。仮想テンプレートおよびダイヤラインターフェイスで BFD を設定しないでください。
- Cisco IOS Release 12.2(18)SXE（およびそれ以降の SX リリース）、12.0(31)S、12.4(4)T、12.0(32)S、12.2(33)SRA、12.2(33)SRB、12.2(33)SRC、および 12.2(33)SB では、IPv4 ネットワークに対してだけシスコの BFD 実装がサポートされます。
- Cisco IOS Release 12.2(33)SRB では、シスコの BFD 実装でサポートされるルーティング プロトコルはボーダー ゲートウェイ プロトコル（BGP）、Enhanced IGRP（EIGRP）、Intermediate System-to-Intermediate System（IS-IS）、および Open Shortest Path First（OSPF）だけです。Cisco IOS Release 12.2(33)SRC では、BFD でスタティック ルーティングがサポートされます。
- Cisco IOS Release 12.2(33)SRA では、シスコの BFD 実装でサポートされるルーティング プロトコルは BGP、IS-IS、および OSPF だけです。
- Cisco IOS Release 12.4(4)T では、シスコの BFD 実装でサポートされるルーティング プロトコルは BGP、EIGRP、IS-IS、および OSPF だけです。
- Cisco IOS Release 12.4(11)T では、シスコの BFD 実装でホットスタンバイ ルータ プロトコル（HSRP）のサポートが導入されています。プラットフォームおよびインターフェイスによっては、BFD サポートを利用できないものがあります。
- Cisco IOS Release 12.0(31)S および 12.0(32)S では、シスコの BFD 実装でサポートされるルーティング プロトコルは BGP、IS-IS、および OSPF だけです。
- Cisco IOS Release 12.2(18)SXE では、シスコの BFD 実装でサポートされるルーティング プロトコルは EIGRP、IS-IS、および OSPF だけです。
- Cisco IOS Release 12.2(18)SXH および 12.2(33)SB では、シスコの BFD 実装でサポートされるルーティング プロトコルは BGP、EIGRP、IS-IS、および OSPF です。
- BFD は直接接続されたネイバーだけに対して動作します。BFD のネイバーは 1 ホップ以内に限られます。マルチホップのコンフィギュレーションはサポートされません。
- プラットフォームおよびインターフェイスによっては、BFD サポートを利用できないものがあります。特定のプラットフォームまたはインターフェイスで BFD のサポートについて確認

し、プラットフォームとハードウェアの正確な制約事項を入手するには、お使いのソフトウェア バージョンの Cisco IOS ソフトウェアのリリース ノートを参照してください。

- Cisco IOS Release 12.2SXF、12.2SRC、および 12.2SRB では、BFD on PortChannel 設定がサポートされません。
- Cisco 10720 インターネット ルータでは、ファスト イーサネット、ギガビット イーサネット、および RPR-IEEE インターフェイスだけで BFD がサポートされます。BFD は、Spatial Reuse Protocol（SRP）および Packet-over-SONET（POS）インターフェイスでサポートされません。
- **bfd** コマンドを使用して（インターフェイス コンフィギュレーション モードで）Cisco 10720 インターフェイスで BFD セッション パラメータを設定する場合、**interval***milliseconds* と **min_rx***milliseconds* パラメータの両方の *milliseconds* 引数でサポートされる設定可能な期間の最小値は 50 ミリ秒（ms）です。
- Cisco 10720 インターネット ルータでは、最大 100 の BFD セッションがサポートされます。BFD がルーティング プロトコル間の接続をセットアップして Cisco 10720 インターネット ルータと隣接ルータの間で 101 番目のセッションを確立しようとすると、次のエラー メッセージが表示されます。

```
00:01:24: %OSPF-5-ADJCHG: Process 100, Nbr 10.0.0.0 on RPR-IEEE1/1 from LOADING to
FULL, Loading Done
00:01:24: %BFD-5-SESSIONLIMIT: Attempt to exceed session limit of 100 neighbors.
```

- BFD パケットは自己生成パケットの QoS ポリシーでは一致しません。
- BFD パケットは **classclass-default** コマンドで一致します。そのため、ユーザは適切な帯域幅の可用性を確認して、オーバーサブスクリプションによる BFD パケットのドロップを防ぐ必要があります。
- Cisco 10720 インターネット ルータでは次の BFD 機能がサポートされません。
  - デマンド モード
  - エコー パケット
  - BFD over IP Version 6
- Cisco 12000 シリーズのルータでは、ピア デバイス間の非対称ルーティングによって、BFD 制御パケットが、セッションを開始したラインカード以外のラインカードで受信されます。このような特殊な場合は、ルーティング ピア間の BFD セッションが確立されません。
- 分散 Cisco 12000 シリーズのインターネット ルータの 1 つのラインカードごとに、最大 100 セッションがサポートされます。ネイバーとのセッションがダウンしていると宣言される前に、リモート システムから受信する BFD 制御パケットの最大 3 回のリトライ回数での最大 hello 間隔は 50 ms です。
- Cisco IOS Release 12.2(33)SB では、BFD がステートフル スイッチオーバー（SSO）に対応しておらず、NSF/SSO でサポートされません。これらの機能は一緒に使用しないでください。NSF/SSO と BFD を同時にイネーブルにすると、BFD の隣接関係が維持されず、ルーティング クライアントには隣接関係停止と再コンバージェンスのマークが強制的に付けられるため、フェールオーバー中にノンストップ フォワーディング機能が動作しません。

- BFD は VTI トンネルではサポートされていません。
- Cisco IOS Release 15.6(3)M からは、Cisco ISR G2 モジュラ ルータの ipbasek9 イメージでも BFD がサポートされます。たとえば、EIGRP 機能が ipbasek9 イメージの一部である場合は、EIGRP の BFD 機能も ipbasek9 イメージの一部です。ある機能が、BFD をサポートする IP Base 以外のソフトウェア パッケージの一部である場合は、関連する BFD 機能は同等のソフトウェア パッケージの一部です。

BFD Control Channel over VCCV：ATM 疑似回線のサポート

- BFD Control Channel over VCCV：非同期転送モード疑似回線のサポート機能では、IP/User Datagram Protocol（UDP）のカプセル化なしで VCCV タイプ 1 のみがサポートされます。
- Any Transport over Multiprotocol Label Switching（AToM）は、BFD Control Channel over VCCV：ATM 疑似回線のサポート機能でサポートされる唯一のトランスポート プロトコルです。
- レイヤ 2 トランスポート プロトコル バージョン 3（L2TPv3）はサポートされません。
- 冗長疑似回線はサポートされません。
- ATM の接続回線（AC）はサポートされます。

Cisco IOS Release 12.2(33)SXI2 と Cisco Catalyst 6500 シリーズ スイッチ

- Cisco Catalyst 6500 シリーズ スイッチでは、最小 hello 間隔 50 ms、倍率 3 で最大 100 の BFD セッションがサポートされます。この倍率は、セッションがダウンしたと宣言される前に失われた可能性のある連続するパケットの最小数を指定します。
- SSO がデュアル RP システムでイネーブルになっている場合、次の制約事項が適用されます。
  - サポートされる BFD セッションの最大数は 50 です。
  - 倍率 3 以上の最小 hello 間隔は 500 ms です。
  - EIGRP がイネーブルの場合、サポートされる BFD セッションの最大数は 30 に減少します。
  - エコー モードは Distributed Forwarding Card（DFC）だけでサポートされます。
- BFD SSO は E シャーシおよび 67xx ラインカードを使用する Cisco Catalyst 6500 シリーズだけでサポートされます。Centralized Forwarding Card（CFC）インターフェイスはサポートされません。
- エコーモードをイネーブルにするには、システムを **noipredirects** コマンドで設定する必要があります。
- In Service Software Upgrade（ISSU）サイクルでは、ラインカードがリセットされ、BFD セッションでルーティング フラップが発生します。

Cisco Catalyst 6000 シリーズ スイッチ

- Cisco Catalyst 6000 シリーズ スイッチでは、スーパバイザ アップリンク ポートを 750*750*5 ミリ秒の BFD タイマー値と関連付ける必要があります。ステートフル スイッチオーバー（SSO）時またはピアのリロード時の冗長ファシリティ（RF）プログレッションと EtherChannel（ポート チャネル）の負荷計算には 1.5 ～ 2.5 秒かかるためです。これは BFD エコー パケットがスーパバイザ アップリンクで交換される場合でも適用されます。

Cisco IOS Release 15.1(2)S および Cisco 7600 シリーズ ルータの ES+ ライン カード

Cisco IOS Release 15.1(2)S では、Cisco 7600 シリーズ ルータで ES+ ライン カードへの BFD セッションのオフロードがサポートされています。ハードウェア オフロードの制限事項の詳細については、『*Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*』の「Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card」の項を参照してください。

Cisco IOS Release 15.1(3)S：BFD マルチホップのサポート

- IPv4 および IPv6 の BFD マルチホップ セッションのみがサポートされます。
- マルチホップ セッションはハードウェアにオフロードされません。
- IPv6 リンク ローカル アドレスは、BFD マルチホップ セッションではサポートされません。
- エコー モードはマルチホップではサポートされません。

（注） プラットフォームとハードウェアの正確な制約事項については、お使いのソフトウェア バージョンの Cisco IOS ソフトウェアのリリース ノートを参照してください。

ポイントツーポイント IPv4、IPv6、および GRE トンネルのサポート

シスコのソフトウェアでは、ご使用のリリースによって、ポイントツーポイント IPv4、IPv6、および Generic Routing Encapsulation（GRE）トンネルでの BFD 転送がサポートされます。

ナンバード インターフェイスのみが許可されます。トンネル タイプがサポート対象のトンネル タイプからサポートされていないトンネルタイプに変更されると、そのトンネルの BFD セッションはダウン状態になり、BFD 設定がインターフェイスから削除されます。

BFD 検出時間はトポロジとインフラストラクチャによって異なります。物理的に隣接するデバイスをまたいで展開されたシングルホップ IP トンネルの場合、150 ms（つまり、50 ms の Hello インターバルで再試行は 3 回まで）の検出速度が適用されます。ただし、トンネルの送信元と宛先のエンドポイントがバックツーバック接続されていない場合、150 ms の検出速度は保証されません。

BFD はトンネル インターフェイスに設定された IP アドレスを使用します。トンネルの送信元アドレスと宛先アドレスは使用しません。

DMVPN での BFD サポート

- 現在、NHRP は BFD のダウン イベントでのみ機能します。アップ イベントでは機能しません。
- BFD サポートを受ける BFD を両方のピアで設定する必要があります。いずれかのピアに BFD が設定されていないと、もう 1 つのピアはダウン状態または不明な状態の BFD セッションを作成します。
- この機能を使用するには、すべてのルータを Cisco IOS XE 16.3 リリースにアップグレードする必要があります。
- スポーク間更新が想定どおりに動作するように、ピアに設定された BFD 間隔は BFD エコーモードと同じである必要があります。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、BFD セッション数が 4095 に制限されているため、ハブを最大 4095 DMVPN セッションまで拡張できます。この制限は、ASR 1000 で現在サポートされる BFD セッション数から生じます。

双方向フォワーディング検出について

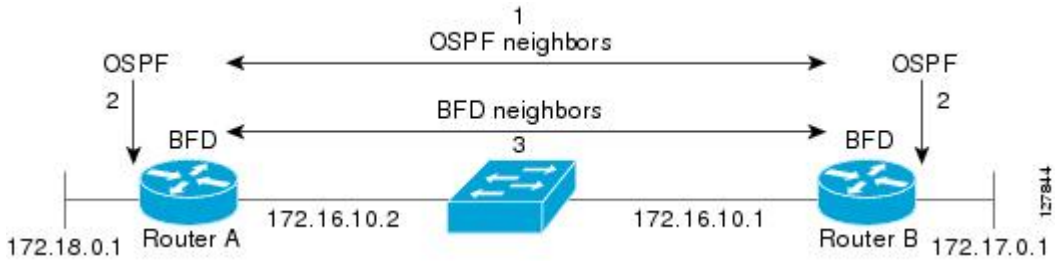
BFD の動作

BFD は、インターフェイス、データリンク、および転送プレーンを含めて、2 つの隣接ルータ間の転送パスで、オーバーヘッドの少ない短期間の障害検出方法を提供します。

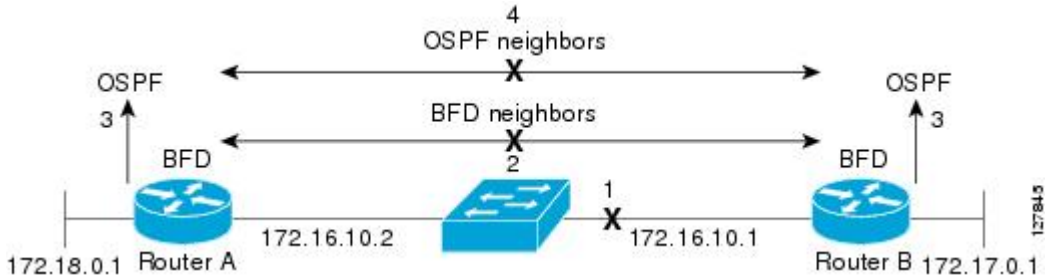
BFD はインターフェイス レベルおよびプロトコル レベルでイネーブルにする検出プロトコルです。シスコでは BFD 非同期モードをサポートしています。このモードは、2 台のシステム間で BFD 制御パケットを送信することでルータ間の BFD ネイバー セッションをアクティブ化して維持します。したがって、BFD セッションを作成するには、両方のシステム（または BFD ピア）で BFD を設定する必要があります。適切なプロトコル（NHRP およびオーバーレイ上のルーティング プロトコル）に対して、インターフェイス レベルおよびルータ レベルで BFD をイネーブルにすると、BFD セッションが作成されて BFD タイマーがネゴシエートされます。BFD ピアはネゴシエートされた間隔で BFD 制御パケットの相互送信を開始します。

ネイバー関係

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、ルーティング プロトコル BGP、EIGRP、IS-IS、および OSPF の個別の高速 BFD ピア障害検出時間を提供します。ローカル ルータのルーティング プロトコルに高速障害検出通知を送信して、ルーティング テーブル再計算プロセスを開始すると、BFD はネットワーク コンバージェンス時間全体を大幅に短縮できます。下の図に、OSPF と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバー（1）を検出すると、OSPF ネイバー ルータ（2）で BFD ネイバー セッションを開始する要求が、ローカル BFD プロセスに送信されます。OSPF ネイバー ルータでの BFD ネイバー セッションが確立されます（3）。



以下の図に、ネットワークで障害が発生した場合を示します（1）。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます（2）。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します（3）。ローカル OSPF プロセスは OSPF ネイバー関係を解除します（4）。代替パスを使用できる場合、ルータはただちにコンバージェンスを開始します。



ルーティング プロトコルでは、取得したネイバーそれぞれについて、BFD で登録する必要があります。ネイバーが登録されると、セッションがまだ存在していない場合、BFDによって、ネイバーとのセッションが開始されます。

次のとき、OSPF では、BFD を使用して登録が行われます。

- ネイバーの有限状態マシン（FSM）は、Full ステートに移行します。
- OSPF BFD と BFD の両方がイネーブルにされます。

ブロードキャスト インターフェイスでは、OSPF によって、指定ルータ（DR）とバックアップ指定ルータ（BDR）とともにのみ、BFD セッションが確立されますが、DROTHER ステートのすべての 2 台のルータ間では確立されません。

BFD の障害検出

BFD セッションが確立され、タイマーの取り消しが完了すると、BFD ピアは IGP hello プロトコルと同様に動作する（ただし、より高速な）、BFD 制御パケットを送信して状態を検出します。次の点に注意する必要があります。

- BFD はフォワーディング パスの障害検出プロトコルです。BFD は障害を検出しますが、障害が発生したピアをバイパスするには、ルーティング プロトコルがアクションを実行する必要があります。

- シスコのデバイスは、Cisco IOS Releases 12.2(18)SXE、12.0(31)S、および 12.4(4)T 用のシスコの BFD 実装では、複数のクライアント プロトコルに対して BFD セッションを 1 つ使用します。たとえば、同じピアへの同じリンクを介してネットワークで OSPF および EIGRP を実行している場合、1 つの BFD セッションだけが確立され、BFD で両方のルーティング プロトコルとセッション情報を共有します。

BFD バージョンの相互運用性

デフォルトでは、すべての BFD セッションがバージョン 1 で実行され、バージョン 0 と相互運用可能です。システムで自動的に FD バージョン検出が実行される場合、ネイバー間の BFD セッションがネイバー間の最も一般的な BFD バージョンで実行されます。たとえば、BFD ネイバーが BFD バージョン 0 を実行し、他の BFD ネイバーがバージョン 1 を実行している場合、セッションで BFD バージョン 0 が実行されます。**showbfdneighbors** [**details**] コマンドの出力で、BFD ネイバーが実行している BFD バージョンを確認できます。

BFD バージョンの検出の例については、エコーモードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定の例を参照してください。

Cisco 12000 ルータでの BFD サポート

Cisco 12000 シリーズのルータでは、Distributed ルート プロセッサ（RP）とラインカード（LC）アーキテクチャを利用する分散 BFD がサポートされます。次の項で説明するように、BFD タスクは分割され、RP および LC で BFD プロセスに割り当てられます。

RP の BFD プロセス

クライアントとの対話

RP の BFD プロセスでは、クライアントとの対話を処理します。これによって、BFD セッションが作成および削除されます。

RP の BFD プロセスのためのセッション管理

主に BFD RP プロセスが、ルータのすべての BFD セッションを所有します。その後、セッションの作成および削除の要求をすべての LC の BFD プロセスに渡します。BFD LC セッションには、クライアントによって追加または削除されるセッションの情報がありません。BFD RP プロセスだけがセッションの追加および削除のコマンドを BFD LC プロセスに送信します。

セッション データベースの管理

BFD RP プロセスは、ルータのすべての BFD セッションのデータベースを維持します。このデータベースには、必要最小限の情報だけが保存されます。

プロセスの EXEC コマンド

BFD RP プロセスは BFD の **show** コマンドを処理します。

LC の BFD プロセス

LC の BFD プロセスのためのセッション管理

BFD LC プロセスではセッションを管理し、BFD RP プロセスからのコマンドを追加および削除し、コマンドに基づいて新しいセッションを作成および削除します。送信の失敗、受信の失敗、またはセッション ダウンの検出が発生した場合、LC BFD インスタンスでただちに BFD RP プロセスが通知されます。また、送信および受信のカウンタが更新されます。BFD セッションは LC で完全に管理されます。BFD 制御パケットが、LC 自体から送信された場合と同様に受信され、処理されます。

セッション データベースの管理

BFD LC プロセスで、LC でホストされるすべての BFD セッションのデータベースを維持します。

受信と送信

BFD LC プロセスでは、LC のセッションに対する BFD の送受信を行います。

BFD セッションの制限

Cisco IOS Release 12.2(33)SRC では、作成できる BFD セッションの数が 128 に増えました。

非ブロードキャスト メディア インターフェイスに対する BFD サポート

Cisco IOS Release 12.2(33)SRC では、BFD 機能が非ブロードキャスト メディア インターフェイス（ATM、POS、シリアル、および VLAN インターフェイスなど）でサポートされます。BFD のサポートは ATM、フレーム リレー（FR）、POS、およびシリアル サブインターフェイスに拡張されます。

bfd interval コマンドは、BFD モニタリングを開始するインターフェイスで設定する必要があります。

VPN ルーティングおよび転送インターフェイスに対する BFD サポート

Cisco IOS Release 12.2(33)SRC では BFD 機能が、プロバイダー エッジ（PE）ルータとカスタマー エッジ（CE）ルータの間のルーティング プロトコル障害の高速検出を提供するように、VPN ルーティングおよび転送（VRF）対応に拡張されています。

ステートフル スイッチオーバーでのノンストップ フォワーディングの BFD サポート

通常、ネットワーキング デバイスを再起動すると、そのデバイスのすべてのルーティング ピアがデバイスの終了および再起動を検出します。この遷移によってルーティング フラップが発生し、そのために複数のルーティング ドメインに分散される可能性があります。ルーティングの再起動

によって発生したルーティング フラップによって、ルーティングが不安定になります。これはネットワーク全体のパフォーマンスに悪影響を及ぼします。ノンストップフォワーディング（NSF）は、ステートフル スイッチオーバー（SSO）がイネーブルになっているデバイスのルーティングフラップを抑制するのに役立ち、それによってネットワークの不安定さが減少します。

NSF では、ルーティング プロトコル情報がスイッチオーバー後に保存されるとき、既知のルータでデータ パケットのフォワーディングを継続できます。NSF を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生しません。データ トラフィックはインテリジェントラインカードまたはデュアルフォワーディングプロセッサを介して転送されますが、スタンバイ RP では、スイッチオーバー中に障害が発生したアクティブな RP からの制御と見なされます。ラインカードおよびフォワーディング プロセッサの機能はスイッチオーバーによって維持され、アクティブな RP の転送情報ベース（FIB）が NSF 動作で最新状態が維持されます。

デュアル RP をサポートするデバイスでは、SSO が RP の 1 つをアクティブなプロセッサとして確立し、他の RP はスタンバイ プロセッサに割り当てられ、それらの間で情報が同期されます。アクティブな RP に障害が発生したとき、ネットワーキング デバイスから削除されたとき、または手動でメンテナンスから排除されたときに、アクティブなプロセッサとスタンバイ プロセッサからのスイッチオーバーが発生します。

ステートフル スイッチオーバーの BFD サポート

BFD プロトコルでは、隣接するフォワーディング エンジン間でパスに短期間の障害検出が行われます。デュアル RP ルータまたはスイッチ（冗長性のため）を使用するネットワーク導入では、ルータにグレースフル リスタート メカニズムがあり、アクティブな RP とスタンバイ RP の間のスイッチオーバー時にフォワーディング状態が保護されます。

ハードウェアの通信障害を検出する機能に応じて、デュアル RP のスイッチオーバー回数が異なります。BFD が RP で稼働している場合、一部のプラットフォームでは BFD プロトコルがタイムアウトになる前にスイッチオーバーを検出することはできません。このようなプラットフォームは低速スイッチオーバー プラットフォームと呼ばれます。

スタンバイ RP のステートフル BFD

スタンバイ RP へのスイッチオーバーを成功させるために、BFD プロトコルでチェックポイントメッセージを使用して、アクティブな RP Cisco IOS インスタンスからセッション情報をスタンバイ RP Cisco IOS インスタンスに送信します。セッション情報には、ローカル識別子およびリモート識別子、隣接ルータのタイマー情報、BFD セットアップ情報、およびセッション固有の情報（セッションのタイプやセッションのバージョンなど）が含まれます。さらに、BFD プロトコルはセッションの作成および削除のチェックポイント メッセージを送信して、スタンバイ RP でセッションを作成または削除します。

スタンバイ RP の BFD セッションはパケットの送受信を行わず、期限切れになったタイマーを処理しません。このようなセッションは、スイッチオーバーの発生を待ってからアクティブ セッションのパケットを送信し、セッションが隣接ルータでタイム アウトにならないようにします。

スタンバイ RP の BFD プロトコルはスイッチオーバーの通知を受けると、状態をアクティブに変更し、自分自身をシスコエクスプレスフォワーディングに登録することで、パケットを受信し、期限切れになったすべての要素にパケットを送信できるようにします。

また、BFDではチェックポイントメッセージを使用して、アクティブなRPでクライアントによって作成されたセッションをスイッチオーバー時に維持します。スイッチオーバーが発生すると、BFDはSSO再要求タイマーを起動します。クライアントは再要求タイマーによって指定された期間内のセッションを再要求する必要があります。そうしないと、セッションが削除されます。

スタティック ルーティングの BFD サポート

OSPFやBGPなどの動的なルーティング プロトコルとは異なり、スタティック ルーティングにはピア検出の方法がありません。したがって、BFD が設定されると、ゲートウェイの到達可能性は完全に指定されたネイバーへのBFDセッションの状態に依存します。BFDセッションが開始されない限り、スタティック ルートのゲートウェイは到達不能と見なされ、したがって、影響を受けるルートが適切なルーティング情報ベース（RIB）にインストールされません。

BFDセッションが正常に確立されるように、ピア上のインターフェイスでBFDを設定し、ピア上の BFD クライアントに BFD ネイバーのアドレスを登録する必要があります。インターフェイスがダイナミック ルーティング プロトコルで使用される場合、後者の要件は通常、BFD の各ネイバーでルーティング プロトコル インスタンスを設定することによって満たされます。インターフェイスがスタティック ルーティングに排他的に使用される場合、この要件はピア上でスタティック ルートを設定することによって満たす必要があります。

BFDセッションが起動状態のときにBFD設定がリモートピアから削除された場合、BFDセッションの最新状態が IPv4 スタティックに送信されません。その結果、スタティック ルートが RIB に残ります。唯一の回避策は、IPv4スタティックBFDネイバー設定を削除して、スタティック ルートがBFDセッション状態を追跡しないようにすることです。また、シリアルインターフェイスのカプセル化のタイプをBFDでサポートされていないタイプに変更する場合、このインターフェイスでBFDがダウン状態になります。回避策はインターフェイスをシャットダウンし、サポートされているカプセル化のタイプに変更してから、BFD を再設定することです。

IPv4 スタティック クライアントでは 1 つの BFD セッションを使用して、特定のインターフェイスを通るネクスト ホップの到達可能性を追跡できます。一連の BFD 追跡対象スタティック ルートに対して BFD グループを割り当てることができます。各グループには 1 つのアクティブ スタティック BFD 設定、1 つ以上のパッシブ BFD 構成、および対応する BFD 追跡対象スタティック ルートが必要です。nongroup エントリは、BFD グループが割り当てられていない BFD 追跡対象スタティック ルートです。BFD グループは、さまざまなVRFの一部として構成可能なスタティックBFD設定に対応する必要があります。実際には、パッシブ スタティックBFD設定は、アクティブな設定と同じ VRF に構成する必要はありません。

BFD グループごとに存在するアクティブなスタティック BFD セッションは 1 つだけです。スタティック BFD 設定とその BFD 設定を使用する対応のスタティック ルートを追加して、アクティブBFDセッションを設定できます。アクティブなスタティックBFD構成とそのスタティックBFD設定を使用するスタティック ルートがある場合にのみ、グループのBFDセッションが作成されます。アクティブなスタティック BFD 設定またはアクティブなスタティック ルートが BFD グループから削除されると、パッシブなスタティック ルートがすべて RIB から削除されます。実際には、すべてのパッシブなスタティック ルートは、アクティブなスタティック BFD 設定と、アクティブなBFDセッションで追跡されるスタティック ルートがグループで設定されるまでは非アクティブです。

同様に、BFD グループごとに 1 つ以上のパッシブなスタティック BFD 設定と、対応する BFD 追跡対象スタティック ルートが存在します。パッシブなスタティック セッション ルートは、アクティブなBFDセッション状態が到達可能であるときだけ有効です。グループのアクティブなBFDセッション状態が到達可能であっても、対応するインターフェイスの状態がアップである場合にのみ、パッシブなスタティック ルートが RIB に追加されます。パッシブな BFD セッションがグループから削除されると、アクティブな BFD セッション（存在する場合）や BFD グループの到達可能性ステータスには影響しません。

ATM 疑似回線の BFD Control Channel over VCCV のサポート

マルチプロトコル ラベル スイッチング（MPLS）の疑似回線では、IP/MPLS コア ネットワークを介して送信するため、L2 トラフィックがイネーブルにされます。BFD Control Channel over VCCV：ATM 疑似回線のサポート機能では、MPLS 疑似回線の Operations And Management（OAM）機能が提供されます。

（注） この機能により、VCCV タイプ 1 のみがサポートされます。VCCV タイプ 1 は、インバンド VCCV で、コントロール ワードが使用されている MPLS 疑似回線のみで使用できます。

BFD 検出プロトコルを使用すると、MPLS プロトコルに OAM 機能を提供できます。VCCV では、疑似回線に関連付けられている制御チャネルが提供され、疑似回線を介して OAM 機能が提供されます。BFD では、VCCV 制御チャネルを疑似回線障害メカニズムとして使用され、データプレーンの障害が検出されます。BFD では、VCCV 制御チャネルを使用して、接続回線（AC）の障害ステータスを示すことができます。

MPLS の疑似回線では、動的に信号を送信するか、静的に仮想回線（VC）ラベルを設定することができます。動的に信号が送信される疑似回線では、Control Channel（CC）タイプおよび Connection Verification（CV）タイプにも、信号が送信されます。静的に設定される疑似回線では、CC タイプと CV タイプは両方とも、疑似回線の両側に設定されます。

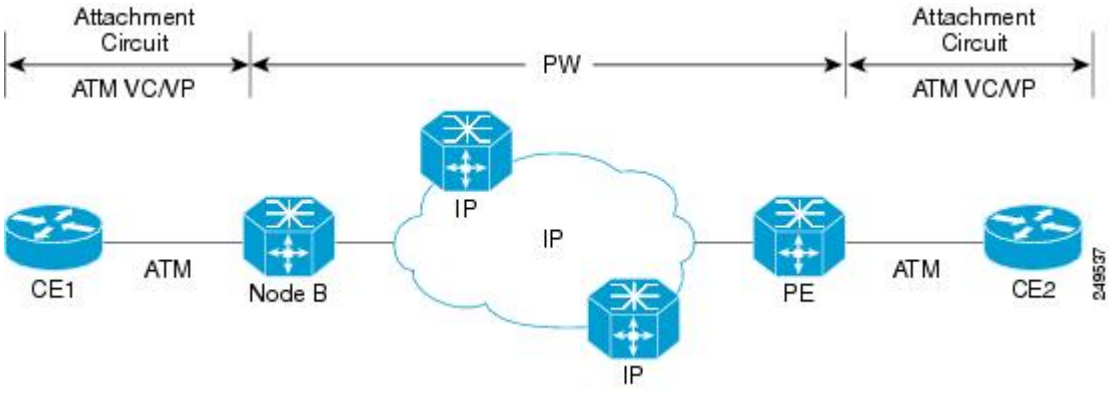
CC タイプでは、疑似回線に対して VCCV パケットはインバンドまたはアウトオブバウンドです。CV タイプでは、疑似回線に対して BFD のモニタリングが必要かどうかが定義されます。疑似回線に対して BFD のモニタリングが必要な場合、CV タイプでは、BFD パケットのカプセル化の方法、および、BFD によって、ステータスのシグナリング機能が提供されるかどうかが、定義されます。

BFD のモニタリングが必要なすべてのプロトコルでは、BFD を使用してクライアントとして登録される必要があります。たとえば、Xconnect プロトコルでは BFD クライアントとして定義され、BFD によって、Xconnect に対するクライアント ID が割り当てられます。Xconnect では、このクライアント ID が使用されて、疑似回線をモニタする BFD セッションが作成されます。

BFD では、疑似回線パスで、転送障害（エンドツーエンド）を検出できます。BFD で疑似回線の転送パスに障害が検出されると、セッションを作成した Xconnect クライアントに通知されます。さらに、BFD では、BFD セッションが中断されたリモートデバイスに、すべての連結パスまたは AC でのステータスの信号が送信されます。

下の図に、ATM ペイロードが含まれる、動的に信号が送信される MPLS 疑似回線を示します。この例では、疑似回線の BFD のモニタリングは、ノード B デバイスから PE デバイスに対して発生

します。BFD では、PE デバイスと CE2 デバイス、ノード B と CE1 デバイスとの間の、AC の信号ステータスがモニタされます。



マルチホップでの BFD

Cisco IOS Release 15.1(3)S 以降のリリースでは、複数のネットワーク ホップにまたがる可能性の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 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。

マルチホップ テンプレートを作成し、それを宛先と関連 BFD タイマーの 1 つ以上のマップに関連付けるには、**bfd-template** および **bfd map** コマンドを設定する必要があります。認証をイネーブルにして、BFD マルチホップ セッションのキー チェーンを設定できます。

障害検出に BFD を使用することの利点

機能を導入するときは、あらゆる代替策を検討し、トレードオフに注意することが重要です。

EIGRP、IS-IS、および OSPF の通常の導入で BFD に最も近い代替策は、EIGRP、IS-IS、および OSPF ルーティング プロトコルの変更された障害検出メカニズムを使用することです。

EIGRP の hello およびホールド タイマーを絶対最小値に設定する場合、EIGRP の障害検出速度が 1～2 秒程度に下がります。

IS-IS または OSPF に fast hello を使用する場合、これらの Interior Gateway Protocol（IGP）プロトコルによって障害検出メカニズムが最小 1 秒に減少します。

ルーティング プロトコルの減少したタイマー メカニズムで BFD を実装すると、いくつかの利点があります。

- EIGRP、IS-IS、および OSPF タイマーによって 1 秒または 2 秒の最小検出タイマーを実現できますが、障害検出が 1 秒未満になる場合もあります。

- BFD は特定のルーティング プロトコルに関連付けられていないため、EIGRP、IS-IS、および OSPF の汎用の整合性のある障害検出メカニズムとして使用できます。
- BFD の一部をデータ プレーンに分散できるため、コントロール プレーンに全体が存在する分散 EIGRP、IS-IS、および OSPF タイマーよりも CPU の負荷を軽くすることができます。

DMVPN での BFD サポートの利点

- リンク障害をより速く検出できます。
- 非暗号化の導入環境の場合、スポークは NHRP 登録のタイムアウト後はハブの障害しか検出できません。また、ルーティングによる再コンバージェンスが早い段階で可能であっても、ハブのキャッシュが期限切れになるまで、ハブはスポークの障害を検出できません。BFD ではこのような障害を迅速に検出できます。
- たとえばハブがスポークの代わりに応答するように設定されている場合に、BFD は権限のないセッション間の転送パスを検証します。
- BFD はトンネルを通過しない IKE キープアライブまたは DPD とは異なり、トンネルを含むエンドツーエンドのデータ パスを検証します。
- BFD プローブはオフロード可能です。

DMVPN での BFD サポート用に特別な NHRP 設定を行う必要はありません。NHRP 対応インターフェイスで BFD をイネーブルにするだけです。DMVPN 設定については、「ダイナミック マルチポイント VPN の設定方法」を参照してください。

双方向フォワーディング検出の設定方法

インターフェイスでの BFD セッション パラメータの設定

この手順では、インターフェイスで基本 BFD セッション パラメータを設定することによって、インターフェイスで BFD を設定する方法を示します。BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの手順を実行します。
   - **ipaddress** *ipv4-address mask*
   - **ipv6address** *ipv6-address/mask*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。

ステップ 3	次のいずれかの手順を実行します。
	• **ipaddress** *ipv4-address mask*
	• **ipv6address** *ipv6-address/mask*
	
	例：
	インターフェイスの IPv4 アドレスの設定：
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	インターフェイスの IPv6 アドレスの設定：
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`
		インターフェイスに IP アドレスを設定します。

ステップ 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*	インターフェイスで BFD をイネーブルにします。 bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。

	コマンドまたはアクション	目的
	例： `Device(config-if)# bfd interval 50 min_rx 50 multiplier 5`	bfd interval 設定は次のような場合には削除されません。 • IPv4 アドレスがインターフェイスから削除された場合 • IPv6 アドレスがインターフェイスから削除された場合 • IPv6 がインターフェイスからディセーブルにされた場合 • インターフェイスがシャットダウンされた場合 • インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合 • インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック ルーティング プロトコルに対する BFD サポートの設定

ルータ レベルでダイナミック ルーティング プロトコルの BFD サポートをイネーブルにして、すべてのインターフェイスに対してグローバルに BFD サポートをイネーブルにするか、またはインターフェイス レベルでインターフェイスごとに BFD を設定することができます。

Cisco IOS Release 12.2(18)SXE では、ルーティング プロトコル EIGRP、IS-IS、および OSPF の 1 つ以上に対して BFD サポートを設定できます。

Cisco IOS Release 12.2(33)SRA では、ルーティング プロトコル EIGRP、IS-IS、および OSPF の 1 つ以上に対して BFD サポートを設定できます。

Cisco IOS Release 12.2(33)SRB では、ルーティング プロトコル BGP、EIGRP、IS-IS、および OSPF の 1 つ以上に対して BFD サポートを設定できます。

Cisco IOS Release 12.2(33)SRC では、スタティック ルーティングに対して BFD サポートを設定できます。

Cisco IOS Release 12.0(31)S および 12.4(4)T では、ルーティング プロトコル BGP、IS-IS、および OSPF の 1 つ以上に対して BFD サポートを設定できます。

Cisco IOS Release 12.0(32)S では、Cisco 10720 プラットフォームで、ルーティング プロトコル BGP、IS-IS、および OSPF の 1 つ以上に対して BFD を設定できます。

Cisco IOS Release 12.4(11)T では、HSRP に対する BFD サポートが導入されました。

ここでは、次の手順について説明します。

BGP に対する BFD サポートの設定

ここでは、BGP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、BGP に対する BFD サポートを設定する手順について説明します。

はじめる前に

BGP は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **routerbgp***as-tag*
4. **neighbor***ip-address***fall-overbfd**
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipbgpneighbor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**routerbgp***as-tag* 例： `Router(config)# router bgp tag1`	BGP プロセスを指定し、ルータ 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***fall-overbfd** 例： `Router(config-router)# neighbor 172.16.10.2 fall-over bfd`	フェールオーバーに対する BFD サポートをイネーブルにします。
ステップ 5	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors detail`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されることを確認します。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 7	**showipbgpneighbor** 例： `Router# show ip bgp neighbor`	（任意）ネイバーへの BGP および TCP 接続についての情報を表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次の項を参照してください。

EIGRP に対する BFD サポートの設定

ここでは、EIGRP が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、EIGRP に対する BFD サポートを設定する手順について説明します。EIGRP に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、EIGRP がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。
- ルータ コンフィギュレーション モードで **bfdinterface***typenumber* コマンドを使用して、EIGRP がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

はじめる前に

EIGRP は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェア オフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

（注） EIGRP に対する BFD は、Cisco IOS Release 12.0(31)S、12.0(32)S、12.4(4)T、および 12.2(33)SRA の Cisco 12000 シリーズ ルータでサポートされません。

手順の概要

1. **enable**
2. **configureterminal**
3. **routereigrp***as-number*
4. 次のいずれかを実行します。
   - **bfdall-interfaces**
   - **bfdinterface***typenumber*
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipeigrpinterfaces** [*typenumber*] [*as-number*] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**routereigrp***as-number* 例： `Router(config)# router eigrp 123`	EIGRP ルーティング プロセスを設定し、ルータ 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	次のいずれかを実行します。
	
	• **bfdall-interfaces**
	
	• **bfdinterface***typenumber*
	
	例：
	
	`Router(config-router)# bfd all-interfaces`
	
	例：
	
	`Router(config-router)# bfd interface FastEthernet 6/0`
		EIGRP ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
		
		または
		
		EIGRP ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。

ステップ 5	**end** 例： `Router(config-router) end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されることを確認します。

	コマンドまたはアクション	目的
		（注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 7	**showipeigrpinterfaces** [*typenumber*] [*as-number*] [**detail**] 例： `Router# show ip eigrp interfaces detail`	（任意）EIGRP に対する BFD サポートがイネーブルになっているインターフェイスを表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次の項を参照してください。

IS-IS に対する BFD サポートの設定

ここでは、IS-IS が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、IS-IS に対する BFD サポートを設定する手順について説明します。IS-IS に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用して、IS-IS が IPv4 ルーティングをサポートしているすべてのインターフェイスに対して BFD をイネーブルにできます。次にインターフェイス コンフィギュレーション モードで **isisbfddisable** コマンドを使用すると、1 つ以上のインターフェイスに対して BFD をディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **isis bfd** コマンドを使用すると、IS-IS がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

IS-IS に対する BFD サポートを設定するには、次のいずれかの手順に従います。

前提条件

IS-IS は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでのBFDセッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

すべてのインターフェイスの IS-IS に対する BFD サポートの設定

IPv4 ルーティングをサポートするすべての IS-IS インターフェイスで BFD を設定するには、この項の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **routerisis***area-tag*
4. **bfdall-interfaces**
5. **exit**
6. **interface***typenumber*
7. **iprouterisis** [*tag*]
8. **isisbfd**[**disable**]
9. **end**
10. **showbfdneighbors**[**details**]
11. **showclnsinterface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**routerisis***area-tag* 例： `Router(config)# router isis tag1`	IS-IS プロセスを指定し、ルータ 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	**bfdall-interfaces** 例： `Router(config-router)# bfd all-interfaces`	IS-IS ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
ステップ 5	**exit** 例： `Router(config-router)# exit`	（任意）ルータでグローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface***typenumber* 例： `Router(config)# interface fastethernet 6/0`	（任意）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 7	**iprouterisis** [*tag*] 例： `Router(config-if)# ip router isis tag1`	（任意）インターフェイスで IPv4 ルーティングのサポートをイネーブルにします。
ステップ 8	**isisbfd**[**disable**] 例： `Router(config-if)# isis bfd`	（任意）IS-IS ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して IS-IS が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 10	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 11	**showclnsinterface** 例： `Router# show clns interface`	（任意）IS-IS に対する BFD が、関連付けられた特定の IS-IS インターフェイスに対してイネーブルになっているかどうかを検証するために使用できる情報を表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。インターフェイスの特定のサブセットに対してだけ設定する場合は、「1 つ以上のインターフェイスの IS-IS に対する BFD サポートの設定」の項のタスクを実行します。

1 つ以上のインターフェイスの IS-IS に対する BFD サポートの設定

1 つ以上の IS-IS インターフェイスだけに BFD を設定するには、この項の手順に従います。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **iprouterisis** [*tag*]
5. **isisbfd[disable]**
6. **end**
7. **showbfdneighbors**[**details**]
8. **showclnsinterface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Router(config)# interface fastethernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**iprouterisis** [*tag*] 例： `Router(config-if)# ip router isis tag1`	インターフェイスで IPv4 ルーティングのサポートをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**isisbfd[disable]** 例： `Router(config-if)# isis bfd`	IS-IS ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して IS-IS が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 8	**showclnsinterface** 例： `Router# show clns interface`	（任意）IS-IS に対する BFD が、関連付けられた特定の IS-IS インターフェイスに対してイネーブルになっているかどうかを検証するために使用できる情報を表示します。

次の作業

BFD のモニタリングとメンテナンスの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次のいずれかの項を参照してください。

OSPF に対する BFD サポートの設定

ここでは、OSPF が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、OSPF に対する BFD サポートを設定する手順について説明します。すべてのインターフェイスでグローバルに OSPF に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。

OSPF に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、OSPF がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ip ospf bfd** [**disable**] コマンドを使用して、個々のインターフェイスで BFD サポートをディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ip ospf bfd** コマンドを使用して、OSPF がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

OSPF に対する BFD サポートのタスクについては、次の項を参照してください。

すべてのインターフェイスの OSPF に対する BFD サポートの設定

すべての OSPF インターフェイスに BFD を設定するには、この項の手順に従います。

すべての OSPF インターフェイスに対して BFD を設定するのではなく、特定の 1 つ以上のインターフェイスに対して BFD サポートを設定する場合は、「Configuring BFD Support for OSPF for One or More Interfaces」の項を参照してください。

はじめる前に

OSPF は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

（注） **showbfdneighborsdetails** コマンドの出力には、設定された間隔が表示されます。ハードウェアオフロードされた BFD セッションが 50 ms の倍数でない Tx および Rx 間隔で設定されていたために変更された間隔は出力に表示されません。

手順の概要

1. **enable**
2. **configureterminal**
3. **router ospf** *process-id*
4. **bfdall-interfaces**
5. **exit**
6. **interface***typenumber*
7. **ipospfbfd**[**disable**]
8. **end**
9. **showbfdneighbors**[**details**]
10. **showipospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospf** *process-id* 例： `Router(config)# router ospf 4`	OSPF プロセスを指定し、ルータ 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	**bfdall-interfaces** 例： `Router(config-router)# bfd all-interfaces`	OSPF ルーティング プロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルにイネーブルにします。
ステップ 5	**exit** 例： `Router(config-router)# exit`	（任意）ルータでグローバル コンフィギュレーション モードに戻ります。手順 7 を実行して 1 つ以上のインターフェイスに対して BFD をディセーブルにする場合にだけ、このコマンドを入力します。

	コマンドまたはアクション	目的
ステップ 6	**interface***typenumber* 例： `Router(config)# interface fastethernet 6/0`	（任意）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。手順 7 を実行して 1 つ以上のインターフェイスに対して BFD をディセーブルにする場合にだけ、このコマンドを入力します。
ステップ 7	**ipospfbfd**[**disable**] 例： `Router(config-if)# ip ospf bfd disable`	（任意）OSPF ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して OSPF が関連付けられたすべてのインターフェイスでBFDをイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 8	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors detail`	（任意）BFDネイバーがアクティブで、BFDが登録したルーティングプロトコルが表示されるかどうかの検証に使用できる情報を表示します。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でないTxおよびRx間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 10	**showipospf** 例： `Router# show ip ospf`	（任意）OSPF に対して BFD がイネーブルになっているかどうかを検証するために使用できる情報を表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次の項を参照してください。

1 つ以上のインターフェイスの OSPF に対する BFD サポートの設定

1 つ以上の OSPF インターフェイスで BFD を設定するには、この項の手順に従います。

はじめる前に

OSPF は、関連するすべてのルータで実行する必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipospfbfd**[**disable**]
5. **end**
6. **showbfdneighbors**[**details**]
7. **showipospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface***typenumber* 例： `Router(config)# interface fastethernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipospfbfd**[**disable**] 例： `Router(config-if)# ip ospf bfd`	OSPF ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルまたはディセーブルにします。 （注） ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して OSPF が関連付けられたすべてのインターフェイスで BFD をイネーブルにした場合にだけ、**disable** キーワードを使用する必要があります。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD ネイバーがアクティブで、BFD が登録したルーティング プロトコルが表示されるかどうかの検証に使用できる情報を表示します。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ラインカードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ラインカードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 7	**showiopspf** 例： `Router# show ip ospf`	（任意）OSPF に対して BFD サポートがイネーブルになっているかどうかを検証するために使用できる情報を表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次の項を参照してください。

HSRP に対する BFD サポートの設定

ホットスタンバイ ルータ プロトコル（HSRP）の BFD サポートをイネーブルにするには、次の作業を実行します。この手順のステップは、HSRP ピアに BFD セッションを実行する各インターフェイスで行ってください。

デフォルトでは、HSRP は BFD をサポートします。BFD に対する HSRP サポートが手動でディセーブルになっている場合、ルータ レベルで再びイネーブルにして、すべてのインターフェイスに対してグローバルに BFD サポートをイネーブルにするか、またはインターフェイス レベルでインターフェイスごとにイネーブルにすることができます。

はじめる前に

- HSRP は、関連するすべてのルータで実行する必要があります。
- シスコ エクスプレス フォワーディングをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipcef**[**distributed**]
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standbybfd**
8. **exit**
9. **standbybfdall-interfaces**
10. **exit**
11. **showstandbyneighbors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipcef**[**distributed**] 例： `Router(config)# ip cef`	シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングをイネーブルにします。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface FastEthernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.11 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.11`	HSRP をアクティブにします。
ステップ 7	**standbybfd** 例： `Router(config-if)# standby bfd`	（任意）インターフェイスで BFD に対する HSRP をイネーブルにします。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**standbybfdall-interfaces** 例： `Router(config)# standby bfd all-interfaces`	（任意）すべてのインターフェイスで BFD に対する HSRP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**showstandbyneighbors** 例： `Router# show standby neighbors`	（任意）BFD に対する HSRP サポートについての情報を表示します。

次の作業

BFD のモニタリングとトラブルシューティングの詳細については、「BFD のモニタリングとトラブルシューティング」の項を参照してください。別のルーティング プロトコルに対して BFD サポートを設定する場合は、次の項を参照してください。

スタティック ルーティングに対する BFD サポートの設定

スタティック ルーティングのための BFD サポートを設定するには、このタスクを実行します。各 BFD ネイバーに対してこの手順を繰り返します。詳細については、「例：スタティック ルーティングに対する BFD サポートの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. 次のいずれかの手順を実行します。
   - **ipaddress** *ipv4-address mask*
   - **ipv6address** *ipv6-address*/*mask*
5. **bfd interval** *milliseconds* **mix_rx** *milliseconds* **multiplier** *interval-multiplier*
6. **exit**
7. **ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]]
8. **ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
9. **exit**
10. **show ip static route**
11. **show ip static route bfd**
12. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface serial 2/0`	インターフェイスを設定し、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 4	次のいずれかの手順を実行します。 • **ipaddress** *ipv4-address mask* • **ipv6address** *ipv6-address*/*mask*	インターフェイスに IP アドレスを設定します。

	コマンドまたはアクション	目的

	例：
	インターフェイスの IPv4 アドレスの設定：
	`Device(config-if)# ip address 10.201.201.1 255.255.255.0`
	インターフェイスの IPv6 アドレスの設定：
	`Device(config-if)# ipv6 address 2001:db8:1:1::1/32`	

ステップ 5	**bfd interval** *milliseconds* **mix_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `Device(config-if)# bfd interval 500 min_rx 500 multiplier 5`	インターフェイスで BFD をイネーブルにします。 bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。 bfd interval 設定は次のような場合には削除されません。 • IPv4 アドレスがインターフェイスから削除された場合 • IPv6 アドレスがインターフェイスから削除された場合 • IPv6 がインターフェイスからディセーブルにされた場合 • インターフェイスがシャットダウンされた場合 • インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合 • インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip route static bfd** *interface-type interface-number ip-address* [**group** *group-name* [**passive**]] 例： `Device(config)# ip route static bfd serial 2/0 10.1.1.1 group group1 passive`	スタティック ルートの BFD ネイバーを指定します。 • BFD が直接接続されたネイバーだけでサポートされているため、*interface-type*、*interface-number*、および *ip-address* 引数は必須です。

	コマンドまたはアクション	目的
ステップ 8	**ip route** [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*] 例： `Device(config)# ip route 10.0.0.0 255.0.0.0`	スタティック ルートの BFD ネイバーを指定します。
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip static route** 例： `Device# show ip static route`	（任意）スタティック ルート データベース情報を表示します。
ステップ 11	**show ip static route bfd** 例： `Device# show ip static route bfd`	（任意）設定された BFD グループおよび nongroup エントリからスタティック BFD の設定に関する情報を表示します。
ステップ 12	**exit** 例： `Device# exit`	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

BFD エコー モードの設定

デフォルトではBFDエコーモードがイネーブルになっていますが、方向ごとに個別に実行できるように、ディセーブルにすることもできます。

BFD エコー モードは非同期 BFD で動作します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために、同じパスで転送されます。反対側のBFDセッションはエコー パケットの実際のフォワーディングに関与しません。エコー機能およびフォワーディングエンジンが検出プロセスを処理するため、2 つの BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディングエンジンが、リモートシステムを介さずにリモート（ネイバー）システムの転送パスをテストするため、パケット内遅延が向上する可能性があり、

それによって BFD バージョン 0 を BFD セッションの BFD 制御パケットで使用する場合に、障害検出時間を短縮できます。

エコー モードを両端で実行している（両方の BFD ネイバーがエコー モードを実行している）場合は、非対称性がないと表現されます。

前提条件

BFD は、関連するすべてのルータで実行する必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**noipredirects** コマンドを入力して、インターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージの送信をディセーブルにする必要があります。

BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」の項を参照してください。

機能制限

BFD バージョン 1 でサポートされる BFD エコー モードは、Cisco IOS Release 12.4(9) および 12.2(33)SRA だけで使用できます。

（注） BFD エコー モードは、ユニキャスト リバース パス転送（uRPF）の設定との組み合わせでは動作しません。BFD エコー モードと uRPF の設定がイネーブルの場合、セッションはフラップします。

BFD 低速タイマーの設定

この手順では、BFD の slow timer 値を変更する方法を示します。各 BFD ルータに対してこの手順を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **bfdslow-timer***milliseconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfdslow-timer***milliseconds* 例： `Switch(config)# bfd slow-timer 12000`	BFD の slow timer を設定します。
ステップ 4	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

非対称性のない BFD エコー モードのディセーブル化

この手順では、非対称性のないBFDエコー モードをディセーブルにする方法を示します。ルータからはエコー パケットが送信されず、ルータはネイバー ルータから受信する BFD エコー パケットを転送しません。

各 BFD ルータに対してこの手順を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **nobfdecho**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nobfdecho** 例： `Router(config)# no bfd echo`	BFD エコー モードをディセーブルにします。 • **no** 形式を使用すると、BFD エコー モードをディセーブルにできます。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

BFD テンプレートの作成と設定

シングルホップ テンプレートは一連の BFD 間隔値を指定するために設定できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。マルチホップ テンプレートを設定して、宛先と関連 BFD タイマーの 1 つまたは複数のマップにこれらの値を関連付けることができます。認証をイネーブルにして、BFD マルチホップ セッションのキー チェーンを設定できます。

シングルホップ テンプレートの設定

BFD シングルホップ テンプレートを作成し、BFD インターバル 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. **enable**
2. **configureterminal**
3. **bfd-templatesingle-hop***template-name*
4. **intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfd-templatesingle-hop***template-name* 例： `Router(config)# bfd-template single-hop bfdtemplate1`	シングルホップ BFD テンプレートを作成し、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 4	**intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value* 例： `Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	BFD パケット間での送受信間隔を設定し、ピアが使用不能であると BFD が宣言する前に損失される連続的な BFD 制御パケット数を指定します。
ステップ 5	**end** 例： `Router(bfd-config)# end`	BFD コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

マルチホップ テンプレートの設定

BFD マルチホップ テンプレートを作成し、BFD インターバル タイマー、認証、キー チェーンを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **bfd-templatemulti-hop***template-name*
4. **intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value*
5. **authentication***authentication-type***keychain***keychain-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfd-templatemulti-hop***template-name* 例： `Router(config)# bfd-template multi-hop mh-template1`	BFD マルチホップ BFD テンプレートを作成し、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 4	**intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value* 例： `Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3`	BFD パケット間での送受信間隔を設定し、ピアが使用不能であると BFD が宣言する前に損失される連続的な BFD 制御パケット数を指定します。
ステップ 5	**authentication***authentication-type***keychain***keychain-name* 例： `Router(bfd-config)# authentication keyed-sha-1 keychain bfd-multihop`	マルチホップ テンプレートの認証を設定し、認証タイプを指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(bfd-config)# end`	BFD コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

作成した BFD テンプレートは、疑似回線に適用し、ATM 疑似回線ネットワークで BFD Control Channel over VCCV をイネーブルにできます。詳細については、「ATM 疑似回線の BFD Control Channel over VCCV サポートの設定」の項を参照してください。

BFD マップの設定

テンプレートに設定されたインターバルタイマーと認証を、マルチホップ BFD セッションの一意の送信元と宛先のアドレス ペアに関連付ける BFD マップを設定するには、次の作業を実行します。

はじめる前に

マップと関連付ける前に、BFD マルチホップ テンプレートを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **bfdmapipv4vrf***vrf-namedestinationlengthsource-addresslengthtemplate-name*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバルコンフィギュレーション モードを開始します。
ステップ 3	**bfdmapipv4vrf***vrf-namedestinationlengthsource-addresslengthtemplate-name* 例： `Router(config)# bfd map ipv4 vrf vpn1 192.168.0.0/24 192.168.42.5/32 mh-template1`	BFD マップを設定し、それをテンプレートに関連付けます。
ステップ 4	**end** 例： `Router(config)# end`	BFD コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ATM 疑似回線の BFD Control Channel over VCCV サポートの設定

ATM 疑似回線ネットワークの BFD over VCCV サポートを設定するには、次の作業を実行します。

はじめる前に

BFD テンプレートは、疑似回線クラスに割り当てる前に、作成し、設定する必要があります。詳細については、「BFD テンプレートの作成と設定」の項を参照してください。

疑似回線で VCCV BFD を実行できるようにするには、疑似回線がネットワーク上に設定されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **pseudowire-class***name*
4. **encapsulation***type*
5. **protocol** {**ldp** | **none**}
6. **vccv** {**control-word** | **router-alert** | **ttl**}
7. **vccvbfdtemplate***name* {**udp** | **raw-bfd**}
8. **vccvbfdstatussignaling**
9. **exit**
10. **interfaceatm***interface-number*
11. **atmasynchronous**
12. **pvcvpi/***vci***l2transport**
13. **xconnect***peer-ip-addressvc-id* {**encapsulationmpls** [**manual**] | **pw-class***pw-class-name*} [**pw-class***pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**pseudowire-class***name* 例： `Router(config)# pseudowire-class vccv-bfd1`	疑似回線クラスの名前を指定し、疑似回線クラスコンフィギュレーション モードを開始します。
ステップ 4	**encapsulation***type* 例： `Router(config-pw-class)# encapsulation mpls`	疑似回線を経由したレイヤ2トラフィックのトンネリングに MPLS がデータ カプセル化方式として使用されることを指定します。

	コマンドまたはアクション	目的
		• AToM 仮想回線を **xconnect** コマンドの一部または疑似回線クラスの一部として適切に動作するように、mpls encapsulation を指定する必要があります。
ステップ 5	**protocol** {**ldp** | **none**} 例： `Router(config-pw-class)# protocol none`	シグナリングは設定されず、手動で設定されたセッションが使用されるように、指定します。 • スタティック疑似回線を設定するには、**none** キーワードを指定します。
ステップ 6	**vccv** {**control-word** | **router-alert** | **ttl**} 例： `Router(config-pw-class)# vccv control-word`	MPLS 疑似回線 CC タイプを設定します。 • IP/UDP ヘッダーが含まれない CV タイプが使用される MPLS 疑似回線では、CC タイプを CC タイプ 1 疑似回線コントロール ワードに設定する必要があります。
ステップ 7	**vccvbfdtemplate***name* {**udp** | **raw-bfd**} 例： `Router(config-pw-class)# vccv bfd template bfdtemplate1 raw-bfd`	疑似回線クラスの VCCV BFD をイネーブルにします。
ステップ 8	**vccvbfdstatussignaling** 例： `Router(config-pw-class)# vccv bfd status signaling`	BFD VCCV のステータス シグナリングをイネーブルにします。
ステップ 9	**exit** 例： `Router(config-pw-class)# exit`	疑似回線 クラス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interfaceatm***interface-number* 例： `Router(config)# interface atm 9/0/0`	ATM インターフェイスを設定し、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 11	**atmasynchronous** 例： `Router(config-if)# atm asynchronous`	ATM インターフェイスで非同期モードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 12	**pvcvpi/*vci*l2transport** 例： `Router(config-if)# pvc 0/100 l2transport`	ATM 相手先固定接続（PVC）を作成し、ATM PVC にカプセル化タイプを指定し、ATM仮想回線コンフィギュレーション モードを開始します。
ステップ 13	**xconnect***peer-ip-addressvc-id* {**encapsulationmpls** [**manual**] | **pw-class***pw-class-name*} [**pw-class***pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] 例： `Router(cfg-if-atm-l2trans-pvc)# xconnect 10.0.0.7 100 pw-class vccv-bfd1`	接続回線を疑似回線にバインドし、AToM スタティック疑似回線を設定し、疑似回線クラスを指定します。
ステップ 14	**end** 例： `Router(cfg-if-atm-l2trans-pvc)# end`	ATM 仮想回線コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

DMVPN での BFD サポートの設定

BFD 間隔は、次のようにトンネル インターフェイスで直接設定できます。

```
enable
configure terminal
interface tunnel1
bfd interval 1000 min_rx 1000 multiplier 5
no echo
```

次に示すように、テンプレートを定義してトンネルインターフェイスに適用することで、BFD間隔を設定することもできます

```
enable
configure terminal
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 5
interface tunnel1
bfd template sample
```

BFD のモニタリングとトラブルシューティング

ここでは、維持とトラブルシューティングのために BFD 情報を取得する方法について説明します。必要に応じてこれらのタスクのコマンドを、正しい順序で入力します。

BFD セッションの開始と障害の詳細については、BFD の動作, （9 ページ）を参照してください。

ここでは、次の Cisco プラットフォームに対する BFD のモニタリングとトラブルシューティングについて説明します。

Cisco 7600 シリーズ ルータの BFD のモニタリングとトラブルシューティング

Cisco 7600 シリーズ ルータの BFD のモニタリングとトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

（注） Cisco 7600 シリーズ ルータの BFD のトラブルシューティングの詳細については、『*Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*』の「Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card」の項を参照してください。

手順の概要

1. **enable**
2. **showbfdneighbors**[**details**]
3. **debugbfd**[**packet** | **event**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。

	コマンドまたはアクション	目的
		（注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** コマンドの出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 3	**debugbfd**[**packet** | **event**] 例： `Router# debug bfd packet`	（任意）BFD パケットのデバッグ情報を表示します。

Cisco 10720 インターネット ルータの BFD のモニタリングとトラブルシューティング

Cisco 10720 シリーズ インターネット ルータの BFD のモニタリングとトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

手順の概要

1. **enable**
2. **showbfdneighbors**[**details**]
3. **debugbfdevent**
4. **debugbfdpacket**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	（任意）BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。 （注） ラインカードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** の出力に表示されません。
ステップ 3	**debugbfdevent** 例： `Router# debug bfd event`	（任意）BFD 状態遷移のデバッグ情報を表示します。
ステップ 4	**debugbfdpacket** 例： `Router# debug bfd packet`	（任意）BFD 制御パケットのデバッグ情報を表示します。

Cisco 12000 シリーズ ルータの BFD のモニタリングとトラブルシューティング

Cisco 12000 シリーズ ルータの BFD のモニタリングとトラブルシューティングを実行するには、この項の 1 つ以上の手順に従います。

手順の概要

1. **enable**
2. **attach***slot-number*
3. **showbfdneighbors**[**details**]
4. **showmonitorevent-tracebfd** [**all**]
5. **debugbfdevent**
6. **debugbfdpacket**
7. **debugbfdipc-error**
8. **debugbfdipc-event**
9. **debugbfdoir-error**
10. **debugbfdoir-event**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**attach***slot-number* 例： `Router# attach 6`	特定のラインカードでモニタリングとメンテナンスのコマンドを実行するため、そのラインカードに接続します。Cisco 12012 のスロット番号の範囲は 0〜11 で、Cisco 12008 のスロット番号の範囲は 0〜7 です。 • スロット番号を省略した場合は、スロット番号の入力を求めるプロンプトが表示されます。 （注） Cisco 12000 シリーズ ルータで **showbfdneighborsdetails** コマンドの全出力を表示するには、ライン カードでコマンドを入力する必要があります。**attach***slot-number* コマンドを実行して、ライン カードとの CLI セッションを確立します。
ステップ 3	**showbfdneighbors**[**details**] 例： `Router# show bfd neighbors details`	BFD 隣接関係データベースを表示します。 • **details** キーワードを指定すると、すべての BFD プロトコル パラメータとネイバーごとにタイマーが表示されます。 （注） ライン カードで入力すると、登録されたプロトコルが **showbfdneighborsdetails** の出力に表示されません。 （注） ハードウェア オフロードされた BFD セッションが、50 ms の倍数でない Tx および Rx 間隔で設定されると、ハードウェア間隔が変更されます。ただし、**showbfdneighborsdetails** コマンドの出力には、変更された間隔ではなく、設定された間隔が表示されます。
ステップ 4	**showmonitorevent-tracebfd** [**all**] 例： `Router# show monitor event-trace bfd all`	ラインカードで発生した「直前の」BFD アクティビティの重要なイベントに関して、記録されたメッセージを表示します。これはローリング バッファ ベースのログで、「最古の」イベントが失われます。トラフィックおよびイベントの頻度によっては、これらのイベントを可変時間ウィンドウに表示できないことがあります。
ステップ 5	**debugbfdevent** 例： `Router# debug bfd event`	BFD 状態遷移のデバッグ情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**debugbfdpacket** 例： `Router# debug bfd packet`	BFD 制御パケットのデバッグ情報を表示します。
ステップ 7	**debugbfdipc-error** 例： `Router# debug bfd ipc-error`	RP および LC でのデバッグ情報と IPC エラーを表示します。
ステップ 8	**debugbfdipc-event** 例： `Router# debug bfd ipc-event`	RP および LC でのデバッグ情報と IPC イベントを表示します。
ステップ 9	**debugbfdoir-error** 例： `Router# debug bfd oir-error`	RP および LC でのデバッグ情報と OIR エラーを表示します。
ステップ 10	**debugbfdoir-event** 例： `Router# debug bfd oir-event`	RP および LC でのデバッグ情報と OIR イベントを表示します。

双方向フォワーディング検出の設定例

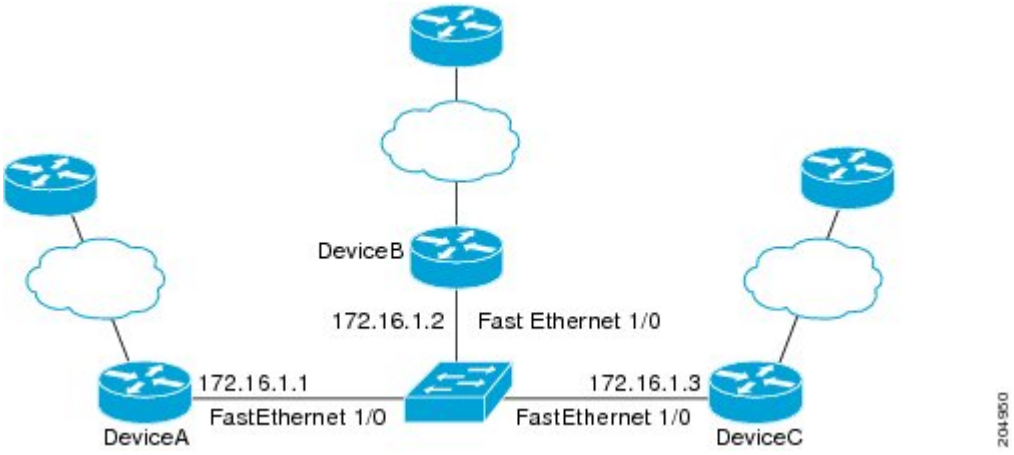
例：エコー モードがデフォルトでイネーブルになった EIGRP ネットワークでの BFD の設定

次の例では、EIGRP ネットワークにルータ A、ルータ B、およびルータ C が含まれています。ルータ A のファスト イーサネット インターフェイス 1/0 がルータ B のファスト イーサネット インターフェイス 1/0 と同じネットワークに接続されています。ルータ B のファスト イーサネット 1/0 がルータ C のファスト イーサネット インターフェイス 1/0 と同じネットワークに接続されています。

ルータ A とルータ B がエコー モードをサポートした BFD バージョン 1 を実行し、ルータ C はエコー モードをサポートしていない BFD バージョン 0 を実行しています。エコー モードはルータ

A とルータ B の転送パスで動作するため、ルータ C とその BFD ネイバーの間の BFD セッションは非対称のエコー モードで実行されます。BFD セッションおよび障害検出のため、エコーパケットは同じパスで返されます。また、BFD ネイバー ルータ C は BFD バージョン 0 を実行し、BFD セッションおよび障害検出のために BFD 制御パケットを使用します。

下の図に、複数のルータがある大規模な EIGRP ネットワークを示します。その中の 3 台は、ルーティング プロトコルとして EIGRP を実行している BFD ネイバーです。



この例は、グローバル コンフィギュレーション モードから開始し、BFD の設定を示します。

ルータ A の設定

```
interface Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.14 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no shutdown
 duplex auto
 speed auto
!
router eigrp 11
 network 172.16.0.0
 bfd all-interfaces
 auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
 exec-timeout 30 0
 stopbits 1
line aux 0
```

```
 stopbits 1
line vty 0 4
 login
!
!
end
```

ルータ B の設定

```
!
interface Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no shtdown
 duplex auto
 speed auto
!
router eigrp 11
 network 172.16.0.0
 bfd all-interfaces
 auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
 exec-timeout 30 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

ルータ C の設定

```
!
!
interface Fast Ethernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface Fast Ethernet1/0
 ip address 172.16.1.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 no shutdown
 duplex auto
 speed auto
!
router eigrp 11
 network 172.16.0.0
```

```
 bfd all-interfaces
 auto-summary
!
ip default-gateway 10.4.9.1
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 10.4.9.1
ip route 172.16.1.129 255.255.255.255 10.4.9.1
!
no ip http server
!
logging alarm informational
!
control-plane
!
line con 0
 exec-timeout 30 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

ルータ A からの **show bfd neighbors details** コマンドの出力で、3 台すべてのルータで BFD セッションが作成され、EIGRP が BFD サポートに対して登録されることを確認できます。出力の最初のグループは、IP アドレスが 172.16.1.3 のルータ C が BFD バージョン 0 を実行しているため、エコー モードを使用しないことを示します。 出力の 2 番目のグループは、IP アドレスが 172.16.1.2 のルータ B が BFD バージョン 1 を実行していて、50 ミリ秒の BFD interval パラメータが使用されていることを示します。この出力では、対応するコマンド出力が太字で表示されています。

```
RouterA# show bfd neighbors details

OurAddr
       NeighAddr
      LD/RD  RH/RS    Holdown(mult)  State     Int
172.16.1.1    172.16.1.3
     5/3    1(RH)    150 (3 )       Up   Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(1364284)
Rx Count: 1351813, Rx Interval (ms) min/max/avg: 28/64/49 last: 4 ms ago
Tx Count: 1364289, Tx Interval (ms) min/max/avg: 40/68/49 last: 32 ms ago
Registered protocols: EIGRP
Uptime: 18:42:45
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 3          - Your Discr.: 5
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.2

    6/1    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(317)
Rx Count: 305, Rx Interval (ms) min/max/avg: 1/1016/887 last: 448 ms ago
Tx Count: 319, Tx Interval (ms) min/max/avg: 1/1008/880 last: 532 ms ago
```

```
Registered protocols: EIGRP
Uptime: 00:04:30
Last packet: Version: 1

         - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 1          - Your Discr.: 6
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

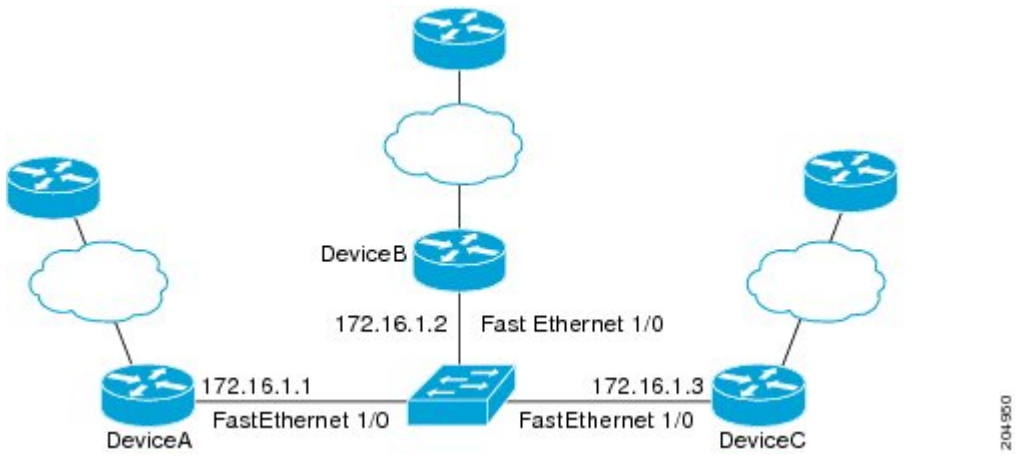
ルータ B の **showbfdneighborsdetails** コマンドによる出力で、BFD セッションが作成され、EIGRP が BFD サポートに対して登録されていることを確認できます。前述のように、ルータ A は BFD バージョン 1 を実行するため、エコー モードを実行しており、ルータ C は BFD バージョン 0 を実行するため、エコー モードを実行しません。この出力では、対応するコマンド出力が太字で表示されています。

```
RouterB# show bfd neighbors details

OurAddr       NeighAddr
     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.1
    1/6    Up        0    (3 )   Up        Fa1/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1
           - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
OurAddr       NeighAddr

 LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.3
     3/6    1(RH)     118  (3 )   Up        Fa1/0
Session state is UP and not using echo function.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 150(0), Hello (hits): 50(5735)
Rx Count: 5731, Rx Interval (ms) min/max/avg: 32/72/49 last: 32 ms ago
Tx Count: 5740, Tx Interval (ms) min/max/avg: 40/64/50 last: 44 ms ago
Registered protocols: EIGRP
Uptime: 00:04:45
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 3
             Min tx interval: 50000    - Min rx interval: 50000
             Min Echo interval: 0
```

下の図は、ルータ B のファスト イーサネット インターフェイス 1/0 に障害が発生したことを示しています。ルータ B でファスト イーサネット インターフェイス 1/0 をシャット ダウンした場合、ルータ A とルータ B の対応する BFD セッションの BFD 統計情報が少なくなります。



ルータ B のファスト イーサネット インターフェイス 1/0 に障害が発生すると、BFD はルータ A またはルータ C の BFD ネイバーとしてルータ B を検出しなくなります。この例では、ルータ B でファスト イーサネット インターフェイス 1/0 が管理的にシャット ダウンされています。

ルータ A での **showbfdneighbors** コマンドによる次の出力では、EIGRP ネットワークのルータ A の唯一の BFD ネイバーが表示されます。この出力では、対応するコマンド出力が太字で表示されています。

```
RouterA# show bfd neighbors
OurAddr       NeighAddr

    LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.1    172.16.1.3

    5/3    1(RH)     134  (3 )   Up        Fa1/0
```

ルータ C での **showbfdneighbors** コマンドによる次の出力では、EIGRP ネットワークのルータ C の唯一の BFD ネイバーが表示されます。この出力では、対応するコマンド出力が太字で表示されています。

```
RouterC# show bfd neighbors

OurAddr       NeighAddr

   LD/RD RH  Holdown(mult)  State     Int
172.16.1.3    172.16.1.1

    3/5  1   114  (3 )      Up        Fa1/0
```

例：OSPF ネットワークでの BFD の設定

次の例では、ルータ A とルータ B でシンプルな OSPF ネットワークが構成されています。ルータ A のファスト イーサネット インターフェイス 0/1 はルータ B のファスト イーサネット インターフェイス 6/0 と同じネットワークに接続されています。グローバル コンフィギュレーション モードで始まるこの例には、BFD の設定が示されています。ルータ A と B に対して、OSPF プロセスに関連付けられたすべてのインターフェイスで、BFD がグローバルに設定されます。

ルータ A の設定

```
!
interface Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
router ospf 123
 log-adjacency-changes detail
 network 172.16.0.0 0.0.0.255 area 0
 network 172.17.0.0 0.0.0.255 area 0
 bfd all-interfaces
```

ルータ B の設定

```
!
interface Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router ospf 123
 log-adjacency-changes detail
 network 172.16.0.0 0.0.255.255 area 0
 network 172.18.0.0 0.0.255.255 area 0
 bfd all-interfaces
```

show bfd neighbors details コマンドによる出力で、BFD セッションが作成され、BFD サポートに対して OSPF が登録されることを確認できます。この出力では、対応するコマンド出力が太字で表示されています。

ルータ A

```
RouterA# show bfd neighbors details
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/2  1   532  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: OSPF

Uptime: 02:18:49
Last packet: Version: 0
            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 2          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

ルータ B のライン カードからの **showbfdneighborsdetails** コマンドの出力で、BFD セッションが作成されたことを確認できます。

ルータ B

```
RouterB# attach 6
```

```
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

showipospf コマンドの出力で、BFD が OSPF に対してイネーブルになっていることを確認できます。この出力では、対応するコマンド出力が太字で表示されています。

ルータ A

```
RouterA# show ip ospf

 Routing Process "ospf 123" with ID 172.16.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
 BFD is enabled

    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 00:00:08.828 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x028417
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

ルータ B

```
RouterB# show ip ospf

 Routing Process "ospf 123" with ID 172.18.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 BFD is enabled

    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 02:07:30.932 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x28417
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show ip ospf interface コマンドの出力で、ルータ A とルータ B を接続しているインターフェイスで OSPF に対して BFD がイネーブルになっていることを確認できます。この出力では、対応するコマンド出力が太字で表示されています。

ルータ A

```
RouterA# show ip ospf interface Fast Ethernet 0/1
show ip ospf interface Fast Ethernet 0/1
Fast Ethernet0/1 is up, line protocol is up
  Internet Address 172.16.10.1/24, Area 0
  Process ID 123, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
  Designated Router (ID) 172.18.0.1, Interface address 172.16.10.2
  Backup Designated router (ID) 172.16.10.1, Interface address 172.16.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.18.0.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

ルータ B

```
RouterB# show ip ospf interface Fast Ethernet 6/1
Fast Ethernet6/1 is up, line protocol is up
  Internet Address 172.18.0.1/24, Area 0
  Process ID 123, Router ID 172.18.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
  Designated Router (ID) 172.18.0.1, Interface address 172.18.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

例：BGP ネットワークでの BFD の設定

次の例では、ルータ A とルータ B でシンプルな BGP ネットワークが構成されています。ルータ A のファスト イーサネット インターフェイス 0/1 はルータ B のファスト イーサネット インターフェイス 6/0 と同じネットワークに接続されています。グローバル コンフィギュレーション モードで始まるこの例には、BFD の設定が示されています。

ルータ A の設定

```
!
interface Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
!
router bgp 40000
 bgp log-neighbor-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
 !
 address-family ipv4
 neighbor 172.16.10.2 activate
 no auto-summary
 no synchronization
 network 172.18.0.0 mask 255.255.255.0
 exit-address-family
!
```

ルータ B の設定

```
!
interface Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router bgp 45000
```

```
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 40000
 neighbor 172.16.10.1 fall-over bfd
 !
 address-family ipv4
 neighbor 172.16.10.1 activate
 no auto-summary
 no synchronization
 network 172.17.0.0 mask 255.255.255.0
 exit-address-family
!
```

ルータ A からの **show bfd neighbors details** コマンドの出力では、BFD セッションが作成されていて、BGP が BFD サポートに登録されていることを確認できます。この出力では、対応するコマンド出力が太字で表示されています。

ルータ A

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   332  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(15491)
Rx Count: 9160, Rx Interval (ms) min/max/avg: 200/440/332 last: 268 ms ago
Tx Count: 15494, Tx Interval (ms) min/max/avg: 152/248/197 last: 32 ms ago
Registered protocols: BGP
Uptime: 00:50:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

ルータ B のライン カードからの **showbfdneighborsdetails** コマンドの出力で、BFD セッションが作成されたことを確認できます。

ルータ B

```
RouterB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
```

```
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

showipbgpneighbors コマンドの出力で、BFD が BGP ネイバーに対してイネーブルになっていることを確認できます。

ルータ A

```
RouterA# show ip bgp neighbors
BGP neighbor is 172.16.10.2,  remote AS 45000, external link
 Using BFD to detect fast fallover
.
.
.
```

ルータ B

```
RouterB# show ip bgp neighbors
BGP neighbor is 172.16.10.1,  remote AS 40000, external link
 Using BFD to detect fast fallover
.
.
.
```

例：IS-IS ネットワークでの BFD の設定

次の例では、ルータ A とルータ B でシンプルな IS-IS ネットワークが構成されています。ルータ A のファスト イーサネット インターフェイス 0/1 はルータ B のファスト イーサネット インターフェイス 6/0 と同じネットワークに接続されています。グローバル コンフィギュレーション モードで始まるこの例には、BFD の設定が示されています。

ルータ A の設定

```
!
interface Fast Ethernet 0/1
 ip address 172.16.10.1 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 3/0.1
ip address 172.17.0.1 255.255.255.0
ip router isis
!
router isis
 net 49.0001.1720.1600.1001.00
 bfd all-interfaces
!
```

ルータ B の設定

```
!
interface Fast Ethernet 6/0
 ip address 172.16.10.2 255.255.255.0
ip router isis
 bfd interval 50 min_rx 50 multiplier 3
!
interface Fast Ethernet 6/1
 ip address 172.18.0.1 255.255.255.0
```

```
ip router isis
!
router isis
 net 49.0000.0000.0002.00
 bfd all-interfaces
!
```

ルータ A からの **show bfd neighbors details** コマンドの出力では、BFD セッションが作成されていて、IS-IS が BFD サポートに登録されていることを確認できます。

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   536  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(23543)
Rx Count: 13877, Rx Interval (ms) min/max/avg: 200/448/335 last: 64 ms ago
Tx Count: 23546, Tx Interval (ms) min/max/avg: 152/248/196 last: 32 ms ago
Registered protocols: ISIS
Uptime: 01:17:09
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

ルータ B のライン カードからの **showbfdneighborsdetails** コマンドの出力で、BFD セッションが作成されたことを確認できます。

```
RouterB# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
Router> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

例：HSRP ネットワークでの BFD の設定

次の例では、ルータ A とルータ B で HSRP ネットワークが構成されています。ルータ A のファスト イーサネット インターフェイス 2/0 はルータ B のファスト イーサネット インターフェイス 2/0

と同じネットワークに接続されています。グローバルコンフィギュレーションモードで始まるこの例には、BFD の設定が示されています。

（注） 次の例では、**standbybfd** コマンドと **standbybfdall-interfaces** コマンドが表示されません。デフォルトでは BFD ピアリングの HSRP サポートがイネーブルになっていて、BFD は **bfdinterval** コマンドを使用してルータまたはインターフェイスで設定されます。**standbybfd** コマンドと **standbybfdall-interfaces** コマンドは、BFD がルータまたはインターフェイスで手動で無効にされている場合にのみ必要です。

ルータ A

```
ip cef
interface Fast Ethernet2/0
 no shutdown
 ip address 10.0.0.2 255.0.0.0
 ip router-cache cef
 bfd interval 200 min_rx 200 multiplier 3
 standby 1 ip 10.0.0.11
 standby 1 preempt
 standby 1 priority 110

 standby 2 ip 10.0.0.12
 standby 2 preempt
 standby 2 priority 110
```

ルータ B

```
interface Fast Ethernet2/0
 ip address 10.1.0.22 255.255.0.0
 no shutdown
 bfd interval 200 min_rx 200 multiplier 3
 standby 1 ip 10.0.0.11
 standby 1 preempt
 standby 1 priority 90
 standby 2 ip 10.0.0.12
 standby 2 preempt
 standby 2 priority 80
```

show standby neighbors コマンドの出力で、BFD セッションが作成されたことを確認できます。

```
RouterA#show standby neighbors

HSRP neighbors on Fast Ethernet2/0
  10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
RouterB# show standby neighbors

HSRP neighbors on Fast Ethernet2/0
  10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

例：スタティック ルーティングに対する BFD サポートの設定

次の例では、ネットワークはデバイス A とデバイス B で構成されています。デバイス A のシリアル インターフェイス 2/0 は、デバイス B のシリアル インターフェイス 2/0 と同じネットワークに接続されています。BFD セッションを起動するには、デバイス B を設定する必要があります。

デバイス A

```
configure terminal
interface Serial 2/0
ip address 10.201.201.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.2
ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2
```

デバイス B

```
configure terminal
interface Serial 2/0
ip address 10.201.201.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 5
ip route static bfd Serial 2/0 10.201.201.1
ip route 10.1.1.1 255.255.255.255 Serial 2/0 10.201.201.1
```

デバイス B のスタティック ルートが単独で存在していて、10.201.201.1 と 10.201.201.2 の間で BFD セッションをイネーブルにすることに注意してください。設定する必要のある有益なスタティック ルートがない場合、パケットの転送に影響しないプレフィックス、たとえば、ローカルで設定されたループバック インターフェイスを選択します。

次の例では、BFD グループ testgroup のイーサネット インターフェイス 0/0 を介して 209.165.200.225 に到達するアクティブなスタティック BFD 設定があります。設定されたスタティック BFD によってトラッキングされるスタティック ルートが設定されるとすぐに、単一のホップ BFD セッションがイーサネット インターフェイス 0/0 を介して 209.165.200.225 に開始されます。BFD セッションが正常に確立されると、プレフィックス 10.0.0.0/8 が RIB に追加されます。

```
configure terminal
ip route static bfd Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
```

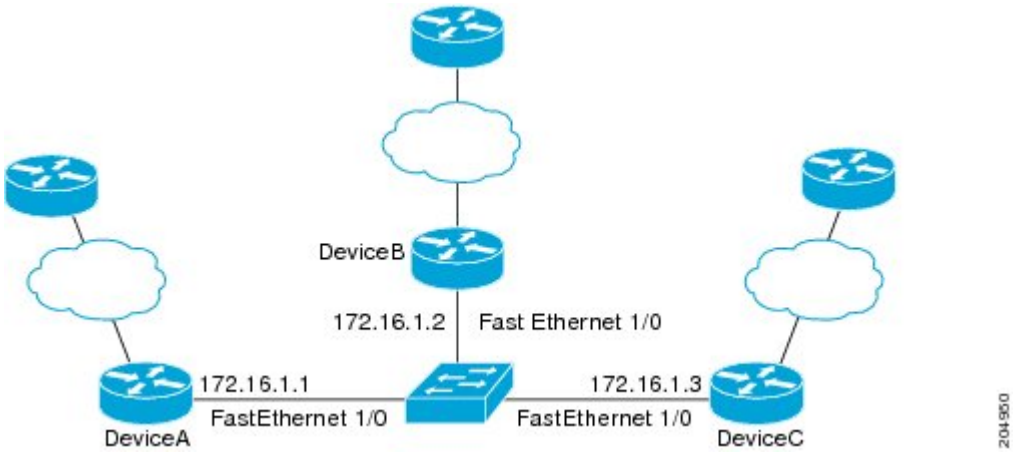
次の例では、イーサネット インターフェイス 0/0.1001 を介した 209.165.200.226 への BFD セッションがグループ testgroup を使用するようにマークされます。つまり、この設定はパッシブなスタティック BFD です。2 つ目のスタティック BFD 設定によってトラッキングされるスタティック ルートがあるものの、209.165.200.226 に対する BFD セッションはイーサネット インターフェイス 0/0.1001 を介しては開始されません。プレフィックス 10.1.1.1/8 と 10.2.2.2/8 の存在は、アクティブなスタティック BFD セッション（イーサネット インターフェイス 0/0 209.165.200.225）によって制御されます。

```
configure terminal
ip route static bfd Ethernet 0/0 209.165.200.225 group testgroup
ip route 10.0.0.0 255.255.255.224 Ethernet 0/0 209.165.200.225
ip route static bfd Ethernet 0/0.1001 209.165.200.226 group testgroup passive
ip route 10.1.1.1 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
ip route 10.2.2.2 255.255.255.224 Ethernet 0/0.1001 209.165.200.226
```

例：BFD Control Channel over VCCV：ATM 疑似回線サポートの設定

下の図に、通常の ATM 疑似回線の設定を示します。ネットワークは、2 つの Terminating Provider Edge（T-PE）デバイスの T-PE1 と T-PE2 との間の ATM ペイロードに含まれる MPLS 疑似回線で構成されます。疑似回線の BFD のモニタリングは、T-PE1 デバイスと Switching Providing Edge（S-PE）デバイスとの間、および、S-PE デバイスと T-PE2 デバイスとの間で、発生します。BFD では、カスタマー エッジ（CE）デバイスと T-PE デバイスとの間の AC の信号ステータスがモニタされます。

（注） S-PE には BFD Control Channel over VCCV に固有の設定は必要ありません。



CE1

```
interface ATM 0/0
 description connect to mfi6 atm9/0/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM 0/0.2 point-to-point
 ip address 10.25.1.1 255.255.255.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 0/100
  encapsulation aal5snap
```

T-PE1

```
interface Loopback 0
 ip address 10.0.0.6 255.255.255.255
bfd-template single-hop nsn
 interval min-tx 500 min-rx 500 multiplier 3
pseudowire-class vccv-bfd1
```

```
 encapsulation mpls
 vccv bfd template nsn raw-bfd
 vccv bfd status signaling
interface ATM 9/0/0
 description connect mfr4 atm0/0
 no ip address
 atm asynchronous
 atm clock INTERNAL
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 pvc 0/100 l2transport
  xconnect 10.0.0.7 100 pw-class vccv-bfd1
```

T-PE2

```
interface Loopback 0
 ip address 10.54.0.1 255.255.255.255
bfd-template single-hop nsn
 interval min-tx 500 min-rx 500 multiplier 3
!
pseudowire-class vccv-bfd1
 encapsulation mpls
 vccv bfd template nsn raw-bfd
 vccv bfd status signaling
interface ATM 2/0
 no ip address
 atm asynchronous
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 pvc 0/100 l2transport
  xconnect 10.0.0.7 102 pw-class vccv-bfd1
 !
```

CE2

```
interface ATM 4/0.2 point-to-point
 ip address 10.25.1.2 255.255.255.0
 no snmp trap link-status
 pvc 0/100
  encapsulation aal5snap
```

例：DMVPN での BFD サポート

例：DMVPN での BFD サポート

次に、ハブで DMVPN での BFD サポートを設定する例を示します。

```
bfd-template single-hop sample
 interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp network-id 5
 ip nhrp redirect
 ip mtu 1400
 ip tcp adjust-mss 1360
 bfd template sample
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
!
```

```
interface GigabitEthernet0/0/0
 ip address 10.0.0.1 255.0.0.0
 negotiation auto
!
router eigrp 2
network 10.0.0.0 0.0.0.255
bfd all-interfaces
auto-summary
!
```

次に、スポークで DMVPN での BFD サポートを設定する例を示します。

```
bfd-template single-hop sample
 interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel1
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp network-id 5
 ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
 bfd template sample
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
!
interface GigabitEthernet0/0/0
 mtu 4000
 ip address 11.0.0.1 255.0.0.0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/0/1
 mtu 6000
 ip address 111.0.0.1 255.255.255.0
 negotiation auto
!
router eigrp 2
 network 11.0.0.0 0.0.0.255
 network 111.0.0.0 0.0.0.255
 network 10.0.0.0 0.0.0.255
bfd all-interfaces
auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

次に、スポークでのコンバージェンスを高速化する例を示します。

```
interface Tunnel1
ip address 18.0.0.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp network-id 12
ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
bfd template sample
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 18
tunnel protection ipsec profile MY_PROFILE
!
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 3
echo
!
router eigrp 2
bfd interface Tunnel1    ------------------------> Specify the interface on which the routing
 protocol must act for BFD up/down events
network 11.0.0.0 0.0.0.255
```

```
network 111.0.0.0 0.0.0.255
```

上記の設定を使用すると、BFD のダウンがレポートされた直後に（3 秒で検出）、EIGRP は RIB からインストールされたルートを削除します。

次の出力例は、ハブのサマリー出力を示しています。

```
device#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 172.17.0.1             10.0.0.1    UP 00:00:14     D
     1 172.17.0.2             10.0.0.2   BFD 00:00:03     D
```

BFD が新しい状態であるということは、セッションは下位レイヤ（IKE、IPSec、および NHRP）で認識されるように UP 状態ですが、BFD がセッションを DOWN と認識したことを意味します。通常どおり、この状態はセッションが UP 状態ではない最下位レイヤを示しています。また、これは親キャッシュ エントリにのみ適用されます。この原因としては、BFD によって DOWN と検出されたこと、または BFD が反対側で設定されていないことが考えられます。

次の出力例は、スポークのサマリー出力を示しています。

```
device#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2 172.17.0.2             10.0.0.2   BFD 00:00:02   DT1
                              10.0.0.2    UP 00:00:02   DT2
     1 172.17.0.11           10.0.0.11    UP 00:05:35     S
```

次の例は、**show ip/ipv6 nhrp** コマンドの出力を示しています。

```
device#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel2 created 00:00:15, expire 00:04:54
   Type: dynamic, Flags: router nhop rib bfd
   NBMA address: 172.17.0.2
10.0.0.11/32 via 10.0.0.11
   Tunnel2 created 00:09:04, never expire
   Type: static, Flags: used bfd
   NBMA address: 172.17.0.11
```

```
192.168.1.0/24 via 10.0.0.1
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.0.1
    (no-socket)
192.168.2.0/24 via 10.0.0.2
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router rib nho
   NBMA address: 172.17.0.2
```

上記の例の BFD フラグは、このピアに BFD セッションがあることを意味しています。このマーキングは親エントリ専用です。

次の例は、**show tunnel endpoints** コマンドの出力を示しています。

```
device#show tunnel endpoints
 Tunnel2 running in multi-GRE/IP mode

 Endpoint transport 172.17.0.2 Refcount 3 Base 0x2ABF53ED09F0 Create Time 00:00:07
   overlay 10.0.0.2 Refcount 2 Parent 0x2ABF53ED09F0 Create Time 00:00:07
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 2 entries; BFD(0x2):U
 Endpoint transport 172.17.0.11 Refcount 3 Base 0x2ABF53ED0B80 Create Time 00:09:07
   overlay 10.0.0.11 Refcount 2 Parent 0x2ABF53ED0B80 Create Time 00:09:07
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries; BFD(0x1):U
```

すべてのトンネル エンドポイントに対して、新しいテキスト「**BFD(handle):state**」が追加されます。状態は UP（U）、DOWN（D）、NONE（N）、または INVALID（I）のいずれかです。

- BFD がピアに設定されていない場合、または最初にセッションが UP ではない場合は、状態が N になります。

次の例は、**show nhrp interfaces** コマンドの出力を示しています。インターフェイス上の設定状態またはグローバルな設定状態が示されます（動作状態ではありません）。

```
device#show nhrp interfaces
NHRP Config State
-----------------
 Global:
    BFD: Registered

 Tunnel1:
    BFD: Disabled

 Tunnel2:
    BFD: Enabled
```

これは内部の隠しコマンドです。現在は、NHRP が BFD のクライアントであるかどうか、および BFD が NHRP インターフェイスでイネーブルになっているかどうかが表示されます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
BGP の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Cisco BGP Overview」の章
BFDハードウェア オフロード	『*Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*』の「Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card」の項
EIGRP の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring EIGRP」の章
HSRP の設定とモニタリング	『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring HSRP」の章
IS-IS の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring Integrated IS-IS」の章
OSPF の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring OSPF」の章
BFD コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
BGP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
EIGRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
HSRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』

関連項目	マニュアル タイトル
IS-IS コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
OSPF コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
BFD IPv6 カプセル化サポート	「*BFD IPv6 Encapsulation Support*」の章
OSPFv3 for BFD	「*OSPFv3 for BFD*」の章
IPv6 での BFD に対するスタティック ルート サポート	「*IPv6 での BFD に対するスタティック ルート サポート*」の章

標準および RFC

標準/RFC	タイトル
IETF ドラフト	*Bidirectional Forwarding Detection*、2009 年 2 月（http://tools.ietf.org/html/draft-ietf-bfd-base-09）
IETF ドラフト	*BFD for IPv4 and IPv6 (Single Hop)*、2009 年 2 月（http://tools.ietf.org/html/draft-ietf-bfd-v4v6-1hop-09）

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

双方向フォワーディング検出に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：双方向フォワーディング検出に関する機能情報

機能名	リリース	機能情報
BFD Control Channel over VCCV：ATM疑似回線のサポート	15.0(1)S	VCCV では、ATM 疑似回線に関連付けられている制御チャネルが提供され、疑似回線を介して操作と管理機能が提供されます。BFD では、VCCV 制御チャネルを使用して、疑似回線のデータプレーンの障害が検出されます。 Cisco IOS Release 15.0(1)S では、VCCV タイプ 1（IP/UDP ヘッダーなし）のみで、BFD Control Channel over VCCV の ATM 疑似回線のサポート機能がサポートされます。 **bfd-template**、**debugmplsl2transportvcvccv**、**interval**（BFD）、**vccv**、**vccvbfdtemplate**、**vccvbfdstatussignaling** のコマンドが導入または変更されました。

機能名	リリース	機能情報
BFD エコー モード	12.2(33)SRB 12.4(9)T 15.0(1)S	BFD エコー モードは非同期 BFD で動作します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために、同じパスで転送されます。反対側の BFD セッションはエコー パケットの実際のフォワーディングに関与しません。エコー機能およびフォワーディング エンジンが検出プロセスを処理するため、2 つの BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディング エンジンが、リモート システムを介さずにリモート（ネイバー）システムの転送パスをテストするため、パケット内遅延が向上する可能性があり、それによって BFD バージョン 0 を BFD セッションの BFD 制御パケットを使用する場合に、障害検出時間を短縮できます。
BFD：BFD ハードウェア オフロードのサポート	15.1(2)S 15.1(1)SG	この機能では、Cisco 7600 シリーズ ルータで ES+ ラインカードへの BFD セッションのオフロードがサポートされています。**showbfdneighbors** コマンドが導入または変更されました。
BFD IPv6 カプセル化サポート	Cisco IOS XE Release 3.11S	この機能により、BFD の IPv6 サポートが拡張されます。 **bfd interval** コマンドが導入または変更されました。

機能名	リリース	機能情報
BFD マルチホップ	15.1(3)S 15.4(1)S	この機能では、IPv4 および IPv6 アドレスのマルチホップ BFD がサポートされます。 Cisco IOS Release 15.4(1)S では、Cisco ASR 901S シリーズルータのサポートが追加されました。 **authentication**、**bfd map**、**bfd-template**、**interval**、**show bfd neighbors**、**show bfd neighbor drops** のコマンドが導入または変更されました。

機能名	リリース	機能情報
BFD：スタティック ルートのサポート	12.2(33)SRC 15.0(1)M 15.0(1)S 15.0(1)SY 15.1(2)S 15.1(1)SG 15.4(1)S	OSPF や BGP などの動的なルーティング プロトコルとは異なり、スタティック ルーティングにはピア検出の方法がありません。したがって、BFD が設定されると、ゲートウェイの到達可能性は完全に指定されたネイバーへの BFD セッションの状態に依存します。BFD セッションが開始されない限り、スタティックルートのゲートウェイは到達不能と見なされ、したがって、影響を受けるルートが適切なRIBにインストールされません。 IPv4 スタティック クライアントでは 1 つの BFD セッションを使用して、特定のインターフェイスを通るネクスト ホップの到達可能性を追跡できます。一連の BFD 追跡対象スタティック ルートに対して BFD グループを割り当てることができます。 Cisco IOS Release 15.4(1)S では、Cisco ASR 901S シリーズルータのサポートが追加されました。 **iproutestaticbfd** と **showipstaticroutebfd** のコマンドが導入または変更されました。
IP トンネルの BFD サポート（GRE、IP アドレス使用）	15.1(1)SY	この機能では、ポイントツーポイント IPv4、IPv6、および GRE トンネルでの BFD 転送をサポートします。 **bfd** コマンドが導入または変更されました。

機能名	リリース	機能情報
ポート チャネルでの BFD サポート	15.1(1)SY 15.1(2)SY	この機能では、ポート チャネル インターフェイスでの BFD タイマーの設定がサポートされます。 **bfd** コマンドが導入または変更されました。
BFD：VRF サポート	12.2(33)SRC 15.0(1)M 15.0(1)S 15.1(1)SY	BFD 機能のサポートが、プロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイス間のルーティング プロトコル障害の高速検出を提供するように、VPN ルーティングおよび転送（VRF）対応に拡張されています。
BFD：WAN インターフェイス サポート	12.2(33)SRC 15.0(1)M 15.0(1)S	BFD 機能がブロードキャスト メディア以外のインターフェイス（ATM、POS、シリアル、および VLAN インターフェイスなど）でサポートされます。BFD のサポートは ATM、FR、POS、およびシリアル サブインターフェイスに拡張されます。 **bfd interval** コマンドは、BFD モニタリングを開始するインターフェイスで設定する必要があります。

機能名	リリース	機能情報
双方向フォワーディング検出（標準実装、バージョン 1）	12.0(31)S 12.0(32)S 12.2(33)SRB 12.2(33)SRC 12.2(18)SXE 12.2(33)SXH 12.4(9)T 12.4(11)T 12.4(15)T 15.0(1)S 15.4(1)S	このマニュアルでは、双方向フォワーディング検出（BFD）プロトコルをイネーブルにする方法について説明します。BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者は BFD を使用して、さまざまなルーティングプロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。 Release 12.0(31)S では、Cisco 12000 シリーズのインターネット ルータのサポートが追加されました。 Release 12.0(32)S では、Cisco 10720 インターネット ルータ、および、Cisco 12000 シリーズ インターネット ルータの IP サービス エンジン（エンジン 3）、エンジン 5 共有ポート アダプタ（SPA）、SPA インターフェイス プロセッサ（SIP）のサポートが追加されました。 Cisco IOS Release 15.4(1)S では、Cisco ASR 901S シリーズ ルータのサポートが追加されました。

機能名	リリース	機能情報
BFD に対する HSRP サポート	12.2(33)SRC 12.4(11)T 12.4(15)T	Release 12.4(11)T では、HSRP のサポートが追加されました。 Release 12.4(15)T では、BFD が Cisco ルータの Integrated Services Router（ISR）ファミリ、たとえば Cisco 3800 ISR シリーズ ルータでサポートされます。 Release 12.2(33)SRC では、作成できる BFD セッションの数が増加し、BFD サポートが ATM、FR、POS、およびシリアル サブインターフェイスに拡張されました。BFD 機能は VRF 対応に拡張されました。計画されたスイッチオーバー時に BFD セッションが「Admin Down」状態になります。BFD サポートがスタティック ルーティングに拡張されました。
IPv4 での BFD に対する IS-IS サポート	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.4(1)S	すべてのインターフェイスでグローバルに OSPF に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。BFD で登録されたプロトコルとして IS-IS で BFD サポートが設定される場合、IS-IS が BFD から転送パスの検出障害メッセージを受信します。 Cisco IOS Release 15.4(1)S では、Cisco ASR 901S シリーズ ルータのサポートが追加されました。

機能名	リリース	機能情報
IPv4 での BFD に対する OSPF サポート	12.0(31)S 12.2(18)SXE 12.2(33)SRA 12.4(4)T 15.0(1)S 15.1(1)SG	すべてのインターフェイスでグローバルにOSPFに対するBFDを設定するか、または1つ以上のインターフェイスで選択的に設定することができます。BFDで登録されたプロトコルとしてOSPFでBFDサポートが設定される場合、OSPFがBFDから転送パスの検出障害メッセージを受信します。
SSO：BFD	12.2(33)SRE 12.2(33)SXI2 12.2(33)XNE 15.0(1)S 15.1(1)SG	デュアル RP ルータおよびスイッチを使用するネットワーク導入には、スイッチオーバー全体でフォワーディング状態を保護するためのグレースフル リスタート メカニズムがあります。この機能によって、BFD はスイッチオーバー全体でセッションを稼働状態に保つことができます。
SSO：BFD（Admin Down）	12.2(33)SRC 15.0(1)S	SSOをサポートするために、計画されたスイッチオーバー時にBFD セッションが「Admin Down」状態になります。BFD 設定はアクティブなプロセッサからスタンバイ プロセッサに同期化され、すべての BFD クライアントがスタンバイ プロセッサでの BFD プロセスで再登録されます。

機能名	リリース	機能情報
Cisco ISR G2 モジュラ ルータの IPbasek9 イメージでの BFD サポート。	15.6(3)M	Cisco IOS Release 15.6(3)M からは、Cisco ISR G2 モジュラ ルータの ipbasek9 イメージでも BFD がサポートされます。たとえば、EIGRP 機能が ipbasek9 イメージの一部である場合は、EIGRP の BFD 機能も ipbasek9 イメージの一部です。ある機能が、BFD をサポートする IP Base 以外のソフトウェア パッケージの一部である場合は、関連する BFD 機能は同等のソフトウェア パッケージの一部です。

第 3 章

IPv6 での BFD に対するスタティック ルート サポート

- 機能情報の確認，87 ページ
- IPv6 での BFD に対するスタティック ルート サポートに関する情報，87 ページ
- IPv6 の双方向フォワーディング検出の設定方法，89 ページ
- IPv6 での BFD に対するスタティック ルート サポートの設定例，91 ページ
- その他の参考資料，91 ページ
- IPv6 での BFD に対するスタティック ルート サポートに関する機能情報，92 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 での BFD に対するスタティック ルート サポートに関する情報

スタティック ルート ネクスト ホップに到達するために BFDv6 プロトコルを使用すると、ネクスト ホップ ネイバーが到達可能なとき、IPv6 スタティック ルートは IPv6 ルーティング情報ベース

（RIB）にだけ挿入されることが保証されます。また、BFDv6 プロトコルを使用すると、ネクスト ホップが到達不能になったとき、IPv6 スタティック ルートを IPv6 RIB から削除することもできます。

ユーザは、IPv6 スタティック BFDv6 ネイバーを設定できます。これらのネイバーは、associated（デフォルト）モードと unassociated モードのいずれかで動作できます。ネイバーは、自身が関連している BFDv6 セッションを中断させずに、これら 2 つのモードの間を遷移できます。

BFDv6 associated モード

IPv6 の双方向フォワーディング検出（BFDv6）の associated モードでは、スタティック ルート ネクスト ホップがスタティック BFDv6 ネイバーと完全に一致すれば、IPv6 スタティック ルートが IPv6 スタティック BFDv6 ネイバーと自動的に関連付けられます。

IPv6 スタティック ルートは、1 つ以上の IPv6 スタティック ルートが関連付けられているスタティック BFDv6 ネイバーごとに BFDv6 セッションを要求し、BFD が設定されているインターフェイス上で設定されます。BFDv6 セッションの状態は、関連付けられた IPv6 スタティック ルートを IPv6 RIB に挿入するかどうかを決定するために使用されます。たとえば、スタティック ルートは、BFDv6 ネイバーが到達可能な場合にだけ、IPv6 RIB に挿入されます。またその後に、BFDv6 ネイバーが到達不能になると、そのスタティック ルートは IPv6 RIB から削除されます。

BFDv6 associated モードでは、BFD モニタ対象スタティック ルートを必要とするデバイスと隣接デバイスの両方で、BFD ネイバーとスタティック ルートを設定する必要があります。

BFDv6 unassociated モード

IPv6 スタティック BFD ネイバーは、unassociated として設定できます。このモードでは、ネイバーはスタティック ルートと関連付けられません。また、インターフェイスが BFDv6 用に設定されていると、ネイバーは常に BFDv6 セッションを要求します。

unassociated モードは、次の状況で役に立ちます。

- IPv6 スタティック ルートがない状態での BFDv6 セッションの構築：これは、スタティック ルートがルータ A 上にあり、ルータ B がネクスト ホップのときに起こります。associated モードでは、B から A への BFDv6 セッションを発生させるために、両方のルータにスタティック BFD ネイバーとスタティック ルートを作成する必要があります。ルータ B 上で unassociated モードでスタティック BFD ネイバーを指定すると、不要なスタティック ルートを設定せずに済みます。
- スタティック ルートの BFD モニタリングへの移行：これは、既存の IPv6 スタティック ルートが IPv6 RIB に挿入されているときに起こります。ここで、トラフィックを中断させずに、これらのスタティック ルートの BFD モニタリングを有効にする場合を考えます。接続されている IPv6 スタティック BFD ネイバーを設定すると、スタティック ルートは、新しいスタティック BFD ネイバーに即座に関連付けられます。しかし、スタティック BFD ネイバーはダウン状態で始まるため、関連付けられたスタティック ルートは IPv6 RIB から一旦削除され、BFDv6 セッションが確立されたときに再挿入されます。したがって、トラフィックの中断を経験することになります。この中断は、スタティック BFD ネイバーを unassociated とし

て設定し、BFDv6セッションが確立するまで待機して、確立後にスタティックBFDネイバーを associated として再設定することで回避できます。

- スタティック ルートの BFD モニタリングからの移行：この場合、IPv6 スタティック ルートは、BFDによってモニタされ、RIBに挿入されています。ここで、トラフィック フローを中断させずに、スタティック ルートの BFD モニタリングを無効にする場合を考えます。このシナリオは、最初にスタティックBFDネイバーを非接続として再設定し（つまり、スタティック ルートからネイバーの関連付けを解除）、その後にスタティック BFD ネイバーの設定を解除することで実現できます。

IPv6 の双方向フォワーディング検出の設定方法

スタティック BFDv6 ネイバーの指定

IPv6 スタティック BFDv6 ネイバーは、IPv6 スタティック ルートとは別に指定されます。IPv6 スタティック BFDv6 ネイバーは、インターフェイスとネイバーアドレスで完全に設定される必要があり、ローカル ルータに直接接続されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6routestaticbfd** [**vrf***vrf-name*] *interface-typeinterface-numberipv6-address* [**unassociated**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6routestaticbfd** [**vrf***vrf-name*] *interface-typeinterface-numberipv6-address* [**unassociated**]	スタティック ルート IPv6 BFDv6 ネイバーを指定します。

	コマンドまたはアクション	目的
	例： `Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1`	

BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け

IPv6 スタティック ルートは、スタティック BFDv6 ネイバーと自動的に関連付けされます。スタティック ネイバーは、スタティック ネクストホップが BFDv6 ネイバーと明確に一致すると、その BFDv6 ネイバーと関連付けられます。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6routestaticbfd** [**vrf***vrf-name*] *interface-typeinterface-numberipv6-address* [**unassociated**]
4. **ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-numberipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6routestaticbfd** [**vrf***vrf-name*] *interface-typeinterface-numberipv6-address* [**unassociated**] 例： `Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1`	スタティック ルート BFDv6 ネイバーを指定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-numberipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*] 例： `Device(config)# ipv6 route 2001:DB8::/64 gigabitethernet 0/0/0 2001::1`	スタティック IPv6 ルートを確立します。

IPv6 での BFD に対するスタティック ルート サポートの設定例

例：IPv6 スタティック BFDv6 ネイバーの指定

次に、完全に設定された IPv6 スタティック BFDv6 ネイバーを指定する例を示します。インターフェイスは GigabitEthernet 0/0/0、ネイバー アドレスは 2001::1 です。

```
Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1
```

例：BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け

この例では、IPv6 スタティック ルート 2001:DB8::/32 が GigabitEthernet 0/0/0 インターフェイス上の BFDv6 ネイバー 2001::1 と関連付けられます。

```
Device(config)# ipv6 route static bfd gigabitethernet 0/0/0 2001::1
Device(config)# ipv6 route 2001:DB8::/32 gigabitethernet 0/0/0 2001::1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』
IPv6 での BFD に対するスタティック ルート サポート	「双方向フォワーディング検出」の章

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	IPv6 の RFC

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 での BFD に対するスタティック ルート サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 2：***IPv6 での BFD に対するスタティック ルート サポートに関する機能情報***

機能名	リリース	機能情報
IPv6 での BFD に対するスタティック ルート サポート	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.6S	スタティック ルート ネクスト ホップに到達するために BFDv6 プロトコルを使用すると、ネクスト ホップ ネイバーが到達可能なとき、IPv6 スタティック ルートは IPv6 ルーティング情報ベース（RIB）にだけ挿入されることが保証されます。また、BFDv6 プロトコルを使用すると、ネクスト ホップが到達不能になったとき、IPv6 スタティック ルートを IPv6 RIB から削除することもできます。 Cisco IOS XE Release 3.6S では、Cisco ASR 903 ルータのサポートが追加されました。 **debug bfd**、**debug ipv6 static**、**ipv6 static**、**ipv6 route static bfd**、**monitor event ipv6 static**、**show ipv6 static** のコマンドが導入または変更されました。

第 4 章

OSPFv3 for BFD

双方向フォワーディング検出プロトコルでは OSPFv3 がサポートされます。

- 機能情報の確認，95 ページ
- OSPFv3 for BFD に関する情報，95 ページ
- OSPFv3 for BFD の設定方法，96 ページ
- OSPFv3 for BFD の設定例，102 ページ
- その他の参考資料，102 ページ
- OSPFv3 for BFD に関する機能情報，104 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

OSPFv3 for BFD に関する情報

双方向フォワーディング検出（BFD）プロトコルでは、Open Shortest Path First バージョン 3（OSPFv3）がサポートされます。

OSPFv3 for BFD の設定方法

OSPFv3 に対する BFD サポートの設定

ここでは、OSPFv3 が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、OSPFv3 に対する BFD サポートを設定する手順について説明します。すべてのインターフェイスでグローバルに OSPFv3 に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。

OSPFv3 に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfdall-interfaces** コマンドを使用して、OSPFv3 がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ipv6ospfbfddisable** コマンドを使用して、個々のインターフェイスで BFD サポートをディセーブルにできます。
- インターフェイス コンフィギュレーション モードで **ipv6ospfbfd** コマンドを使用して、OSPFv3 がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

（注） OSPF は、FULL ステートの OSPF ネイバーに対する BFD セッションを開始するだけです。

インターフェイスの基本 BFD セッション パラメータの設定

BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、次の作業を繰り返します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイスコンフィギュレーションモードにします。
ステップ 4	**bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier* 例： `Device(config-if)# bfd interval 50 min_rx 50 multiplier 5`	インターフェイスでBFDをイネーブルにします。

すべてのインターフェイスの OSPFv3 に対する BFD サポートの設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションをBFDネイバーに対して実行するインターフェイスで、BFDセッションの基本パラメータを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipv6routerospf***process-id*[**vrf***vpn-name*]
4. **bfdall-interfaces**
5. **exit**
6. **showbfdneighbors** [**vrf***vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6***ipv6-address*] [**details**]
7. **showipv6ospf** [*process-id*] [*area-id*] [**rate-limit**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6routerospf***process-id*[**vrf***vpn-name*] 例： `Device(config)# ipv6 router ospf 2`	OSPFv3 ルーティング プロセスを設定します。
ステップ 4	**bfdall-interfaces** 例： `Device(config-router)# bfd all-interfaces`	ルーティングプロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 5	**exit** 例： `Device(config-router)# exit`	このコマンドを 2 回入力して、特権 EXEC モードにします。
ステップ 6	**showbfdneighbors** [**vrf***vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6***ipv6-address*] [**details**]	（任意）既存の BFD 隣接関係の行単位のリストを表示します。

	コマンドまたはアクション	目的
	例： `Device# show bfd neighbors detail`	
ステップ 7	**showipv6ospf** [*process-id*] [*area-id*] [**rate-limit**] 例： `Device# show ipv6 ospf`	（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。

1 つ以上の OSPFv3 インターフェイスの OSPFv3 に対する BFDv6 サポートの設定

はじめる前に

OSPFv3 は、参加しているすべてのデバイスで実行されている必要があります。BFD セッションをBFDネイバーに対して実行するインターフェイスで、BFDセッションの基本パラメータを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipv6ospfbfd**[**disable**]
5. **exit**
6. **showbfdneighbors** [**vrf***vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address*| **ipv6***ipv6-address*] [**details**]
7. **showipv6ospf** [*process-id*] [*area-id*] [**rate-limit**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6ospfbfd**[**disable**] 例： `Device(config-if)# ipv6 ospf bfd`	OSPFv3 ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。
ステップ 5	**exit** 例： `Device(config-router)# exit`	このコマンドを 2 回入力して、特権 EXEC モードにします。
ステップ 6	**showbfdneighbors** [**vrf***vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address*| **ipv6***ipv6-address*] [**details**] 例： `Device# show bfd neighbors detail`	（任意）既存の BFD 隣接関係の行単位のリストを表示します。
ステップ 7	**showipv6ospf** [*process-id*] [*area-id*] [**rate-limit**] 例： `Device# show ipv6 ospf`	（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。

モニタリングおよびトラブルシューティングのための BFDv6 情報の取得

手順の概要

1. **enable**
2. **monitoreventipv6static** [**enable** | **disable**]
3. **showipv6static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface***typenumber* | **recursive**] [**vrf***vrf-name*] [**bfd**] [**detail**
4. **showipv6static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface***typenumber* | **recursive**] [**vrf***vrf-name*] [**bfd**] [**detail**]
5. **debugipv6static**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitoreventipv6static** [**enable** | **disable**] 例： `Device# monitor event ipv6 static enable`	イベント トレースの使用をイネーブルにして、IPv6 スタティック ネイバーと IPv6 スタティック BFDv6 ネイバーの動作をモニタします。
ステップ 3	**showipv6static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface***typenumber* | **recursive**] [**vrf***vrf-name*] [**bfd**] [**detail** 例： `Device# show ipv6 static vrf vrf1 detail`	スタティック BFDv6 ネイバーに関連付けられたスタティック ルートの BFDv6 ステータスを表示します。
ステップ 4	**showipv6static** [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface***typenumber* | **recursive**] [**vrf***vrf-name*] [**bfd**] [**detail**] 例： `Device# show ipv6 static vrf vrf1 bfd`	スタティック BFDv6 ネイバーおよび関連付けられたスタティック ルートを表示します。

	コマンドまたはアクション	目的
ステップ 5	**debugipv6static** 例： `Device# debug ipv6 static`	BFDv6 デバッグをイネーブルにします。

OSPFv3 for BFD の設定例

例：BFD に関する OSPF インターフェイス情報の表示

次の表示例は、OSPF インターフェイスが BFD に対してイネーブルになっていることを示しています。

```
Device# show ipv6 ospf interface

Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』
OSPFv3 for BFD	「双方向フォワーディング検出」の章

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	IPv6 の RFC

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

OSPFv3 for BFD に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3*：***OSPFv3 for BFD*** に関する機能情報

機能名	リリース	機能情報
OSPFv3 for BFD	Cisco IOS XE Release 2.1	BFD では、ダイナミック ルーティング プロトコル OSPFv3 がサポートされています。 **bfd**、**bfd all-interfaces**、**debug bfd**、**ipv6 router ospf**、**show bfd neighbors**、**show ipv6 ospf**、**show ipv6 ospf interface**、**show ospfv3**、**show ospfv3 interface** のコマンドが導入または変更されました。

第 5 章

BDI インターフェイスでの BFD

BDIインターフェイスでのシスコのBFD機能は、スイッチド仮想インターフェイス（SVI）によるシステムあたりのインターフェイス最大数の制限を緩和します。このマニュアルでは、ブリッジドメインインターフェイス（BDI）で双方向フォワーディング検出（BFD）プロトコルを設定する方法について説明します。

- 機能情報の確認，105 ページ
- ブリッジ ドメイン インターフェイスの BFD に関する情報，106 ページ
- BDI インターフェイスの BFD の設定方法，106 ページ
- BDI インターフェイスの BFD の設定例，110 ページ
- その他の参考資料，111 ページ
- ブリッジ ドメイン インターフェイスの BFD に関する機能情報，113 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ブリッジ ドメイン インターフェイスの BFD に関する情報

ブリッジ ドメイン インターフェイスの BFD

各 BDI は、関連するイーサネット フロー ポイント（EFP）で定義され、設定された基準を使用してトラフィックがマップされているブリッジ ドメインに関連付けられます。単一または複数の EFP を特定のブリッジ ドメインに関連付けることができます。そのため、グローバル テーブルまたは VPN ルーティングおよび転送（VRF）テーブルのいずれかで定義された BDI インターフェイス上で BFD シングルホップ セッションを確立でき、既存のすべてのシングルホップ BFD クライアントが BDI 経由の BFD でサポートされます。

BDI でのシスコの BFD 機能は、SSO 対応のプラットフォームでの BFD ステートフル スイッチオーバー（SSO）には影響しません。

BDI インターフェイスの BFD の設定方法

ブリッジ ドメイン インターフェイス上での BFD のイネーブル化

個々の BDI インターフェイス上でシングルホップ BFD をイネーブルにするには、次の手順を実行します。

（注） マルチホップ BFD はインターフェイス固有ではないため、マルチホップ BFD セッションを確立するために BDI インターフェイス レベルの設定は必要ありません。

はじめる前に

2 つ以上のノードが接続されている必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Router(config)# interface bdi 100`	ブリッジドメインインターフェイスを設定し、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 4	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.201.201.1 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 5	**bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier* 例： `Router(config-if)# bfd interval 500 min_rx 500 multiplier 5`	インターフェイスで BFD をイネーブルにします。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ブリッジ ドメインとイーサネット フロー ポイントの関連付け

はじめる前に

両方のノードで BFD をイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***type slot/subslot/port*
4. **no ip address**
5. **negotiation auto**
6. **cdp enable**
7. **service instance***id service-type*
8. **encapsulation dot1q***vlan-id*
9. **rewrite ingress tag pop 1 symmetric**
10. **exit**
11. **exit**
12. **bridge-domain***vlan-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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***type slot/subslot/port* 例： `Router(config)# interface GigabitEthernet0/0/3`	インターフェイス タイプを設定し、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 4	**no ip address** 例： `Router(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Router(config-if)# negotiation auto`	インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーションプロトコルで設定できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**cdp enable** 例： `Router(config-if)# cdp enable`	インターフェイスで Cisco Discovery Protocol をイネーブルにします。
ステップ 7	**service instance***id service-type* 例： `Router(config-if)# service instance 2 ethernet`	イーサネットサービスインスタンスを設定し、サービスインスタン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 8	**encapsulation dot1q***vlan-id* 例： `Router(config-if-srv)# encapsulation dot1q 2`	サブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 9	**rewrite ingress tag pop 1 symmetric** 例： `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	サービスインスタンス入力側のフレームからの一番外側のタグの削除と出力方向のタグの追加を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	サービス インスタンス コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 11	**exit** 例： `Router(config-if)# exit`	インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 12	**bridge-domain***vlan-id* 例： `Router(config)# bridge-domain 2`	イーサネット フロー ポイントとブリッジ ドメインを関連付けます。

例：

次の作業

BDI インターフェイスの BFD の設定例

BDI インターフェイスの BFD の例

次に、BDI で BFD を設定する例を示します。

```
Router#show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.1.1.2                             2049/1          Up        Up        BD2
Router#
Router#show running interface gi0/0/3
Building configuration...

Current configuration : 230 bytes
!
interface GigabitEthernet0/0/3
no ip address
ip pim passive
ip igmp version 3
negotiation auto
cdp enable
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
!
end

Router#show running interface bdi2

Building configuration...

Current configuration : 127 bytes
!
interface BDI2
ip address 10.1.1.3 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.2
end
```

同様に、もう一方のノードの例を示します。

```
Router2#show running interface bdi2

Building configuration...

Current configuration : 127 bytes
!
interface BDI2
ip address 10.1.1.2 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3
bfd neighbor ipv4 10.1.1.3
end
```

```
ED3#show run int gig0/0/3
Building configuration...

Current configuration : 195 bytes
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
cdp enable
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
!
end

Router2#show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.1.1.3                                1/2049       Up        Up        BD2
ED3#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
BGP の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Cisco BGP Overview」の章
BFDハードウェア オフロード	『*Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide*』の「Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card」の項
EIGRP の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring EIGRP」の章
HSRP の設定とモニタリング	『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring HSRP」の章
IS-IS の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring Integrated IS-IS」の章
OSPF の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring OSPF」の章

関連項目	マニュアル タイトル
BFD コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
BGP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
EIGRP コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
HSRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』
IS-IS コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
OSPF コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
BFD IPv6 カプセル化サポート	「*BFD IPv6 Encapsulation Support*」の章
OSPFv3 for BFD	「*OSPFv3 for BFD*」の章
IPv6 での BFD に対するスタティック ルート サポート	「*IPv6 での BFD に対するスタティック ルート サポート*」の章

標準および RFC

標準/RFC	タイトル
IETF ドラフト	*Bidirectional Forwarding Detection*、2009 年 2 月（http://tools.ietf.org/html/draft-ietf-bfd-base-09）
IETF ドラフト	*BFD for IPv4 and IPv6 (Single Hop)*、2009 年 2 月（http://tools.ietf.org/html/draft-ietf-bfd-v4v6-1hop-09）

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ブリッジ ドメイン インターフェイスの BFD に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：ブリッジ ドメイン インターフェイスの *BFD* に関する機能情報

機能名	リリース	機能情報
ブリッジ ドメイン インターフェイスの BFD	Cisco IOS XE Release 3.5S	この機能では、ブリッジ ドメイン インターフェイスの BFD がサポートされます。

第 6 章

BFD シングルホップ認証

BFD シングルホップ認証機能では、直接接続された 2 台のデバイス間のシングルホップ双方向フォワーディング検出（BFD）セッションの認証をイネーブルにします。この機能では、Message Digest 5（MD5）とセキュア ハッシュ アルゴリズム 1（SHA-1）認証タイプをサポートします。

この章では、BFD シングルホップ認証機能について説明します。

- 機能情報の確認，115 ページ
- BFD シングルホップ認証の前提条件，116 ページ
- BFD シングルホップ認証の制限事項，116 ページ
- BFD シングルホップ認証に関する情報，116 ページ
- BFD シングルホップ認証の設定方法，117 ページ
- BFD シングルホップ認証の設定例，121 ページ
- その他の参考資料，123 ページ
- BFD シングルホップ認証に関する機能情報，123 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BFD シングルホップ認証の前提条件

BFDセッションに関与する両方の接続デバイスのキーおよびキーチェーンを設定する必要があります。設定が一致するように、両方のデバイスのアルゴリズムとキー チェーンを設定する必要があります。

BFD シングルホップ認証の制限事項

- 確立した BFD シングルホップ セッションからキー チェーンが削除されたり、アクティブなキーがキー チェーン内に存在しない場合は、BFD テンプレートとマップ エントリが無効になります。このような無効化はマップ エントリの削除と見なされます。
- シーケンス番号のチェックポイントがすべてのパケットで行われるわけではないため、緻密性の高いキーによるMD5認証と緻密性の高いキーによるSHA-1は、In-Service Software Upgrade（ISSU）ではサポートされていません。
- 緻密性の高い MD5 と緻密性の高い SHA-1 の認証タイプは、ステートフル スイッチオーバー（SSO）モードでルートプロセッサ（RP）に障害が発生した後は保存されません。セッションがフラップし、登録されたプロトコルのリンクが不安定になる可能性があります。
- 50 ミリ秒以上のタイマー値だけがサポートされます。
- 2 つの BFD ピア間の認証タイプ ネゴシエーションとキー交換は行われません。
- 不明なキーチェーンがある場合、またはキーチェーン内にキーが設定されていない場合は、BFD テンプレートとその関連マップ エントリが無効になり、BFD セッションは作成されません。
- 双方向フォワーディング検出（BFD）のシングルホップ認証を適用できるのは、BFDテンプレートの設定だけです。従来の構成では BFD シングルホップ認証を適用できません。

BFD シングルホップ認証に関する情報

BFD シングルホップ認証の利点

RFC 5880 で定義されている Message Digest 5（MD5）とセキュア ハッシュ アルゴリズム 1（SHA-1）の認証方式を使用して、BFD シングルホップ認証機能では、BFD セッションに関与する直接接続されたデバイスペア間のデータ リンク上での攻撃に対するセキュリティを提供します。この機能は、着信インターフェイスに関連付けられたシングル IP ホップで IPv4 および IPv6 プロトコルを使用して通信する BFD の送信元と宛先のペア間のデータ リンクに適用されます。この通信は物理メディア、仮想回線、およびトンネルを経由して発生することがあります。

サービス妨害（DoS）攻撃を防ぐ際の BFD シングルホップ認証の役割

サービス妨害（DoS）攻撃を防ぐために、BFD シングルホップ セッションではパケット受信時にパケットのシーケンス番号が確認されます。検出係数は、ローカル デバイスが転送パスの障害を検出するまでに喪失した、別の BFD デバイスからの BFD Hello メッセージの数です。検出係数は検出タイマーを決定するために使用します。BFD シングルホップ認証機能で許容される有効なシーケンス番号の範囲は次のとおりです。

- 緻密性の低いキー タイプの場合：最後に受信したシーケンス番号から（最後に受信したシーケンス番号 + 3 * 検出係数）
- 緻密性の高いキー タイプの場合：（最後に受信したシーケンス番号 + 1）から（最後に受信したシーケンス番号 + 3 * 検出係数）

（注） BFD の場合は、（伝送間隔）*（検出係数）= 検出タイマーになります。BFD 制御パケットが detect-timer 間隔内にリモート システムから受信されない場合、障害が発生しています。

BFD シングルホップ認証の設定方法

キー チェーンの設定

BFD セッションに関与する 2 台のデバイスの一方でこの作業を実行し、もう一方のデバイスで手順を繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *chain-name*
4. **key** *key-id*
5. **key-string** *text*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *chain-name* 例： `Device(config)# key chain chain1`	ルーティング プロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン 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	**key** *key-id* 例： `Device(config-keychain)# key 1`	キーチェーンの認証キーを定義し、キーチェーン キー コンフィギュレーション モードを開始します。
ステップ 5	**key-string** *text* 例： `Device(config-keychain-key)# key-string key1`	キーの認証文字列を定義します。
ステップ 6	**end** 例： `Device(config-keychain-key)# end`	キーチェーン キー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

認証を使用した BFD テンプレートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **bfd-templatesingle-hop***template-name*
4. **intervalmin-tx** *milliseconds***min-rx***milliseconds* **multiplier***multiplier-value*
5. **authentication** *authentication-type* **keychain** *keychain-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfd-templatesingle-hop***template-name* 例： `Device(config)# bfd-template single-hop template1`	BFD テンプレートを作成し、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 4	**intervalmin-tx** *milliseconds***min-rx***milliseconds* **multiplier***multiplier-value* 例： `Device(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3`	BFD パケット間での送受信間隔を設定し、ピアが使用不能であると BFD が宣言する前に損失される連続的な BFD 制御パケット数を指定します。
ステップ 5	**authentication** *authentication-type* **keychain** *keychain-name* 例： `Device(config-bfd)# authentication sha-1 keychain keychain1`	BFD テンプレートでシングルホップ セッションの認証を設定します。
ステップ 6	**end** 例： `Device(config-bfd)# end`	BFD コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスでのシングルホップ テンプレートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd template** *template-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	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ます。
ステップ 4	**bfd template** *template-name* 例： `Device(config-if)# bfd template bfdtemplate`	シングルホップ BFD テンプレートをインターフェイスにバインドします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

BFD シングルホップ認証の確認

手順の概要

1. **show bfd drops**
2. **show bfd neighbor**

手順の詳細

ステップ 1 **show bfd drops**

例：

```
Device> show bfd drops
```

このコマンドでは、BFD でドロップされたパケット数が表示されます。

ステップ 2 **show bfd neighbor**

例：

```
Device> show bfd neighbor
```

このコマンドでは、既存の BFD 隣接関係の行単位のリストを表示します。

BFD シングルホップ認証の設定例

例：キー チェーンの設定

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

例：認証を使用した BFD テンプレートの設定

```
Device> enable
Device# configure terminal
Device(config)# bfd-template single-hop template1
Device(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
Device(bfd-config)# authentication sha-1 keychain keychain1
Device(bfd-config)# end
```

例：インターフェイスでのシングルホップ テンプレートの設定

```
Device> enable
Device# configure terminal
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# end
```

例：BFD シングルホップ認証の確認

show bfd neighbor コマンドの出力例

```
Device> show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.168.0.2                            1/12          Up        Up        Et0/0
Session state is UP and using echo function with 300 ms interval.
Session Host: Software
OurAddr: 192.168.0.1
Handle: 12
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 1000(62244)
Rx Count: 62284, Rx Interval (ms) min/max/avg: 1/2436/878 last: 239 ms ago
Tx Count: 62247, Tx Interval (ms) min/max/avg: 1/1545/880 last: 246 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub CEF
Template: my-template
Authentication(Type/Keychain): sha-1/my-chain
Uptime: 00:22:06
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 12               - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 300000
```

show bfd drops コマンドの出力例。

```
Device> show  bfd drops

BFD Drop Statistics
                      IPV4    IPV6    IPV4-M  IPV6-M  MPLS_PW MPLS_TP_LSP
Invalid TTL           0        0       0       0       0       0
BFD Not Configured    0        0       0       0       0       0
No BFD Adjacency      0        0       0       0       0       0
Invalid Header Bits   0        0       0       0       0       0
Invalid Discriminator 0        0       0       0       0       0
Session AdminDown     0        0       0       0       0       0
Authen invalid BFD ver 0       0       0       0       0       0
Authen invalid len    0        0       0       0       0       0
Authen invalid seq    0        0       0       0       0       0
Authen failed         0        0       0       0       0       0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
IP ルーティング：プロトコル独立型コマンド	『*Cisco IOS IP Routing Protocol-Independent Command Reference*』

標準および RFC

標準/RFC	タイトル
RFC 5880	双方向フォワーディング検出

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

BFD シングルホップ認証に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5*：*BFD* シングルホップ認証に関する機能情報

機能名	リリース	機能情報
BFD シングルホップ認証	15.2(4)S	BFD シングルホップ認証機能は、直接接続されたデバイス間のシングルホップ BFD セッションの認証をイネーブルにします。この機能は、Message Digest 5（MD5）とセキュアハッシュ アルゴリズム 1（SHA1）認証タイプをサポートします。 **authentication（BFD）**、**bfd template**、**bfd-template**、**show bfd drops**、および **show bfd neighbors** のコマンドが導入または変更されました。

第 7 章

IPv4 スタティック ルートの BFD マルチホップ サポート

IPv4 スタティック ルートの BFD マルチホップ サポート機能により、直接接続されていないパス間の IPv4 ネットワーク障害の検出が可能になります。双方向フォワーディング検出（BFD）セッションがアップ状態の場合（つまり、ネクストホップの宛先に到達可能な場合）、IPv4 スタティック BFD 設定に関連付けられている IPv4 スタティック ルートがルーティング テーブルに追加されます。BFD セッションがダウン状態の場合、ルーティング テーブルから関連付けられているすべてのスタティック ルートが削除されます。

この機能は、物理インターフェイス、サブインターフェイス、および仮想トンネルなど、さまざまな種類のインターフェイスに、エリア内およびエリア間のトポロジ全体で適用できます。

- 機能情報の確認，125 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートの前提条件，126 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートに関する情報，126 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートの設定方法，127 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートの確認，128 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートの設定例，129 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートに関する追加情報，130 ページ
- IPv4 スタティック ルートの BFD マルチホップ サポートに関する機能情報，131 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv4 スタティック ルートの BFD マルチホップ サポートの前提条件

- IPv4 スタティック ルートを設定する必要がある BFD の宛先は、すべてのデバイスが到達可能でなければなりません。
- 設定されているデバイスは、関連するセッションの BFD の宛先としてネクストホップの宛先をもつスタティック ルートが少なくとも 1 つ必要です。そのようにしないと、デバイスで BFD セッションが作成されません。

IPv4 スタティック ルートの BFD マルチホップ サポートに関する情報

BFDv4 associated モード

IPv4 の双方向フォワーディング検出（BFDv4）の associated モードでは、スタティック ルート ネクスト ホップがスタティック BFDv4 マルチホップ宛先アドレスと完全に一致すれば、IPv4 スタティック ルートが IPv4 スタティック BFDv4 マルチホップ宛先アドレスと自動的に関連付けられます。

BFDv4 セッションの状態は、関連付けられた IPv4 スタティック ルートを IPv4 ルーティング情報ベース（RIB）に追加するかどうかを決定するために使用されます。たとえば、スタティック ルートは、BFDv4 マルチホップ宛先が到達可能な場合にだけ、IPv4 RIB に追加されます。またその後に、BFDv4 マルチホップ宛先が到達不能になると、そのスタティック ルートは IPv4 RIB から削除されます。

BFDv4 unassociated モード

IPv4 の双方向フォワーディング検出（BFDv4）では、IPv4 スタティック BFD マルチホップ宛先を unassociated モードで設定できます。unassociate モードでは、BFD ネイバーはスタティック ルートに関連付けられません。また、IPv4 スタティック BFD が設定されていると、BFD セッションが要求されます。

unassociated モードは、次のような場合に役立ちます。

- IPv4 スタティック ルートがない場合：この状況は、スタティック ルートがデバイス A 上にあり、デバイス B がネクスト ホップのときに発生します。associated モードでは、両方のデバイス上でスタティック BFD マルチホップ宛先アドレスとスタティック ルートを作成し、デバイス B からデバイス A への BFDv4 セッションを発生させる必要があります。デバイス B 上で unassociated モードでスタティック BFD マルチホップ宛先を指定すると、不要なスタティック ルートを設定せずに済みます。

IPv4 スタティック ルートの BFD マルチホップ サポートの設定方法

BFD マルチホップ IPv4 スタティック ルートの設定

はじめる前に

- IPv4 スタティック ルートのネクスト ホップまたはゲートウェイ アドレスと同じである BFD 宛先アドレスを指定します。
- デバイス上でインターフェイスの BFD マップと BFD マルチホップ テンプレートを設定します。BFD マップ用に設定された宛先アドレスと送信元アドレスは、BFD スタティック マルチホップ設定に一致する必要があり、送信元アドレスがルーティング テーブルのインターフェイスに設定されている有効な IP アドレスでなければなりません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask ip-address*
4. **ip route static bfd** *multihop-destination-address multihop-source-address*
5. **ip route static bfd** *multihop-destination-address multihop-source-address* **unassociate**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip route** *prefix mask ip-address* 例： `Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2`	BFD マルチホップでスタティック ルートをモニタするために使用する IPv4 スタティック ルートを設定します。
ステップ 4	**ip route static bfd** *multihop-destination-address multihop-source-address* 例： `Device(config)# ip route static bfd 192.0.2.1 10.1.1.1`	スタティック IPv4 ルートに関連付けるスタティック IPv4 BFD マルチホップを設定します。
ステップ 5	**ip route static bfd** *multihop-destination-address multihop-source-address* **unassociate** 例： `Device(config)# ip route static bfd 192.0.2.1 10.1.1.1 unassociate`	（任意）unassociated モードでスタティック IPv4 ルートに関連付けるスタティック IPv4 BFD マルチホップを設定します。
ステップ 6	**end** 例： `Device(config)# end`	グローバルコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

IPv4 スタティック ルートの BFD マルチホップ サポートの確認

次の show コマンドは、BFD マルチホップの IPv4 スタティック ルートを確認するために使用できます。

手順の概要

1. **show bfd neighbor**
2. **show ip static route bfd**

手順の詳細

ステップ 1 **show bfd neighbor**

既存の BFD 隣接関係の詳細なリストを表示します。

ステップ 2 **show ip static route bfd**
IPv4 スタティック BFD で設定されたパラメータに関する情報を表示します。

IPv4 スタティック ルートの BFD マルチホップ サポートの設定例

例：associated モードでの IPv4 スタティック ルートの BFD マルチホップの設定

```
Device> enable
Device# configure terminal
Device(config)# bfd map ipv4 192.0.2.1/32  10.1.1.1/32 test
Device(config)# bfd-template multi-hop test
Device(config-bfd)# interval min-tx 51 min-rx 51 multiplier 3
Device(config-bfd)# exit
Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# exit
Device(config)# ip route static bfd 192.0.2.1 10.1.1.1
Device(config)# end
```

例：unassociated モードでの BFD の IPv4 スタティック マルチホップの設定

```
Device> enable
Device# configure terminal
Device(config)# bfd map ipv4 192.0.2.1/32  10.1.1.1/32 test
Device(config)# bfd-template multi-hop test
Device(config-bfd)# interval min-tx 51 min-rx 51 multiplier 3
Device(config-bfd)# exit
Device(config)# ip route 192.0.2.0 255.255.255.0 10.1.1.2
Device(config)# interface GigabitEthernet 1/1
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# exit
Device(config)# ip route static bfd 192.0.2.1 10.1.1.1 unassociate
Device(config)# end
```

IPv4 スタティック ルートの BFD マルチホップ サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP ルーティング：Protocol-Independent コマンド	『IP Routing: Protocol-Independent Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5883	『*BFD for Multihop Paths*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv4 スタティック ルートの BFD マルチホップ サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：*IPv4* スタティック ルートの *BFD* マルチホップ サポートに関する機能情報

機能名	リリース	機能情報
IPv4 スタティック ルートの BFD マルチホップ サポート	Cisco IOS XE Release 3.9S	IPv4 スタティック ルートの BFD マルチホップ サポート機能により、直接接続されていないパス間の IPv4 ネットワーク障害の検出が可能になります。双方向フォワーディング検出（BFD）セッションがアップ状態の場合（つまり、ネクストホップの宛先に到達可能な場合）、IPv4 スタティック BFD 設定に関連付けられている IPv4 スタティック ルートがルーティング テーブルに追加されます。BFD セッションがダウン状態の場合、ルーティング テーブルから関連付けられているすべてのスタティック ルートが削除されます。 **ip route static bfd** と **show ip static route bfd** のコマンドが変更されました。

第 8 章

BFD の IS-IS IPv6 クライアント

双方向フォワーディング検出（BFD）サポートが、BFDに登録されたプロトコルとしてIntermediate System to Intermediate System（IS-IS）で設定された場合、IS-IS が BFD から転送パスの検出障害メッセージを受信します。

- 機能情報の確認，133 ページ
- BFD の IS-IS IPv6 クライアントの前提条件，133 ページ
- BFD の IS-IS IPv6 クライアントに関する情報，134 ページ
- BFD の ISIS IPv6 クライアントの設定方法，135 ページ
- BFD の ISIS IPv6 クライアントの設定例，138 ページ
- その他の参考資料，138 ページ
- BFD の IS-IS IPv6 クライアントに関する機能情報，139 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BFD の IS-IS IPv6 クライアントの前提条件

- IS-IS は、関連するすべてのデバイスで実行する必要があります。

- BFD セッションの基本パラメータは BFD ネイバーに対して BFD セッションを実行するインターフェイス上で設定する必要があります。

BFD の IS-IS IPv6 クライアントに関する情報

IS-IS BFD トポロジ

BFD で登録されたプロトコルとして IS-IS で BFD サポートが設定される場合、IS-IS が BFD から転送パスの検出障害メッセージを受信します。IS-IS に対する BFD サポートは、ルータ アドレス ファミリ コンフィギュレーション 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 モードで設定できます。IS-IS IPv6 はシングルトポロジ モードまたはマルチトポロジ（MT）モードで動作可能です。

IS-IS BFD は、シングルトポロジ モードまたはマルチトポロジ モードの同じ接続関係で IPv4 と IPv6 の両方をサポートします。BFD が IPv4 と IPv6 の両方にイネーブルの場合、IS-IS は BFD に 2 つの BFD セッション作成要求を送信します。シングルトポロジモードでは、IS-IS 隣接状態は、両方の BFD セッションがアップした場合にのみ、アップ状態になります。BFD セッションのいずれかがダウンすると、関連する IS-IS 隣接状態もまたダウンします。MT モードでは、IS-IS 隣接状態は、トポロジのいずれかにアップ状態の BFD セッションがある限り、アップ状態になります。

IS-IS BFD IPv6 セッションの作成

IS-IS は、次の条件がすべて満たされると、隣接デバイスのインターフェイスと IPv6 アドレスに対する BFD セッションを要求します。

- IS-IS 隣接エントリが存在する。
- アドレス ファミリ識別子（AFI）固有のピアインターフェイスアドレスが認識されている。
- IS-IS BFD がインターフェイスでその AFI に対してイネーブルになっている。
- IS-IS がローカル インターフェイスでその AFI に対してイネーブルになっている。
- 隣接デバイスが RFC 6213 をサポートしている場合、BFD が指定されたマルチトポロジ識別子（MTID）またはネットワーク層プロトコル識別子（NLPID）に対しイネーブルになっている必要がある。

IS-IS BFD IPv6 セッションの削除

IS-IS BFD IPv6 がインターフェイスでディセーブルの場合、IS-IS は隣接デバイスから IPv6 の関連 BFD セッションを削除します。IS-IS 隣接エントリを削除すると、すべての BFD セッションも削

除されます。IS-IS は、次のいずれかのイベントが発生したときに要求した各 BFD セッションを削除するように BFD に要求します。

- IS-IS インスタンスが削除または設定解除される。
- IS-IS 隣接エントリが削除される。
- IS-IS BFD がアドレス ファミリのネクスト ホップ インターフェイスでディセーブルになる。
- 隣接デバイスが RFC 6213 をサポートし、指定された MTID または NLPID に対して BFD がサポート対象でなくなったことを示す。

BFD の ISIS IPv6 クライアントの設定方法

インターフェイスでの BFD の IS-IS IPv6 クライアント サポートの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **isisipv6bfd**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 6/0/0`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ididipv6bfd** 例： `Device(config-if)# isis ipv6 bfd`	IS-IS に設定されている特定のインターフェイスで BFD IPv6 をイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

すべてのインターフェイスでの BFD の IS-IS IPv6 クライアント サポートの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **routerisis**
4. **metric-style wide**
5. **address-familyipv6**
6. **multi-topology**
7. **bfd all-interfaces**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**routerisis** 例： `Device(config)# router isis`	IS-IS ルーティング プロトコルをイネーブルにし、ルータ 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	**metric-style wide** 例： `Device(config-router)# metric-style wide`	（任意）新しいスタイルのタイプ、長さ、値オブジェクト（TLV）のみを生成し受け入れるように、IS-IS を実行しているデバイスを設定します。
ステップ 5	**address-familyipv6** 例： `Device(config-router)# address-family ipv6`	標準の IPv6 アドレス プレフィックスを使用する IS-IS ルーティングセッションを設定するアドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**multi-topology** 例： `Device(config-router-af)# multi-topology`	（任意）IPv6 に対するマルチトポロジ IS-IS をイネーブルにします。
ステップ 7	**bfd all-interfaces** 例： `Device(config-router-af)# bfd all-interfaces`	ルーティング プロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 8	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BFD の ISIS IPv6 クライアントの設定例

例：単一インターフェイスでの BFD の IS-IS IPv6 クライアント サポート

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0/0
Device(config-if)# isis ipv6 bfd
Device(config-if)# end

Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 6/0
Device(config-if)# isis ipv6 bfd
Device(config-if)# end
```

例：すべてのインターフェイスでの BFD の IS-IS IPv6 クライアント サポート

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# metric-style wide
Device(config-router)# address-family ipv6
Device(config-router-af)# multi-topology
Device(config-router-af)# bfd all-interfaces
Device(config-router-af)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
BFD コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例。	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
IS-IS の設定とモニタリング	『*IP Routing Protocols Configuration Guide*』の「Configuring Integrated IS-IS」の章

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

BFD の IS-IS IPv6 クライアントに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：***BFD の IS-IS IPv6 クライアントに関する機能情報***

機能名	リリース	機能情報
BFD の IS-IS IPv6 クライアント	15.1(1)SY 15.2(4)S 15.3(1)T	BFD で登録されたプロトコルとして IS-IS で BFD サポートが設定される場合、IS-IS が BFD から転送パスの検出障害メッセージを受信します。 **bfd all-interfaces**、**isis ipv6 bfd** のコマンドが導入または変更されました。

第 9 章

BFD C ビットの IS-IS クライアント サポート

双方向フォワーディング検出（BFD）プロトコルでは、隣接する転送エンジン間のパスにおける障害を、ネットワーキング オーバーヘッドを低く維持しながら短期間で検出できます。双方向フォワーディング検出（BFD）の Intermediate System-to-Intermediate System（IS-IS）クライアント サポート機能では、IS-IS で BFD サポートを使用できるようになります。BFD の検出と障害の時間はほとんどのネットワーク トポロジで IS-IS コンバージェンス時間よりも速くなるため、IS-IS コンバージェンスが改善されます。BFD C ビットの IS-IS クライアント サポート機能では、BFD セッションの障害が本当であるか、ルータの再起動によるコントロール プレーン障害の結果であるかどうかをネットワークで特定することができます。ルータの再起動を計画するときは、すべての隣接ルータにこの機能を設定する必要があります。

- 機能情報の確認，141 ページ
- BFD C ビットの IS-IS クライアント サポートの前提条件，142 ページ
- BFD C ビットの IS-IS クライアント サポートに関する情報，142 ページ
- BFD C ビットの IS-IS クライアント サポートの設定方法，143 ページ
- BFD C ビットの IS-IS クライアント サポートの設定例，144 ページ
- その他の参考資料，144 ページ
- BFD C ビットの IS-IS クライアント サポートに関する機能情報，145 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BFD C ビットの IS-IS クライアント サポートの前提条件

- IS-IS は、関連するすべてのデバイスで実行する必要があります。
- BFD セッションの基本パラメータは BFD ネイバーに対して BFD セッションを実行するインターフェイス上で設定する必要があります。

BFD C ビットの IS-IS クライアント サポートに関する情報

IS-IS の再起動と BFD セッション

BFD C ビットの IS-IS クライアント サポート機能では、BFD 実装がコントロール プレーンと同じステータスを共有するかどうか、ピアに信号を送信する方法を BFD に提供します。隣接ルータのコントロール プレーンが再起動すると、BFD セッションの障害が発生することがありますが、実在の転送障害を実際に示しているわけではありません。このような場合に、再起動ルータのネイバー ルータがその BFD セッションの障害に反応することは望ましくありません。

IS-IS には、ルータが再起動する前に信号を送信できるプロトコル拡張機能がありません。これは、システムが実際の転送障害と再起動を区別できないことを意味します。BFD C ビットの IS-IS クライアント サポート機能により、コントロール プレーン関連の BFD セッションの障害を無視するようにデバイスを設定することができます。シスコは、計画的なデバイスの再起動の直前に再起動デバイスのネイバーでこの機能を設定し、再起動が完了した後に設定を削除することをお勧めします。

下の表に、セッション ダウン イベントで BFD から受信した、コントロール プレーンに依存しない障害ステータスがそのイベントの IS-IS の処理にどのように影響するかを示します。

表 *8*：コントロール プレーン障害およびセッション ダウン イベント

コントロール プレーン障害の IS-IS チェック	BFD コントロール プレーンに依存しない障害ステータス	BFD セッション「ダウン」イベント時の IS-IS 動作
イネーブル	True	セッション ダウンを受け入れ
イネーブル	False	セッション ダウンを無視
ディセーブル	True	セッション ダウンを受け入れ
ディセーブル	False	セッション ダウンを受け入れ

BFD C ビットの IS-IS クライアント サポートの設定方法

BFD C ビットの IS-IS クライアント サポートの設定

コントロール プレーン障害チェックをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **router isis**
4. **bfd check-control-plane-failure**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** 例： `Device(config)# router isis`	IS-IS ルーティング プロトコルをイネーブルにし、ルータ 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 check-control-plane-failure** 例： `Device(config-router)# bfd check-control-plane-failure`	IS-IS ルーティング プロトコルの BFD コントロール プレーン障害チェックをイネーブルにします。
ステップ 5	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

BFD C ビットの IS-IS クライアント サポートの設定例

例：BFD C ビットの IS-IS クライアント サポートの設定

次の例では、IS-IS プロトコルを実行するルータでコントロールプレーン障害検出を設定しています。

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# bfd check-ctrl-plane-failure
Device(config-router)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
BFD コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
IS-IS の設定とモニタリング	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring Integrated IS-IS」の章
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	タイトル
RFC 5882	『*Generic Application of Bidirectional Forwarding Detection (BFD)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

BFD C ビットの IS-IS クライアント サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9* : ***BFD C*** ビットの ***IS-IS*** クライアント サポートに関する機能情報

機能名	リリース	機能情報
BFD C ビットの IS-IS クライアント サポート	15.1(1)SY 15.3(1)T	BFD C ビットの IS-IS クライアント サポート機能では、BFD セッションの障害が本当であるか、ルータの再起動によるコントロールプレーン障害の結果であるかどうかをネットワークで特定することができます。 **bfd check-ctrl-plane-failure** コマンドが導入されました。

第 10 章

BFD ダンプニング

BFD ダンプニング機能は、設定可能な指数関数的遅延メカニズムを導入し、双方向フォワーディング検出（BFD）によってフラップが発生している、リモート ノードの到達可能性イベントの過度な影響を抑制します。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。高速インターフェイスで BFD ダンプニング機能をルーティング クライアントとともに設定することで、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。

- 機能情報の確認，147 ページ
- BFD ダンプニングに関する情報，148 ページ
- BFD ダンプニングの設定方法，149 ページ
- BFD ダンプニングの設定例，150 ページ
- BFD ダンプニングに関する追加情報，151 ページ
- BFD ダンプニングに関する機能情報，151 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BFD ダンプニングに関する情報

BFD ダンプニングの概要

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明らかにするため、ルーティング プロトコルで使用されるメカニズムです。BFD でネイバーの到達可能性ステータスの変更が検出されると、クライアントは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システム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 ダンプニング機能は、設定可能な指数関数的遅延メカニズムを導入し、BFD によってフラップが発生している、リモート ノードの到達可能性イベントの過度な影響を抑制します。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、モニタリング下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 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。セッションでダンプニングを行わない場合は、新しいセッションに対してダンプニングが有効になっていない新規の 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 ダンプニングの設定方法

BFD ダンプニングの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **bfd-template multi-hop***template-name*
4. **intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value*
5. **dampening** [*half-life-periodreuse-thresholdsuppress-thresholdmax-suppress-time*]
6. **end**
7. **showbfdneighborsdetails**
8. **showbfdneighborsdampening**
9. **showbfdneighborsdampened**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bfd-template multi-hop***template-name* 例： `Device(config)# bfd-template multi-hop doctemplate`	双方向フォワーディング検出（BFD）テンプレートを作成し、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 4	**intervalmin-tx***milliseconds***min-rx***milliseconds***multiplier***multiplier-value* 例： `Device(config-bfd)# interval min-tx 120 min-rx 100 multiplier 3`	BFD パケット間での送受信間隔を設定し、ピアが使用不能であると BFD が宣言する前に損失される連続的な BFD 制御パケット数を指定します。

	コマンドまたはアクション	目的
ステップ 5	**dampening** [*half-life-periodreuse-thresholdsuppress-thresholdmax-suppress-time*] 例： `Device(config-bfd)# dampening 2 1000 3000 8`	フラップが発生しているセッションのダンプニングを行うようにデバイスを設定します。
ステップ 6	**end** 例： `Device(config-bfd)# end`	BFD コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**showbfdneighborsdetails** 例： `Device# show bfd neighbors details`	（任意）既存の BFD 隣接関係のリストと、BFD セッションに関するダンプニング情報（BFD ダンプニングがセッションで有効な場合）を表示します。
ステップ 8	**showbfdneighborsdampening** 例： `Device# show bfd neighbors dampening`	（任意）BFD ダンプニングが設定された BFD セッションに関するダンプニング情報を表示します。
ステップ 9	**showbfdneighborsdampened** 例： `Device# show bfd neighbors dampened`	（任意）現在ダンプニングを行っている BFD セッションに関するダンプニング情報を表示します。

BFD ダンプニングの設定例

例：BFD ダンプニングの設定

次の例は、BFD ダンプニングを設定する方法を示しています。

```
bfd-template multi-hop doctemplate
 interval min-tx 120 min-rx 100 multiplier 3
 dampening 2 1000 3000 8
```

BFD ダンプニングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
BFD コマンド	『Cisco IOS IP Routing: Protocol-Independent Command Reference』
双方向フォワーディング検出	『*IP ルーティング BFD コンフィギュレーション ガイド*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

BFD ダンプニングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：*BFD* ダンプニングに関する機能情報

機能名	リリース	機能情報
BFD ダンプニング	Cisco IOS XE Release 3.8S Cisco IOS Release 15.3(2)T	BFD ダンプニング機能は、設定可能な指数関数的遅延メカニズムを導入し、BFD によってフラップが発生している、リモート ノードの到達可能性イベントの過度な影響を抑制します。また、この機能を使用して、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。 **dampening**（**bfd**）と **show bfd neighbors** のコマンドが導入または変更されました。