



Cisco IOS IP ルーティング : BFD コンフィギュレーション ガイド

Cisco IOS IP Routing: BFD Configuration

リリース 15.1

【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、米国シスコシステムズ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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco IOS IP ルーティング : BFD コンフィギュレーション ガイド
Copyright © 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社.
All rights reserved.



Cisco IOS ソフトウェア マニュアルについて

このマニュアルでは、Cisco IOS ソフトウェアのマニュアルで使用される目標、対象読者、表記法、およびマニュアルの構成について説明します。技術サポート、追加のマニュアル、およびその他の情報をシスコから取得するためのリソースも記載されています。このマニュアルは、次のセクションから構成されています。

- 「マニュアルの目標」 (P.i)
- 「対象読者」 (P.i)
- 「マニュアルの表記法」 (P.i)
- 「マニュアルの構成」 (P.iii)
- 「追加のリソースとマニュアルのフィードバック」 (P.xiii)

マニュアルの目標

Cisco IOS マニュアルでは、シスコのネットワーク デバイスを設定して保守するために使用可能なタスクとコマンドについて説明します。

対象読者

Cisco IOS マニュアルセットは、シスコのネットワーク デバイス（ルータやスイッチなど）の設定と保守を行うが、設定タスクと保守タスク、タスク間の関係、または特定のタスクを実行するために必要な Cisco IOS コマンドに関する知識がないユーザを対象としています。Cisco IOS マニュアルセットは、Cisco IOS ソフトウェアの使用経験があり、Cisco IOS の現行リリースの新機能、新しい設定オプション、および新しいソフトウェア特性を理解する必要があるユーザも対象としています。

マニュアルの表記法

Cisco IOS マニュアルでは、ルータという用語は、さまざまなシスコ製品（たとえば、ルータ、アクセス サーバ、およびスイッチ）を指すために使用されることがあります。Cisco IOS ソフトウェアをサポートするこれらの製品とその他のネットワーク デバイスは、例で同じように示され、図示のためだけに使用されます。ある製品を示す例は、他の製品がサポートされないことを必ずしも意味しているわけではありません。

このセクションには次のトピックがあります。

- 「印刷時の表記法」(P.ii)
- 「コマンド構文の表記」(P.ii)
- 「ソフトウェアの表記法」(P.iii)
- 「読者への警告の表記法」(P.iii)

印刷時の表記法

Cisco IOS マニュアルでは、次の印刷時の表記法が使用されます。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control (Ctrl) キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します (キーは大文字で表記しますが、小文字で入力してもかまいません)。
ストリング	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) コミュニティストリングを <i>public</i> に設定する場合は、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。

コマンド構文の表記

Cisco IOS マニュアルでは、次のコマンド構文の表記が使用されます。

表記法	説明
太字	記載されているとおりに入力するコマンドおよびキーワードは、太字で示します。
イタリック体	ユーザが値を指定する引数は、イタリック体で示します。
[x]	省略可能なキーワードまたは引数は角カッコで囲みます。
...	構文要素の後の省略記号 (3 つの連続する太字ではないピリオドでスペースを含まない) は、その要素を繰り返すことができることを示します。
	波カッコまたは角カッコで囲まれたパイプと呼ばれる縦棒は、キーワードセットまたは引数セットのうちの選択肢を示します。
[x y]	パイプで区切られたキーワードまたは引数を囲む角カッコは、省略可能な選択肢を示します。
{x y}	パイプで区切られたキーワードまたは引数を囲む波カッコは、必須の選択肢を示します。
[x {y z}]	角カッコ内の波カッコおよびパイプは、省略可能な要素の中で、必ずいずれかか 1 つを選択しなければならないことを示します。

ソフトウェアの表記法

Cisco IOS ソフトウェアでは、次のプログラム コードの表記法が使用されます。

表記法	説明
Courier font	courier フォントは PC または端末画面に表示される情報に使用されます。
Bold Courier font	太字の courier フォントは、ユーザが入力しなければならないテキストを示します。
< >	山カッコで囲まれたテキストは、パスワードなど、表示されないテキストを表します。山カッコは、ASCII テキストなど、イタリック体スタイルがサポートされないコンテキストでも使用されます。
!	行の先頭にある感嘆符は、コードの行ではなくコメントの後に続くテキストです。感嘆符は、Cisco IOS ソフトウェアの特定のプロセスでも表示されます。
[]	角カッコは、システム プロンプトに対するデフォルトの応答です。

読者への警告の表記法

Cisco IOS マニュアルでは、読者への警告について次の表記法が使用されます。



注意

「**要注意**」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



(注)

「**注釈**」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ワンポイントアドバイス

「**時間の節約に役立つ操作**」です。記述されている操作を実行すると時間を節約できます。

マニュアルの構成

ここでは、Cisco IOS マニュアルセット、その構成方法、および Cisco.com でのアクセス方法について説明します。コンフィギュレーションガイド、コマンドリファレンス、およびマニュアルセットを構成する補足の参照とリソースもリストされています。次のトピックがあります。

- 「[Cisco IOS マニュアルセット](#)」(P.iv)
- 「[Cisco.com の Cisco IOS マニュアル](#)」(P.iv)
- 「[コンフィギュレーションガイド、コマンドリファレンス、および補足リソース](#)」(P.v)

Cisco IOS マニュアル セット

Cisco IOS マニュアル セットは次のように構成されます。

- リリース ノートおよび警告には、リリースのプラットフォーム、テクノロジー、および機能サポートに関する情報と、リリースされた Cisco IOS ソフトウェアでの重大度 1（最悪）、重大度 2（重大）、および重大度 3（中程度）の障害に関する説明が記載されています。他のマニュアルの前にリリース ノートを確認して、機能に更新が行われたかどうかを調べてください。
- テクノロジー別に編成され、標準の Cisco IOS リリースごとに発行される一連のコンフィギュレーション ガイドとコマンド リファレンス。
 - コンフィギュレーション ガイド：Cisco IOS 機能の概念的な説明とタスク指向の説明が記載されているマニュアルの組み合わせ。
 - コマンド リファレンス：関連するコンフィギュレーション ガイドを構成する、Cisco IOS 機能とプロセスで使用されるコマンドに関する詳細が記載された、アルファベット順のコマンド ページの組み合わせ。テクノロジーごとに、すべての Cisco IOS リリースをサポートし、標準のリリースのたびに更新される単一のコマンド リファレンスがあります。
- 特定のリリースにおける全コマンドと、リリースでの新規、変更済み、削除済み、または置き換え済みの全コマンドのリスト。
- **debug** コマンドのコマンド リファレンス マニュアル。コマンド ページはアルファベット順にリストされます。
- すべての Cisco IOS リリースのシステム メッセージのリファレンス マニュアル。

Cisco.com の Cisco IOS マニュアル

次のセクションでは、Cisco IOS マニュアル セットの構成と、さまざまなタイプのマニュアルへのアクセス方法について説明します。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

機能ガイド

Cisco IOS 機能は、機能ガイドに文書化されています。機能ガイドでは、多数の異なるソフトウェア リリースとプラットフォームでサポートされる 1 つの機能または関連する機能グループについて説明します。Cisco IOS ソフトウェア リリースまたはプラットフォームでは、機能ガイドで文書化されているすべて機能がサポートされないことがあります。そのガイドでどの機能がソフトウェア リリースでサポートされるかについては、機能ガイドの最後にある機能情報の表を参照してください。

コンフィギュレーション ガイド

コンフィギュレーション ガイドは、テクノロジーとリリース別に提供され、リリースとテクノロジーに関連する個々の機能ガイドセットで構成されます。

コマンド リファレンス

コマンド リファレンス マニュアルには、多数の異なるソフトウェア リリースとプラットフォームでサポートされる Cisco IOS コマンドの説明が記載されています。マニュアルはテクノロジー別に構成されています。すべての Cisco IOS コマンドについては、<http://tools.cisco.com/Support/CLILookup> で Command Lookup Tool を使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html にある *Cisco IOS Master Command List, All Releases* を使用してください。

Cisco IOS 補足マニュアルとリソース

補足マニュアルとリソースは、表 2 (P.xii) にリストされています。

コンフィギュレーション ガイド、コマンド リファレンス、および補足リソース

表 1 には、マニュアルの内容の簡単な説明を含め、Cisco IOS ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスがアルファベット順にリストされています。Cisco IOS コマンド リファレンスには、すべてのリリースの Cisco IOS ソフトウェアのコマンドが記載されています。コンフィギュレーション ガイドとコマンド リファレンスでは、多数の異なるソフトウェア リリースとプラットフォームがサポートされます。お使いの Cisco IOS ソフトウェア リリースまたはプラットフォームでは、一部のテクノロジーがサポートされないことがあります。

表 2 には、Cisco IOS ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスを補足するマニュアルとリソースがリストされています。これらの補足リソースには、リリース ノートおよび警告、マスター コマンド リスト、新規、変更済み、削除済み、および置き換え済みのコマンドのリスト、システム メッセージ、およびデバッグ コマンド リファレンスがあります。

特定のネットワーク デバイスの設定と操作に関する追加情報を取得して、Cisco IOS マニュアルにアクセスするには、次の URL にある Cisco.com の Product/Technologies Support エリアにアクセスしてください。

<http://www.cisco.com/go/techdocs>

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス

コンフィギュレーション ガイドとコマンド リファレンスのタイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS AppleTalk Configuration Guide』 『Cisco IOS AppleTalk Command Reference』 	AppleTalk プロトコル。
<ul style="list-style-type: none"> 『Cisco IOS Asynchronous Transfer Mode Configuration Guide』 『Cisco IOS Asynchronous Transfer Mode Command Reference』 	LAN ATM、Multiprotocol over ATM (MPoA)、および WAN ATM。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> • 『Cisco IOS Bridging and IBM Networking Configuration Guide』 • 『Cisco IOS Bridging Command Reference』 • 『Cisco IOS IBM Networking Command Reference』 	<p>トランスペアレントおよび Source-Route Transparent (SRT; ソースルート トランスペアレント) ブリッジング、Source-Route Bridging (SRB; ソースルート ブリッジング)、Token Ring Inter-Switch Link (TRISL; トークンリング スイッチ間リンク)、ならびに Token Ring Route Switch Module (TRRSM; トークンリング ルート スイッチ モジュール)。</p> <p>Data-link Switching Plus (DLSw+; データリンク スイッチング プラス)、Serial Tunnel (STUN; シリアル トンネル)、Block Serial Tunnel (BSTUN; ブロック シリアル トンネル)、Logical Link Control, Type 2 (LLC2; 論理リンク制御タイプ 2)、Synchronous Data Link Control (SDLC; 同期データ リンク制御)、IBM Network Media Translation (Synchronous Data Logical Link Control (SDLLC; 同期データ論理リンク制御) および Qualified LLC (QLLC; 修飾 LLC) を含む)、Downstream Physical Unit (DSPU; 下流物理ユニット)、Systems Network Architecture (SNA; システム ネットワーク アーキテクチャ) サービス ポイント、SNA フレーム リレー アクセス、Advanced Peer-to-Peer Networking (APPN; 拡張分散ネットワーク機能)、Native Client Interface Architecture (NCIA; ネイティブ クライアント インターフェイス アーキテクチャ) クライアント/サーバテクノロジー、ならびに IBM Channel Attach。</p>
<ul style="list-style-type: none"> • 『Cisco IOS Broadband Access Aggregation and DSL Configuration Guide』 • 『Cisco IOS Broadband Access Aggregation and DSL Command Reference』 	<p>PPP over ATM (PPPoA) と PPP over Ethernet (PPPoE)。</p>
<ul style="list-style-type: none"> • 『Cisco IOS Carrier Ethernet Configuration Guide』 • 『Cisco IOS Carrier Ethernet Command Reference』 	<p>Operations, Administration, and Maintenance (OAM; 操作、管理、メンテナンス)。イーサネット Connectivity Fault Management (CFM) ITU-T Y.1731 障害管理機能。イーサネット Local Management Interface (ELMI)。サービス インスタンス、ブリッジ ドメイン、および Pseudo Wire 上での MAC アドレス サポート。IEEE 802.3ad リンク ブリッジ。イーサネット、ギガビット イーサネット リンク、および EtherChannel バンドルの Link Aggregation Control Protocol (LACP) サポート。ギガビット EtherChannel バンドル上での Stateful Switchover (SSO)、In Service Software Upgrade (ISSU; インサービス ソフトウェア アップグレード)、Cisco Nonstop Forwarding (NSF) の LACP サポート、および Link Layer Discovery Protocol (LLDP) および Media Endpoint Discovery (MED)。</p>
<ul style="list-style-type: none"> • 『Cisco IOS Configuration Fundamentals Configuration Guide』 • 『Cisco IOS Configuration Fundamentals Command Reference』 	<p>自動インストール、設定、Cisco IOS Command-Line Interface (CLI; コマンドライン インターフェイス)、Cisco IOS File System (IFS)、Cisco IOS Web ブラウザ ユーザ インターフェイス (UI)、基本的なファイル転送サービス、およびファイル管理。</p>

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS DECnet Configuration Guide』 『Cisco IOS DECnet Command Reference』 	DECnet プロトコル。
<ul style="list-style-type: none"> 『Cisco IOS Dial Technologies Configuration Guide』 『Cisco IOS Dial Technologies Command Reference』 	非同期通信、ダイヤル バックアップ、ダイヤラ テクノロジー、ダイヤルイン端末サービスと AppleTalk Remote Access (ARA)、Dial-on-Demand Routing (DDR; ダイヤル オンデマンドルーティング)、ダイヤルアウト、ISDN、大規模のダイヤルアウト、モデムとリソース プーリング、Multilink PPP (MLP; マルチリンク PPP)、PPP、および Virtual Private Dial-up Network (VPDN; バーチャル プライベート ダイヤルアップ ネットワーク)。
<ul style="list-style-type: none"> 『Cisco IOS Flexible NetFlow Configuration Guide』 『Cisco IOS Flexible NetFlow Command Reference』 	柔軟性のある NetFlow。
<ul style="list-style-type: none"> 『Cisco IOS High Availability Configuration Guide』 『Cisco IOS High Availability Command Reference』 	High Availability (HA; ハイ アベイラビリティ) を備えたエンドツーエンド ネットワークの作成を容易にするためのさまざまなネットワーク セグメント (企業アクセスからサービス プロバイダー コアに至る) で使用可能なさまざまなハイ アベイラビリティ機能とテクノロジー。Cisco IOS HA 機能とテクノロジーは、システムレベルの復元力、ネットワークレベルの復元力、および復元力のために埋め込まれた管理の 3 つの主な領域にカテゴリ化できます。
<ul style="list-style-type: none"> 『Cisco IOS Intelligent Services Gateway Configuration Guide』 『Cisco IOS Intelligent Services Gateway Command Reference』 	加入者 ID、サービスとポリシーの判別、セッション作成、セッション ポリシー適用、セッション ライフサイクル管理、アクセスおよびサービス使用のアカウンティング、およびセッション状態モニタリング。
<ul style="list-style-type: none"> 『Cisco IOS Interface and Hardware Component Configuration Guide』 『Cisco IOS Interface and Hardware Component Command Reference』 	LAN インターフェイス、論理インターフェイス、シリアル インターフェイス、仮想インターフェイス、およびインターフェイス コンフィギュレーション。
<ul style="list-style-type: none"> 『Cisco IOS IP Addressing Services Configuration Guide』 『Cisco IOS IP Addressing Services Command Reference』 	Address Resolution Protocol (ARP; アドレス解決プロトコル)、Network Address Translation (NAT; ネットワーク アドレス変換)、Domain Name System (DNS; ドメイン ネーム システム)、Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル)、および Next Hop Address Resolution Protocol (NHRP)。
<ul style="list-style-type: none"> 『Cisco IOS IP Application Services Configuration Guide』 『Cisco IOS IP Application Services Command Reference』 	Enhanced Object Tracking (EOT; 拡張オブジェクト トラッキング)、Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル)、Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)、IP サービス、Server Load Balancing (SLB)、Stream Control Transmission Protocol (SCTP)、Transmission Control Protocol (TCP; 伝送制御プロトコル)、Web Cache Communication Protocol (WCCP; Web キャッシュ通信プロトコル)、User Datagram Protocol (UDP; ユーザ データグラム プロトコル)、および Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル)。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS IP Mobility Configuration Guide』 『Cisco IOS IP Mobility Command Reference』 	Mobile Ad hoc Network (MANet) およびシスコのモバイルネットワーク。
<ul style="list-style-type: none"> 『Cisco IOS IP Multicast Configuration Guide』 『Cisco IOS IP Multicast Command Reference』 	Protocol Independent Multicast (PIM) sparse mode 希薄モード (PIM-SM; PIM 希薄モード)、bidirectional PIM (bidir-PIM; 双方向 PIM)、Source Specific Multicast (SSM)、Multicast Source Discovery Protocol (MSDP)、Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)、および Multicast VPN (MVPN; マルチキャスト VPN)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: BFD Configuration Guide』 	Bidirectional Forwarding Detection (BFD)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: BGP Configuration Guide』 『Cisco IOS IP Routing: BGP Command Reference』 	Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル)、マルチプロトコル BGP、IP マルチキャスト用マルチプロトコル BGP 拡張。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: EIGRP Configuration Guide』 『Cisco IOS IP Routing: EIGRP Command Reference』 	Enhanced Interior Gateway Routing Protocol (EIGRP)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: ISIS Configuration Guide』 『Cisco IOS IP Routing: ISIS Command Reference』 	Intermediate System-to-Intermediate System (IS-IS)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: ODR Configuration Guide』 『Cisco IOS IP Routing: ODR Command Reference』 	On-Demand Routing (ODR; オンデマンド ルーティング)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: OSPF Configuration Guide』 『Cisco IOS IP Routing: OSPF Command Reference』 	Open Shortest Path First (OSPF)。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: Protocol-Independent Configuration Guide』 『Cisco IOS IP Routing: Protocol-Independent Command Reference』 	IP ルーティング プロトコル独立機能およびコマンド。一般的な Policy-Based Routing (PBR; ポリシーベース ルーティング) 機能およびコマンドが含まれます。
<ul style="list-style-type: none"> 『Cisco IOS IP Routing: RIP Configuration Guide』 『Cisco IOS IP Routing: RIP Command Reference』 	Routing Information Protocol (RIP)。
<ul style="list-style-type: none"> 『Cisco IOS IP SLAs Configuration Guide』 『Cisco IOS IP SLAs Command Reference』 	Cisco IOS IP Service Level Agreement (IP SLA; IP サービス レベル契約)。
<ul style="list-style-type: none"> 『Cisco IOS IP Switching Configuration Guide』 『Cisco IOS IP Switching Command Reference』 	Cisco Express Forwarding、ファスト スイッチング、および Multicast Distributed Switching (MDS)。
<ul style="list-style-type: none"> 『Cisco IOS IPv6 Configuration Guide』 『Cisco IOS IPv6 Command Reference』 	IPv6 機能、プロトコル、およびテクノロジーについては、IPv6 のマニュアル『 Start Here 』にアクセスしてください。
<ul style="list-style-type: none"> 『Cisco IOS ISO CLNS Configuration Guide』 『Cisco IOS ISO CLNS Command Reference』 	ISO Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス)。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> • 『Cisco IOS LAN Switching Configuration Guide』 • 『Cisco IOS LAN Switching Command Reference』 	VLAN、Inter-Switch Link (ISL; スイッチ間リンク) カプセル化、IEEE 802.10 カプセル化、IEEE 802.1Q カプセル化、および Multilayer Switching (MLS; マルチレイヤ スイッチング)。
<ul style="list-style-type: none"> • 『Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide』 • 『Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference』 	第 2.5 世代 General Packet Radio Service (GPRS; グローバル パケット ラジオ サービス) および第 3 世代 Universal Mobile Telecommunication System (UMTS) ネットワークにおける Cisco IOS Gateway GPRS Support Node (GGSN; ゲートウェイ GPRS サポート ノード)。
<ul style="list-style-type: none"> • 『Cisco IOS Mobile Wireless Home Agent Configuration Guide』 • 『Cisco IOS Mobile Wireless Home Agent Command Reference』 	Cisco Mobile Wireless Home Agent : モバイル IP またはプロキシ モバイル IP サービスが提供されるモバイル端末のアンカー ポイント。
<ul style="list-style-type: none"> • 『Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide』 • 『Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference』 	Cisco Packet Data Serving Node (PDSN) : モバイル インフラストラクチャと標準の IP ネットワーク間にあり、Code Division Multiple Access (CDMA; 符号分割多重接続) 環境でパケット データ サービスを使用可能にするワイヤレス ゲートウェイ。
<ul style="list-style-type: none"> • 『Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide』 • 『Cisco IOS Mobile Wireless Radio Access Networking Command Reference』 	Cisco IOS 無線アクセス ネットワーク製品。
<ul style="list-style-type: none"> • 『Cisco IOS Multiprotocol Label Switching Configuration Guide』 • 『Cisco IOS Multiprotocol Label Switching Command Reference』 	MPLS Label Distribution Protocol (LDP; ラベル配布プロトコル)、MPLS レイヤ 2 VPN、MPLS レイヤ 3 VPN、MPLS Traffic Engineering (TE; トラフィック エンジニアリング)、および MPLS Embedded Management (EM) と MIB。
<ul style="list-style-type: none"> • 『Cisco IOS Multi-Topology Routing Configuration Guide』 • 『Cisco IOS Multi-Topology Routing Command Reference』 	ユニキャストおよびマルチキャスト トポロジの設定、トラフィックの分類、ルーティング プロトコル サポート、および ネットワーク管理サポート。
<ul style="list-style-type: none"> • 『Cisco IOS NetFlow Configuration Guide』 • 『Cisco IOS NetFlow Command Reference』 	ネットワーク トラフィック データの分析、集約キャッシュ、およびエクスポート機能。
<ul style="list-style-type: none"> • 『Cisco IOS Network Management Configuration Guide』 • 『Cisco IOS Network Management Command Reference』 	基本的なシステム管理、システム モニタリングとロギング、トラブルシューティング、ロギング、および障害管理、Cisco Discovery Protocol、Cisco IOS Scripting with Tool Control Language (TCL)、Cisco Networking Service (CNS)、DistributedDirector、Embedded Event Manager (EEM; 組み込み型イベントマネージャ)、Embedded Resource Manager (ERM)、Embedded Syslog Manager (ESM)、HTTP、Remote Monitoring (RMON; リモート モニタリング)、SNMP、および VPN Device Manager Client for Cisco IOS ソフトウェア (XSM Configuration)。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS Novell IPX Configuration Guide』 『Cisco IOS Novell IPX Command Reference』 	Novell Internetwork Packet Exchange (IPX) プロトコル。
<ul style="list-style-type: none"> 『Cisco IOS Optimized Edge Routing Command Reference』 	Optimized Edge Routing (OER) モニタリング、およびネットワーク間の複数接続の場合の自動ルート最適化と負荷分散。
<ul style="list-style-type: none"> 『Cisco IOS Performance Routing Configuration Guide』 	Performance Routing (PfR) は標準的なルーティング技術の機能を高める技術であり、アプリケーション トラフィック用に最適な出力パスまたは入力パスを判断するため、WAN インフラストラクチャ上の 2 つのデバイス間のパスのパフォーマンスの追跡または品質の確認が行えます。
<ul style="list-style-type: none"> 『Cisco IOS Quality of Service Solutions Configuration Guide』 『Cisco IOS Quality of Service Solutions Command Reference』 	トラフィック キューイング、トラフィック ポリシング、トラフィック シェーピング、Modular QoS CLI (MQC; モジュラ QoS CLI)、Network-Based Application Recognition (NBAR)、QoS のマルチリンク PPP (MLP)、ヘッダー圧縮、AutoQoS、Resource Reservation Protocol (RSVP; リソース予約プロトコル)、および Weighted Random Early Detection (WRED; 重み付けランダム早期検出)。
<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference』 	Access Control List (ACL; アクセス コントロール リスト)、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントリング)、ファイアウォール、IP セキュリティと暗号化、ネイバルータ認証、ネットワーク アクセス セキュリティ、ルータの認証によるネットワーク データ暗号化、Public Key Infrastructure (PKI; 公開鍵インフラストラクチャ)、RADIUS、TACACS+、端末アクセス セキュリティ、およびトラフィック フィルタ。
<ul style="list-style-type: none"> 『Cisco IOS Security Configuration Guide: Securing the Data Plane』 	アクセス コントロール リスト (ACL)、ファイアウォール、Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) およびゾーンベース ファイアウォール、Cisco IOS Intrusion Prevention System (IPS; 侵入防御システム)、Flexible Packet Matching、Unicast Reverse Path Forwarding (uRPF; ユニキャスト RPF)、Threat Information Distribution Protocol (TIDP) および TMS。
<ul style="list-style-type: none"> 『Cisco IOS Security Configuration Guide: Securing the Control Plane』 	Control Plane Policing、ネイバフッド ルータ認証。
<ul style="list-style-type: none"> 『Cisco IOS Security Configuration Guide: Securing User Services』 	AAA (802.1x 認証と Network Admission Control (NAC; ネットワーク アドミッションコントロール) を含む)、セキュリティ サーバプロトコル (RADIUS と TACACS+)、Secure Shell (SSH; セキュア シェル)、ネットワークング デバイスのセキュア アクセス (Autosecure とロールベース CLI アクセスを含む)、合法的傍受。
<ul style="list-style-type: none"> 『Cisco IOS セキュリティ コンフィギュレーション ガイド : Secure Connectivity』 	IPsec VPN の Internet Key Exchange (IKE; インターネットキー エクスチェンジ)、IPsec データ プレーン機能、IPsec 管理機能、公開鍵インフラストラクチャ (PKI)、Dynamic Multipoint VPN (DMVPN; ダイナミック マルチポイント VPN)、Easy VPN、Cisco Group Encrypted Transport VPN (GETVPN)、SSL VPN。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS Service Advertisement Framework Configuration Guide』 『Cisco IOS Service Advertisement Framework Command Reference』 	Cisco Service Advertisement Framework。
<ul style="list-style-type: none"> 『Cisco IOS Service Selection Gateway Configuration Guide』 『Cisco IOS Service Selection Gateway Command Reference』 	加入者認証、サービス アクセス、およびアカウンティング。
<ul style="list-style-type: none"> 『Cisco IOS Software Activation Configuration Guide』 『Cisco IOS Software Activation Command Reference』 	シスコ ソフトウェアのライセンスを取得して検証することによって、Cisco IOS ソフトウェア フィーチャセットを有効にするために編成されたプロセスとコンポーネントの集合。
<ul style="list-style-type: none"> 『Cisco IOS Software Modularity Installation and Configuration Guide』 『Cisco IOS Software Modularity Command Reference』 	ソフトウェア モジュラリティ イメージのインストールと基本設定。単一のルート プロセッサと二重のルート プロセッサへのインストール、インストールのロールバック、ソフトウェア モジュラリティ バインディング、ソフトウェア モジュラリティ プロセス、およびパッチが含まれます。
<ul style="list-style-type: none"> 『Cisco IOS Terminal Services Configuration Guide』 『Cisco IOS Terminal Services Command Reference』 	DEC、Local-Area Transport (LAT)、および X.25 Packet Assembler/Disassembler (PAD; パケット アセンブラ/ディスアセンブラ)。
<ul style="list-style-type: none"> 『Cisco IOS Virtual Switch Command Reference』 	仮想スイッチの冗長性、ハイ アベイラビリティ、およびパケット処理、スタンドアロンスイッチ モードと仮想スイッチ モード間の変換、Virtual Switch Link (VSL; 仮想スイッチ リンク)、Virtual Switch Link Protocol (VSLP; 仮想スイッチ リンク プロトコル)。 (注) 仮想スイッチの設定については、Cisco Catalyst 6500 シリーズ スイッチまたは Metro Ethernet 6500 シリーズ スイッチの製品固有のソフトウェア設定情報を参照してください。
<ul style="list-style-type: none"> 『Cisco IOS Voice Configuration Library』 『Cisco IOS Voice Command Reference』 	音声制御プロトコルの Cisco IOS サポート、相互運用性、物理および仮想インターフェイス管理、およびトラブルシューティング。ライブラリには、IP テレフォニー アプリケーションのマニュアルが含まれています。
<ul style="list-style-type: none"> 『Cisco IOS VPDN Configuration Guide』 『Cisco IOS VPDN Command Reference』 	Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) ダイアルアウトロード バランシングと冗長性、L2TP 拡張フェールオーバー、L2TP セキュリティ VPDN、Dialed Number Identification Service (DNIS; 着信番号識別サービス) によるマルチホップ、L2TP および Layer 2 Forwarding (L2F) の場合のタイマーと再試行の改良、RADIUS アトリビュート 82 (トンネル割り当て ID)、VPDN ユーザのシェルベース認証、トンネル ターミネータでの RADIUS によるトンネル認証。

表 1 Cisco IOS コンフィギュレーション ガイドとコマンド リファレンス (続き)

コンフィギュレーション ガイドとコマンド リファレンスの タイトル	機能/プロトコル/テクノロジー
<ul style="list-style-type: none"> 『Cisco IOS Wide-Area Networking Configuration Guide』 『Cisco IOS Wide-Area Networking Command Reference』 	フレーム リレー、Layer 2 Tunnel Protocol Version 3 (L2TPv3; レイヤ 2 トンネル プロトコル バージョン 3)、L2VPN 擬似回線冗長性、L2VPN インターワーキング、レイヤ 2 ローカル スイッチング、Link Access Procedure, Balanced (LAPB; 平衡型リンク アクセス手順)、および X.25。
<ul style="list-style-type: none"> 『Cisco IOS Wireless LAN Configuration Guide』 『Cisco IOS Wireless LAN Command Reference』 	ブロードキャスト キー ローテーション、IEEE 802.11x サポート、IEEE 802.1x オーセンティケータ、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) のための IEEE 802.1x ローカル認証サービス、Multiple Basic Service Set ID (BSSID)、Wi-Fi Multimedia (WMM) 必須要素、および Wi-Fi Protected Access (WPA)。

表 2 には、Cisco IOS ソフトウェアのコンフィギュレーション ガイドとコマンド リファレンスを補足するマニュアルとリソースがリストされています。

表 2 Cisco IOS 補足マニュアルとリソース

マニュアル タイトルまたはリソース	説明
『Cisco IOS Master Command List, All Releases』	すべての Cisco IOS リリースで文書化されている全コマンドのアルファベット順のリスト。
『Cisco IOS New, Modified, Removed, and Replaced Commands』	Cisco IOS リリースの新規、変更済み、削除済み、および置き換え済みの全コマンドのリスト。
『Cisco IOS System Message Guide』	Cisco IOS システム メッセージのリストと説明。システム メッセージは、ご使用のシステムの問題を示しているか、単なる通知である場合があります。通信回線、内部ハードウェア、またはシステム ソフトウェアの問題の診断に役立つことがあります。
『Cisco IOS Debug Command Reference』	使用に関する簡単な説明、コマンド構文、使用上のガイドラインを含む、 debug コマンドのアルファベット順のリスト。
リリース ノートおよび監視	新機能と変更された機能およびシステム要件に関する情報、および特定のソフトウェア リリースに関するその他の役立つ情報。特定の Cisco IOS ソフトウェア リリースの障害に関する情報。
MIB	ネットワークのモニタリングに使用されるファイル。選択したプラットフォーム、Cisco IOS リリース、およびフィチャセット用の MIB を見つけてダウンロードするには、 Cisco MIB Locator を使用します。
RFC	(適切な場合) Cisco IOS マニュアルで参照する、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) によって保守される標準のドキュメント。参照される RFC の全文は次の URL で入手できます。 http://www.rfc-editor.org/

追加のリソースとマニュアルのフィードバック

『*What's New in Cisco Product Documentation*』は毎月リリースされ、シスコの新規および改訂版のすべての技術マニュアルについて説明しています。『*What's New in Cisco Product Documentation*』には、次のリソースの入手/利用方法に関する情報も記載されています。

- 技術マニュアル
- シスコ製品のセキュリティの概要
- Product Alert および Field Notice
- テクニカル サポート

Cisco IOS の技術マニュアルには、フィードバックのための専用フォームが含まれています。ユーザはこれを使用して、マニュアルの内容を評価し、改善のための提案を行うことができます。マニュアルの品質向上のため、ぜひフィードバックをお寄せください。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2008–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2010, シスコシステムズ合同会社。
All rights reserved.



Cisco IOS ソフトウェアのコマンドライン インターフェイスの使用

このマニュアルでは、Cisco IOS ソフトウェアの Command-Line Interface (CLI; コマンドライン インターフェイス) および一部の CLI 機能の使用方法に関する基本的な情報について説明します。このマニュアルの構成は、次のとおりです。

- 「デバイスの初期設定」(P.i)
- 「CLI の使用」(P.ii)
- 「コンフィギュレーションに対する変更の保存」(P.xii)
- 「その他の情報」(P.xiii)

CLI の使用方法については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「[Using the Cisco IOS Command-Line Interface](#)」のセクションを参照してください。

ソフトウェアのマニュアル一式については、『[About Cisco IOS Software Documentation](#)』のマニュアルを参照してください。

デバイスの初期設定

デバイスの初期設定はプラットフォームによって異なります。初期設定の実行方法については、製品出荷時の同梱材に含まれるハードウェア設置マニュアルを参照するか、<http://www.cisco.com/go/techdocs> の Cisco.com の Product/Technologies Support サイトを参照してください。

初期設定を実行し、ネットワークにデバイスを接続した後、コンソールポートまたは Telnet や Secure Shell (SSH; セキュア シェル) などのリモート アクセス方式を使用して CLI にアクセスするか、または Security Device Manager など、デバイスで提供される設定方法を使用することにより、デバイスを設定できます。

コンソール ポートまたは Auxiliary (AUX; 補助) ポートのデフォルト設定の変更

コンソール ポートおよび AUX ポートに対して行うことができる変更は次の 2 点だけです。

- **config-register 0x** コマンドを使用したポート速度の変更。ポート速度を変更することは推奨されていません。既知のデフォルト速度は 9600 です。
- たとえば、パスワードの追加やタイムアウト値の変更による、ポートの動作の変更。



(注)

Cisco ASR 1000 シリーズ ルータに搭載された Route Processor (RP; ルート プロセッサ) の AUX ポートは、実用的なカスタマーの目的に提供されるものではなく、カスタマー サポート担当者の助言に基づく場合にだけアクセスする必要があります。

CLI の使用

ここでは、次の内容について説明します。

- 「コマンド モードの概要」 (P.ii)
- 「対話型ヘルプ機能の使用」 (P.vi)
- 「コマンド シンタックスの概要」 (P.vii)
- 「イネーブル パスワードおよびイネーブル シークレット パスワードの概要」 (P.viii)
- 「コマンド履歴機能の使用」 (P.ix)
- 「コマンドの省略」 (P.x)
- 「CLI コマンドのエイリアスの使用」 (P.x)
- 「コマンドの no 形式および default 形式の使用」 (P.x)
- 「debug コマンドの使用」 (P.xi)
- 「出力修飾子を使用する出力のフィルタリング」 (P.xi)
- 「CLI エラー メッセージの概要」 (P.xii)

コマンド モードの概要

CLI コマンド モードの構造は階層型であり、各モードで一連の特定コマンドをサポートしています。ここでは、存在する多数のモードのうち最も一般的なモードについて説明します。

表 1 に、CLI プロンプトに関連する一般的なコマンド モード、アクセス方法、終了方法、および各モードの使用方法についての簡単な説明を示します。

表 1 CLI コマンド モード

コマンド モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	ログイン。	Router>	logout コマンドまたは exit コマンドを発行します。	<ul style="list-style-type: none"> • 端末設定の変更。 • 基本的なテストの実行。 • デバイスのステータスの表示。
特権 EXEC	ユーザ EXEC モードから、 enable コマンドを発行します。	Router#	disable コマンドまたは exit コマンドを発行して、ユーザ EXEC モードに戻ります。	<ul style="list-style-type: none"> • show コマンドおよび debug コマンドの発行。 • デバイスへのイメージのコピー。 • デバイスのリロード。 • デバイスのコンフィギュレーション ファイルの管理。 • デバイスのファイル システムの管理。
グローバル コンフィギュレーション	特権 EXEC モードから、 configure terminal コマンドを発行します。	Router (config) #	exit コマンドまたは end コマンドを発行して、特権 EXEC モードに戻ります。	デバイスの設定。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードから、 interface コマンドを発行します。	Router (config-if) #	exit コマンドを発行してグローバル コンフィギュレーション モードに戻るか、または end コマンドを発行して特権 EXEC モードに戻ります。	個々のインターフェイスの設定。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードから、 line vty コマンドまたは line console コマンドを発行します。	Router (config-line) #	exit コマンドを発行してグローバル コンフィギュレーション モードに戻るか、または end コマンドを発行して特権 EXEC モードに戻ります。	個々の端末回線の設定。

表 1 CLI コマンド モード (続き)

コマンド モード	アクセス方法	プロンプト	終了方法	モードの用途
ROM モニタ	特権 EXEC モードから、 reload コマンドを発行します。システムの起動時、最初の 60 秒以内に Break キーを押します。	rommon # > # 記号は行番号を示し、プロンプトごとに番号が増分されます。	continue コマンドを発行します。	<ul style="list-style-type: none"> 有効なイメージをロードできない場合、デフォルトの動作モードとして実行されます。 デバイスに有効なイメージがなく、デバイスを起動できない場合、フォールバック手順を利用してイメージをロードします。 電源投入またはリロードのイベント発生後、60 秒以内に Ctrl+Break シーケンスが発行された場合、パスワード回復を実行します。

表 1 CLI コマンドモード (続き)

コマンドモード	アクセス方法	プロンプト	終了方法	モードの用途
診断 (Cisco ASR 1000 シリーズ ルータ上でだけ使用可能)	次の状況では、ルータが起動されるか、または診断モードが開始されます。1 つ以上の Cisco IOS プロセスが失敗したときは、ほとんどの場合、ルータがリロードされます。 <ul style="list-style-type: none"> • transport-map コマンドを使用して、ユーザ設定のアクセス ポリシーが設定されると、ユーザは診断モードに誘導されます。 • RP 補助ポートを使用して、ルータへのアクセスが行われた場合。 • ブレーク信号 (Ctrl+C キー、Ctrl+Shift+6 キー、または send break コマンド) が入力され、このブレーク信号の受信時に診断モードを開始するようにルータが設定されていた場合。 	Router (diag) #	Cisco IOS プロセスの失敗により、診断モードが開始された場合、診断モードを終了するには、その失敗を解決し、ルータを再起動する必要があります。 transport-map のコンフィギュレーションにより、ルータが診断モードになった場合、別のポートを使用してルータにアクセスするか、または設定済みの Cisco IOS CLI に接続する方法を使用します。 RP 補助ポートを使用してルータにアクセスした場合、アクセスには別のポートを使用します。補助ポートを使用するルータへのアクセスは、カスタマーの目的に合わせた用途には使用しません。	<ul style="list-style-type: none"> • Cisco IOS ステートを含む、ルータの各種ステートの検査。 • コンフィギュレーションの置き換えまたはロールバック。 • Cisco IOS ソフトウェアまたはその他のプロセスを再起動する方法の提供。 • ハードウェア (ルータ全体、RP、ESP、SIP、SPA など) またはその他のハードウェア コンポーネントの再起動。 • FTP、TFTP、および SCP などのリモート アクセス方式を使用した、ルータに対するファイル転送、またはルータからのファイル転送。

EXEC コマンドは、ソフトウェアの再起動時に保存されません。コンフィギュレーション モードで発行するコマンドをスタートアップ コンフィギュレーションに保存できます。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する場合は、これらのコマンドをソフトウェアのリポート時に実行します。グローバル コンフィギュレーション モードは、最もレベルの高いコンフィギュレーション モードです。グローバル コンフィギュレーション モードから、プロトコル固有のモードを含む、他のさまざまなコンフィギュレーション モードを開始できます。

ROM モニタ モードは、ソフトウェアが適切にロードできない場合に使用される独立したモードです。ソフトウェアの起動時、または起動時にコンフィギュレーション ファイルが破損している場合に、有効なソフトウェア イメージが見つからなければ、ソフトウェアは ROM モニタ モードを開始することがあります。デバイスが ROM モニタ モードである間に使用できるコマンドを表示するには、疑問符記号 (?) を使用します。

```
rommon 1 > ?
alias          set and display aliases command
boot          boot up an external process
confreg       configuration register utility
```

```

cont          continue executing a downloaded image
context       display the context of a loaded image
cookie        display contents of cookie PROM in hex
.
.
.
rommon 2 >

```

次に、別のコマンドモードを示すようにコマンドプロンプトを変える例を示します。

```

Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#

```



(注) end コマンドに代わるキーは、キーボードの Ctrl+Z キーです。

対話型ヘルプ機能の使用

CLI には対話型ヘルプ機能があります。表 2 で、CLI の対話型ヘルプ コマンドの目的について説明します。

表 2 CLI 対話型ヘルプコマンド

コマンド	目的
help	任意のコマンドモードでヘルプ機能を簡単に説明します。
?	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
コマンド (一部) ?	この文字列で始まるコマンドをリストします (コマンドと疑問符の間にスペースなし)。
コマンド (一部) <Tab>	一部のみ入力したコマンド名を補完します (コマンドと <Tab> の間にスペースなし)。
コマンド?	このコマンドに関連付けられたキーワード、引数、またはその両方をリストします (コマンドと疑問符の間にスペースあり)。
コマンド キーワード?	このキーワードに関連付けられた引数をリストします (キーワードと ? の間にスペースあり)。

次に、help コマンドの使用例を示します。

help

```
Router> help
```

```
Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.
```

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
Exec commands:
  access-enable          Create a temporary access-List entry
  access-profile        Apply user-profile to interface
  access-template       Create a temporary access-List entry
  alps                  ALPS exec commands
  archive               manage archive files
<snip>
```

コマンド (一部) ?

```
Router(config)# zo?
zone zone-pair
```

コマンド (一部) <Tab>

```
Router(config)# we<Tab> webvpn
```

コマンド?

```
Router(config-if)# pppoe ?
enable          Enable pppoe
max-sessions    Maximum PPPOE sessions
```

コマンド キーワード?

```
Router(config-if)# pppoe enable ?
group attach a BBA group
<cr>
```

コマンド シンタックスの概要

コマンド シンタックスは、コマンドの形式であり、CLI ではこの形式で入力する必要があります。コマンドは、コマンド、キーワード、および引数の名前で作成されます。キーワードは、文字通り使用される英数字の文字列です。引数は、ユーザが指定する必要がある値のプレースホルダーです。キーワードおよび引数は必須の場合も、任意の場合もあります。

特定の表記法を用いて、シンタックスおよびコマンドの要素に関する情報を表します。表 3 には、これらの表記法について説明します。

表 3 CLI シンタックス表記法

記号/テキスト	機能	注意事項
<> (山形カッコ)	オプションが引数であることを示します。	山形カッコを用いずに引数を表示することもあります。
A.B.C.D.	ドット付き 10 進 IP アドレスを入力する必要があることを示します。	山形カッコ (<>) を使用していても、IP アドレスが引数であることを常に示しているとは限りません。
WORD (すべて大文字)	1 語を入力する必要があることを示します。	山形カッコ (<>) を使用していても、WORD が引数であることを常に示しているとは限りません。

表 3 CLI シンタックス表記法 (続き)

記号/テキスト	機能	注意事項
LINE (すべて大文字)	2 語以上入力する必要があることを示します。	山形カッコ (<>) を使用していても、LINE が引数であることを常に示しているとは限りません。
<cr> (復帰)	使用可能なキーワードおよび引数のリストの最後を示します。また、キーワードおよび引数が任意であるときに表示されます。<cr> が唯一のオプションである場合、分岐の最後に到達しています。または、分岐のないコマンドであれば、コマンドの最後に到達しています。	—

次に、シンタックスの表記法の例を示します。

```
Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>

Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
```

イネーブル パスワードおよびイネーブル シークレット パスワードの概要

一部の特権 EXEC コマンドは、システムに影響を及ぼす処理に使用します。不正使用を防ぐため、これらのコマンドにはパスワードを設定することをお勧めします。イネーブル (暗号化なし) とイネーブル シークレット (暗号化あり) の 2 種類のパスワードを設定できます。次のコマンドは、これらのパスワードを設定します。次のコマンドをグローバル コンフィギュレーション モードで発行します。

- **enable password**
- **enable secret password**

イネーブル シークレット パスワードは暗号化され、イネーブル パスワードよりも安全であるため、イネーブル シークレット パスワードの使用が推奨されます。イネーブル シークレット パスワードを使用する場合、テキストが `config.text` ファイルに書き込まれる前に暗号化 (判読できないように) します。イネーブル パスワードを使用する場合、入力されたとおりに (判読できる状態で) テキストが `config.text` ファイルに書き込まれます。

どちらの種類のパスワードも大文字と小文字が区別され、1 ~ 25 文字の大文字と小文字の英数字を使用できます。パスワードを数字で始めることもできます。スペースもパスワードに有効な文字です。たとえば、「two words」は有効なパスワードです。先行するスペースは無視されますが、末尾のスペースは認識されます。



(注)

どちらのパスワード コマンドにも、単体の整数値である数字のキーワードがあります。パスワードの最初の文字に数字を選択し、その後にスペースを続けた場合、システムはその数字を、数字のキーワードであり、パスワードには含まれないものとして読み取ります。

両方のパスワードを設定した場合、イネーブル シークレット パスワードがイネーブル パスワードよりも優先されます。

パスワードを削除するには、**no enable password** コマンドまたは **no enable secret password** コマンドの **no** 形式を使用します。

シスコ製品のパスワードの回復手順の詳細については、次を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

コマンド履歴機能の使用

コマンド履歴機能では、コマンド履歴バッファに、セッション中に入力するコマンドを保存します。保存するコマンド数のデフォルトは 10 ですが、0 ~ 256 の範囲で数を設定できます。このコマンド履歴機能は、特に長いコマンドや複雑なコマンドを再呼び出しする場合に便利です。

ターミナル セッション用の履歴バッファに保存するコマンド数を変更するには、**terminal history size** コマンドを発行します。

```
Router# terminal history size num
```

コマンド履歴バッファは、同じデフォルト値および設定のオプションを用いて、ライン コンフィギュレーション モードでも使用できます。ライン コンフィギュレーション モードでターミナル セッションのコマンド履歴バッファ サイズを設定するには、**history** コマンドを発行します。

```
Router(config-line)# history [size num]
```

履歴バッファからコマンドを再呼び出しするには、次の方法を使用します。

- **Ctrl+P** キーまたは上矢印キーを押す：最近使用したコマンドからコマンドを再呼び出しします。このキーを連続して繰り返すと、順に古いコマンドを再呼び出しします。
- **Ctrl+N** キーまたは下矢印キーを押す：**Ctrl+P** キーまたは上矢印キーを使用してコマンドを再呼び出した後の履歴バッファの中から、最近使用したコマンドを再呼び出しします。このキーを連続して繰り返すと、順に新しいコマンドを再呼び出しします。



(注) 矢印キーは、VT100 などの ANSI 互換端末上でだけ機能します。

- ユーザ EXEC モードまたは特権 EXEC モードでの **show history** コマンドの発行：最近入力したコマンドをリストします。表示されるコマンド数は、**terminal history size** コマンドおよび **history** コマンドの設定によります。

コマンド履歴機能はデフォルトでイネーブルに設定されています。ターミナル セッションでこの機能をディセーブルにするには、ユーザ EXEC モードまたは特権 EXEC モードで **terminal no history** コマンドを発行するか、ライン コンフィギュレーション モードで **no history** コマンドを発行します。

コマンドの省略

コマンドを実行するために、常に完全なコマンド名を入力する必要はありません。CLI は、省略形でも一意に識別できるだけの十分な文字が含まれていれば、省略されたコマンドを認識します。たとえば、**show version** コマンドは、**sh ver** として省略できます。**s** は **show**、**set**、または **systat** を意味する可能性があるため、**s ver** として省略することはできません。また、**show** コマンドにはキーワードとして **version** の他に **vrp** があるため、**sh v** の省略形は有効ではありません（コマンドおよびキーワードの例は、Cisco IOS リリース 12.4(13)T によるものです）。

CLI コマンドのエイリアスの使用

時間を節約し、何度も同じコマンド入力の繰り返しを省くために、コマンドのエイリアスを使用できます。コマンドラインで実行可能であればどのコマンドでも、実行するようにエイリアスを設定できますが、エイリアスでは、モード間の移動、パスワードの入力、対話型機能の実行のいずれも行いません。

表 4 に、デフォルトのコマンドエイリアスを示します。

表 4 デフォルトのコマンドエイリアス

コマンドエイリアス	元のコマンド
h	help
lo	logout
p	ping
s	show
u または un	undebg
w	where

コマンドエイリアスを作成するには、グローバル コンフィギュレーション モードで **alias** コマンドを発行します。コマンドのシンタックスは、**alias mode command-alias original-command** です。次に、いくつかの例を示します。

- Router(config)# **alias exec prt partition** : 特権 EXEC モード
- Router(config)# **alias configure sb source-bridge** : グローバル コンフィギュレーション モード
- Router(config)# **alias interface rl rate-limit** : インターフェイス コンフィギュレーション モード

デフォルトおよびユーザによって作成されたエイリアスの両方を表示するには、**show alias** コマンドを発行します。

alias コマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html

コマンドの no 形式および default 形式の使用

ほとんどのコンフィギュレーション コマンドは **no** 形式があり、この形式を使用して、コマンドをデフォルト値に戻したり、フィーチャや機能をディセーブルにしたりします。たとえば、**ip routing** コマンドはデフォルトでイネーブルに設定されています。このコマンドをディセーブルにするには、**no ip routing** コマンドを発行します。IP ルーティングを再びイネーブルにするには、**ip routing** コマンドを発行します。

コンフィギュレーション コマンドはまた、**default** 形式を持つ場合もあり、この形式を使用して、コマンドの設定をデフォルト値に戻します。デフォルトでディセーブルに設定されているコマンドの場合、**default** 形式を使用することで、コマンドの **no** 形式を使用する場合と同様の作用があります。デフォルトでイネーブルに設定されていて、デフォルト設定を持つコマンドの場合、**default** 形式はコマンドをイネーブルにし、設定をデフォルト値に戻します。お使いのシステム上で使用できる **default** コマンドについては、**default ?** を コマンドライン インターフェイスの適切なコマンド モードで入力します。

no 形式は、Cisco IOS コマンド リファレンスのコマンドのページに記載されています。**default** 形式は通常、**default** 形式がコマンドのプレーン形式および **no** 形式とは異なる機能を実行する場合にだけ、コマンド ページに記載されます。

コマンド ページには、多くの場合に「コマンドのデフォルト」に関する項が設けられています。コマンドのデフォルトに関する項には、設定コマンドに対してコマンドが使用されないときの設定状態、または EXEC コマンドに対してオプションのキーワードまたは引数が指定されていないときのコマンドの使用結果が記載されています。

debug コマンドの使用

debug コマンドは、ネットワーク上の問題に対するトラブルシューティングを助ける広範な出力を生成します。これらのコマンドは、Cisco IOS ソフトウェア内の多くのフィーチャおよび機能に使用できます。**debug** コマンドの一部として、**debug all**、**debug aaa accounting**、および **debug mpls packets** があります。デバイスとの Telnet セッション中に **debug** コマンドを使用する場合は、最初に **terminal monitor** コマンドを入力する必要があります。デバッグを完全にオフにするには、**undebug all** コマンドを入力する必要があります。

debug コマンドに関する詳細については、『Cisco IOS Debug Command Reference』(http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html) を参照してください。



注意

デバッグは、デバイスを使用不可にする可能性のある、高プライオリティで CPU 使用率の高いプロセスです。**debug** コマンドを使用するのは、特定の問題に対するトラブルシューティングの場合だけです。デバッグの実行に最適なのは、ネットワーク トラフィックが少ない期間で、かつネットワークを使用してやりとりしているユーザが少ないときです。このような期間にデバッグすることで、**debug** コマンド処理のオーバーヘッドにより、ネットワーク パフォーマンス、ユーザ アクセス、または応答時間に影響を及ぼす可能性を低減します。

出力修飾子を使用する出力のフィルタリング

コマンドの多くは、複数の画面にわたり表示する大量の出力を生成します。出力修飾子を使用して、この出力をフィルタし、確認の必要な情報だけを表示できます。

次の 3 つの出力修飾子を使用できます。

- **begin regular-expression** : 正規表現の一致を検出した最初の行とそれに続くすべての行を表示します。
- **include regular-expression** : 正規表現の一致を検出したすべての行を表示します。
- **exclude regular-expression** : 正規表現の一致を検出した行以外のすべての行を表示します。

これらの出力修飾子のうち 1 つを使用する場合は、コマンドの後に続けて、検索またはフィルタするパイプ記号 (|)、修飾子、および正規表現を入力します。正規表現は大文字と小文字を区別する英数字のパターンです。1 文字、1 数字、語句、またはさらに複雑な文字列を使用できます。

次に、**show interface** コマンドの出力をフィルタして、「protocol」の表現を含む行だけを表示する例を示します。

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

CLI エラー メッセージの概要

CLI 使用時にいくつかのエラー メッセージが表示されることがあります。表 5 に、一般的な CLI エラー メッセージを示します。

表 5 一般的な CLI エラー メッセージ

エラー メッセージ	意味	ヘルプの利用方法
% Ambiguous command: "show con"	コマンドを認識するのに十分な文字列を入力していません。	コマンドの後に続けてスペースと疑問符 (?) を再入力します。コマンドに対して入力可能なキーワードが表示されます。
% Incomplete command.	コマンドに必要なキーワードまたは値をすべて入力していません。	コマンドの後に続けてスペースと疑問符 (?) を再入力します。コマンドに対して入力可能なキーワードが表示されます。
% Invalid input detected at "^" marker.	コマンドを誤って入力しています。キャレット (^) は、エラーの場所を示します。	疑問符 (?) を入力して、このコマンドモードで使用可能なすべてのコマンドを表示します。コマンドに対して入力可能なキーワードが表示されます。

システム エラー メッセージの詳細については、『[Cisco IOS Release 12.4T System Message Guide](#)』を参照してください。

コンフィギュレーションに対する変更の保存

デバイスのコンフィギュレーションに対して行った変更を保存するには、**copy running-config startup-config** コマンドまたは **copy system:running-config nvram:startup-config** コマンドを発行する必要があります。これらのコマンドを発行すると、コンフィギュレーションに対して行った変更がスタートアップ コンフィギュレーションに保存されます。保存されるのは、ソフトウェアのリロード時、デバイスの電源がオフになったとき、または電源が遮断された場合です。次に、**copy running-config startup-config** コマンドのシンタックスを表示する例を示します。

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

Enter キーを押して **startup-config** のファイル名 (デフォルト) を使用するか、新しいファイル名を入力して Enter キーを押し、その名前を使用します。次の出力が表示され、コンフィギュレーションが保存されたことを示します。

```
Building configuration...  
[OK]  
Router#
```

ほとんどのプラットフォームで、コンフィギュレーションは NVRAM に保存されます。クラス A フラッシュ ファイル システムを備えるプラットフォームの場合、コンフィギュレーションは CONFIG_FILE 環境変数によって指定された場所に保存されます。CONFIG_FILE 変数のデフォルトは NVRAM になります。

その他の情報

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using the Cisco IOS Command-Line Interface」セクション
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product/Technology Support
<http://www.cisco.com/go/techdocs>
- Cisco.com のサポートサイト（タスクまたは製品によるマニュアル検索もできます）
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center（ダウンロード/ツール/ライセンス、登録、アドバイザリ、一般情報）（Cisco.com のユーザ ID およびパスワードが必要）
<http://www.cisco.com/kobayashi/sw-center/>
- エラー メッセージ デコーダ。Cisco IOS ソフトウェアのエラー メッセージを調査し解決を支援するツールです。
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool。Cisco IOS コマンドの詳しい説明の検索を支援するツールです（Cisco.com のユーザ ID およびパスワードが必要）。
<http://tools.cisco.com/Support/CLILookup>
- Output Interpreter。サポート対象の **show** コマンドのコマンド出力を分析するトラブルシューティング ツールです。
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2008–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2010, シスコシステムズ合同会社。
All rights reserved.



双方向フォワーディング検出

このドキュメントでは、Bidirectional Forwarding Detection (BFD; 双方向フォワーディング検出) 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、複数のルーティング プロトコルの hello メカニズムの可変レートではなく、統一レートで転送パス障害を検出でき、ネットワークのプロファイリングおよび計画が簡単になり、コンバージェンス時間が一貫して予測できます。

機能情報の検索

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報および警告については、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。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[双方向フォワーディング検出の機能情報](#)」(P.51)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 Cisco IOS および Catalyst OS 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 には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

- 「[双方向フォワーディング検出の前提条件](#)」(P.2)
- 「[双方向フォワーディング検出の制約事項](#)」(P.2)
- 「[双方向フォワーディング検出について](#)」(P.4)
- 「[双方向フォワーディング検出の設定方法](#)」(P.10)
- 「[双方向フォワーディング検出の設定例](#)」(P.33)
- 「[参考資料](#)」(P.48)
- 「[双方向フォワーディング検出の機能情報](#)」(P.51)

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 ソフトウェアでの 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 \(P.2\)](#)」を参照してください。

双方向フォワーディング検出の制約事項

- Cisco IOS リリース 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 リリース 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。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 リリース 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 リリース 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 Border Gateway プロトコル (BGP; ボーダー ゲートウェイ プロトコル)、Enhanced IGRP (EIGRP)、Intermediate System-to-Intermediate System (IS-IS)、および Open Shortest Path First (OSPF) だけです。Cisco IOS リリース 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 リリース 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 リリース 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 リリース 12.4(11)T では、シスコの BFD 実装でホットスタンバイ ルーティング 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 リリース 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 リリース 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 リリース 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の BFD サポートを確認し、プラットフォームとハードウェアの正確な制約事項を知るには、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 リリース 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) 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、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.
```

- 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 リリース 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。

Cisco IOS リリース 12.2(33)SX12 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 **no ip redirects** 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。



(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。

双方向フォワーディング検出について

BFD を設定する前に、次の項の内容について理解しておく必要があります。

- 「[BFD の動作](#)」 (P.4)
- 「[障害検出に BFD を使用することの利点](#)」 (P.9)

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 レベルおよびルーティング 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。これは、ルータ間の BFD ネイバー セッションをアクティブにして維持するための、2 台のシステム間の BFD 制御パケットの送信に依存します。したがって、BFD セッションを作成するには、両方のシステムで (または BFD ピアで) BFD を設定する必要があります。適切な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 がイネーブルになっている場合、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、ネゴシエートされた間隔で BFD ピアが互いに BFD 制御パケットの送信を開始します。

ここでは、次の内容について説明します。

- 「[ネイバー関係](#)」 (P.5)
- 「[BFD の障害検出](#)」 (P.5)
- 「[BFD バージョンの相互運用性](#)」 (P.6)
- 「[Cisco 12000 ルータでの BFD サポート](#)」 (P.6)
- 「[BFD セッションの制限](#)」 (P.7)
- 「[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](#)」 (P.7)
- 「[VPN Routing and Forwarding \(VRF; VPN ルーティングおよび転送\) インターフェイスのための BFD サポート](#)」 (P.7)
- 「[ステートフル スイッチオーバー機能を持つノンストップフォワーディングのための BFD サポート](#)」 (P.7)
- 「[ステートフル スイッチオーバーのための BFD サポート](#)」 (P.8)
- 「[スタティック ルーティングのための BFD サポート](#)」 (P.9)

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。図 1 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)。

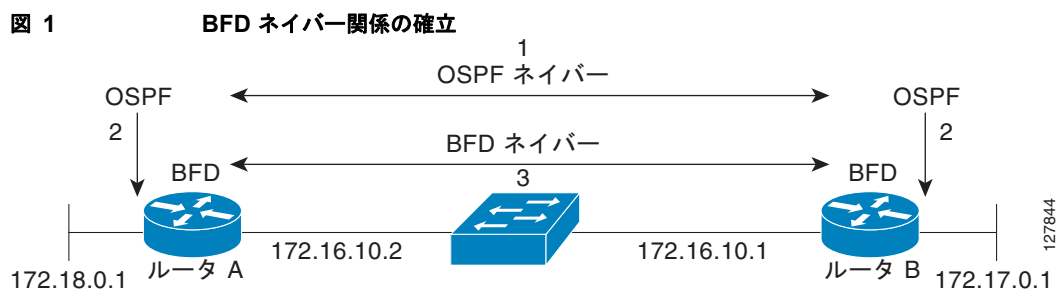
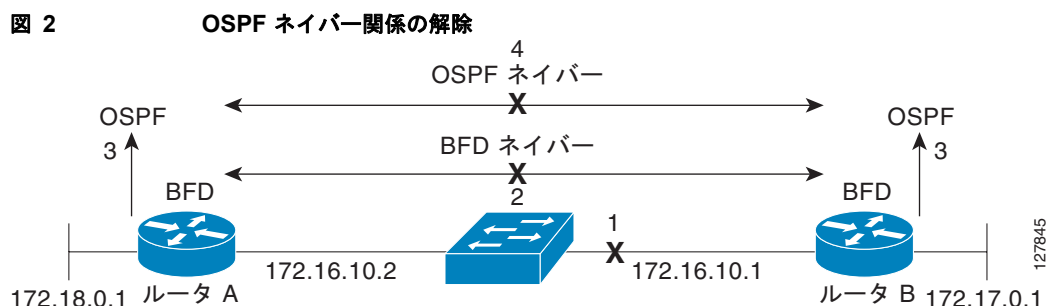


図 2 に、ネットワーク (1) で障害が発生した場合を示します。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます (2)。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します (3)。ローカル OSPF プロセスは OSPF ネイバー関係を解除します (4)。代替パスを使用できる場合、ルータはただちにコンバージェンスを開始します。



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。
- 通常、BFD はどのプロトコル レイヤでも使用できます。ただし、Cisco IOS リリース 12.0(31)S および 12.4(4)T 用のシスコの BFD 実装では、特に BGP、EIGRP、IS-IS、および OSPF ルーティング プロトコルのレイヤ 3 クライアントだけがサポートされます。Cisco IOS リリース 12.2(33)SRC の場合、スタティック ルーティングに BFD がサポートされます。
- Cisco IOS リリース 12.2(18)SXЕ 用のシスコの BFD 実装では、レイヤ 3 クライアントおよび EIGRP、IS-IS、および OSPF ルーティング プロトコルだけがサポートされます。BGP ルーティング プロトコルはサポートされません。

- Cisco IOS リリース 12.2(18)SXE、12.0(31)S、および 12.4(4)T のシスコの BFD 実装では、シスコのデバイスが複数のクライアントプロトコルに 1 つの BFD セッションを使用します。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

Cisco IOS リリース 12.4(9)T では BFD バージョン 1 および BFD バージョン 0 がサポートされます。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。**show bfd neighbors [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：例](#)」(P.33) 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 Route Processor (RP; ルートプロセッサ) 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](#)」(P.6)
- 「[LC の BFD プロセス](#)」(P.7)

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 リリース 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 リリース 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 Routing and Forwarding (VRF; VPN ルーティングおよび転送) インターフェイスのための BFD サポート

Cisco IOS リリース 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 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 Routing and Forwarding (VRF; VPN ルーティングおよび転送) 対応に拡張されています。

ステートフル スイッチオーバー機能を持つノンストップ フォワーディングのための BFD サポート

通常、ネットワークング 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 ネットワークング 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 からの制御とみなされます。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 Forwarding Information Base (FIB; 転送情報ベース) 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、ネットワーク 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。

Cisco IOS リリース 12.2(33)SRC では、計画的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。

Cisco IOS リリース 12.2(33)SB では、BFD が SSO 対応ではなく、NSF/SSO でサポートされません。これらの機能は組み合わせて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。

ステートフル スイッチオーバーのための 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 (CEF) 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 ルーティングのための 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みなされ、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。

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。

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。

双方向フローディング検出の設定方法

インターフェイスで BFD を設定して、BFD プロセスを開始します。BFD プロセス が開始されると、隣接するデータベースにエントリが作成されません。つまり、BFD 制御パケットが送受信されません。Cisco IOS リリース 12.4(9)T の BFD バージョン 1 でサポートされない BFD エコー モードは、デフォルトではイネーブルです。BFD 制御パケットに加えて、BFD エコー パケットが送受信されます。適用可能なルーティング プロトコルの BFD サポートを設定すると、隣接作成が実行されます。ここでは、次の手順について説明します。

- 「インターフェイスでの BFD セッション パラメータの作成」 (P.10) (必須)
- 「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」 (P.11) (必須)
- 「スタティック ルーティングのための BFD サポートの設定」 (P.25) (任意)
- 「BFD エコー モードの設定」 (P.27) (任意)
- 「BFD の監視とトラブルシューティング」 (P.29) (任意)

インターフェイスでの BFD セッション パラメータの作成

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. **interface type number**
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： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 number 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。

	コマンドまたはアクション	目的
ステップ 4	<pre>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</pre> <p>例： Router(config-if)# bfd interval 50 min_rx 50 multiplier 5</p>	インターフェイスで BFD をイネーブルにします。
ステップ 5	<pre>end</pre> <p>例： Router(config-if)# end</p>	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。

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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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 リリース 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」 (P.11) (任意)
- 「EIGRP に対する BFD サポートの設定」 (P.13) (任意)
- 「IS-IS に対する BFD サポートの設定」 (P.15) (任意)
- 「OSPF に対する BFD サポートの設定」 (P.19) (任意)
- 「HSRP に対する BFD サポートの設定」 (P.23) (任意)

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。

前提条件

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作成](#)」(P.10) を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp *as-tag***
4. **neighbor *ip-address* fall-over bfd**
5. **end**
6. **show bfd neighbors [details]**
7. **show ip bgp neighbor**

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 bgp <i>as-tag</i> 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 <i>ip-address</i> fall-over bfd 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。

コマンドまたはアクション	目的
<p>ステップ 6 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors detail</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズ ルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 7 <code>show ip bgp neighbor</code></p> <p>例： Router# show ip bgp neighbor</p>	<p>(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。</p>

次の作業

BFD の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング \(P.29\)](#)」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 \(P.13\)](#)」
- 「[IS-IS に対する BFD サポートの設定 \(P.15\)](#)」
- 「[OSPF に対する BFD サポートの設定 \(P.19\)](#)」
- 「[HSRP に対する BFD サポートの設定 \(P.23\)](#)」

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 **bfd all-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 **bfd interface type number** 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。

前提条件

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作成 \(P.10\)](#)」を参照してください。

制約事項

EIGRP に対する BFD は、Cisco IOS リリース 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. **configure terminal**
3. **router eigrp as-number**
4. **bfd all-interfaces**
または
bfd interface type number
5. **end**
6. **show bfd neighbors [details]**
7. **show ip eigrp interfaces [type number] [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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 eigrp 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	bfd all-interfaces または bfd interface type number 例： Router(config-router)# bfd all-interfaces または 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。

コマンドまたはアクション	目的
<p>ステップ 6 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズのルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 7 <code>show ip eigrp interfaces [type number] [as-number] [detail]</code></p> <p>例： Router# show ip eigrp interfaces detail</p>	<p>(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。</p>

次の作業

BFD の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング \(P.29\)](#)」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。

- [「BGP に対する BFD サポートの設定」 \(P.11\)](#)
- [「IS-IS に対する BFD サポートの設定」 \(P.15\)](#)
- [「OSPF に対する BFD サポートの設定」 \(P.19\)](#)
- [「HSRP に対する BFD サポートの設定」 \(P.23\)](#)

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。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 disable** コマンドを使用して、1つ以上のインターフェイス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** コマンドを使用して、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。

- [「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」 \(P.16\)](#)
- [「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」 \(P.18\)](#)

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作成](#)」(P.10) を参照してください。

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. **configure terminal**
3. **router isis [area-tag]**
4. **bfd all-interfaces**
5. **exit**
6. **interface type number**
7. **ip router isis [tag]**
8. **isis bfd [disable]**
9. **end**
10. **show bfd neighbors [details]**
11. **show clns interface**

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。 <ul style="list-style-type: none">• プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 isis 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	bfd all-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。

コマンドまたはアクション	目的
<p>ステップ 5 <code>exit</code></p> <p>例： Router(config-router)# exit</p>	<p>(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。</p>
<p>ステップ 6 <code>interface type number</code></p> <p>例： Router(config)# interface fastethernet 6/0</p>	<p>(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。</p>
<p>ステップ 7 <code>ip router isis [tag]</code></p> <p>例： Router(config-if)# ip router isis tag1</p>	<p>(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。</p>
<p>ステップ 8 <code>isis bfd [disable]</code></p> <p>例： Router(config-if)# isis bfd</p>	<p>(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。</p> <p>(注) 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。</p>
<p>ステップ 9 <code>end</code></p> <p>例： Router(config-if)# end</p>	<p>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。</p>
<p>ステップ 10 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズ ルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 11 <code>show clns interface</code></p> <p>例： Router# show clns interface</p>	<p>(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。</p>

次の作業

BFD の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング](#)」(P.29) 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](#)」(P.18) 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。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip router isis [tag]`
5. `isis bfd [disable]`
6. `end`
7. `show bfd neighbors [details]`
8. `show clns interface`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 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	<code>interface type number</code> 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	<code>ip router isis [tag]</code> 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。
ステップ 5	<code>isis bfd [disable]</code> 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 bfd all-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	<code>end</code> 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。

コマンドまたはアクション	目的
<p>ステップ 7 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズ ルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 8 <code>show clns interface</code></p> <p>例： Router# show clns interface</p>	<p>(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。</p>

次の作業

BFD の監視とメンテナンスの詳細については、「[BFD の監視とトラブルシューティング](#)」(P.29) 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。

- [「BGP に対する BFD サポートの設定」](#) (P.11)
- [「EIGRP に対する BFD サポートの設定」](#) (P.13)
- [「OSPF に対する BFD サポートの設定」](#) (P.19)
- [「HSRP に対する BFD サポートの設定」](#) (P.23)

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 **bfd all-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 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」](#) (P.20) (任意)
- [「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」](#) (P.22) (任意)

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、「[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](#)」(P.22) を参照してください。

前提条件

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作成](#)」(P.10) を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospf process-id**
4. **bfd all-interfaces**
5. **exit**
6. **interface type number**
7. **ip ospf bfd [disable]**
8. **end**
9. **show bfd neighbors [details]**
10. **show ip ospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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	bfd all-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。

コマンドまたはアクション	目的
<p>ステップ 5 <code>exit</code></p> <p>例： Router(config-router)# exit</p>	<p>(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。</p>
<p>ステップ 6 <code>interface type number</code></p> <p>例： Router(config)# interface fastethernet 6/0</p>	<p>(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。</p>
<p>ステップ 7 <code>ip ospf bfd [disable]</code></p> <p>例： Router(config-if)# ip ospf bfd disable</p>	<p>(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。</p> <p>(注) 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 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。</p>
<p>ステップ 8 <code>end</code></p> <p>例： Router(config-if)# end</p>	<p>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。</p>
<p>ステップ 9 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors detail</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズ ルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 10 <code>show ip ospf</code></p> <p>例： Router# show ip ospf</p>	<p>(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。</p>

次の作業

BFD の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング \(P.29\)](#)」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。

- 「[BGP に対する BFD サポートの設定 \(P.11\)](#)」
- 「[EIGRP に対する BFD サポートの設定 \(P.13\)](#)」
- 「[IS-IS に対する BFD サポートの設定 \(P.15\)](#)」
- 「[HSRP に対する BFD サポートの設定 \(P.23\)](#)」

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。

前提条件

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作成](#)」(P.10) を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ip ospf bfd [disable]**
5. **end**
6. **show bfd neighbors [details]**
7. **show ip ospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 <i>type number</i> 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	ip ospf bfd [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 bfd all-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。

コマンドまたはアクション	目的
<p>ステップ 5 <code>end</code></p> <p>例： Router(config-if)# end</p>	<p>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。</p>
<p>ステップ 6 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>(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。</p> <p>(注) Cisco 12000 シリーズ ルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 7 <code>show ip ospf</code></p> <p>例： Router# show ip ospf</p>	<p>(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。</p>

次の作業

BFD の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング \(P.29\)](#)」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。

- 「[BGP に対する BFD サポートの設定 \(P.11\)](#)」
- 「[EIGRP に対する BFD サポートの設定 \(P.13\)](#)」
- 「[IS-IS に対する BFD サポートの設定 \(P.15\)](#)」
- 「[HSRP に対する BFD サポートの設定 \(P.23\)](#)」

HSRP に対する BFD サポートの設定

Hot-Standby Routing Protocol (HSRP) に対して BFD サポートをイネーブルにするには、このタスクを実行します。HSRP ピアに対して 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。

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。

前提条件

- 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. configure terminal
3. ip cef [distributed]
4. interface *type number*
5. ip address *ip-address mask*
6. standby [*group-number*] ip [*ip-address* [**secondary**]]
7. standby bfd
8. exit
9. standby bfd all-interfaces
10. exit
11. show standby [**neighbors**]

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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	ip cef [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 <i>type number</i> 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	ip address <i>ip-address mask</i> 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 [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.11	HSRP をアクティブにします。

	コマンドまたはアクション	目的
ステップ 7	standby bfd 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	standby bfd all-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。
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	show standby neighbors 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 の監視とトラブルシューティングの詳細については、「[BFD の監視とトラブルシューティング](#)」(P.29) 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。

- 「[BGP に対する BFD サポートの設定](#)」(P.11)
- 「[EIGRP に対する BFD サポートの設定](#)」(P.13)
- 「[IS-IS に対する BFD サポートの設定](#)」(P.15)
- 「[OSPF に対する BFD サポートの設定](#)」(P.19)

スタティック ルーティングのための 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、「[スタティック ルーティングのための BFD サポートの設定：例](#)」(P.47) を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask**
5. **bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier**
6. **ip route static bfd [vrf vrf-name] interface-type interface-number gateway**

7. `ip route prefix mask {ip-address | interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]`
8. `end`
9. `show ip static route`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 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	<code>interface type number</code> 例： Router(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	<code>ip address ip-address mask</code> 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	<code>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</code> 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	<code>ip route static bfd [vrf vrf-name] interface-type interface-number gateway</code> 例： Router(config-if)# ip route static bfd Serial 2/0 10.201.201.2	スタティック ルートの BFD ネイバーを指定します。 • BFD サポートは直接接続されたネイバーだけに存在するため、 <code>interface-type interface-number</code> および <code>gateway</code> 引数は必須です。
ステップ 7	<code>ip route prefix mask {ip-address interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent track number] [tag tag]</code> 例： Router(config-if)# ip route 10.0.0.0 255.0.0.0 Serial 2/0 10.201.201.2	スタティック ルートの BFD 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 8	<pre>end</pre> <p>例:</p> <pre>Router(config-if)# end</pre>	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	<pre>show ip static route</pre> <p>例:</p> <pre>Router# show ip static route</pre>	(任意) スタティック プロセスのローカル Routing Information Base (RIB) 情報を表示します。

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。エコー モードを設定するには、その前に次の概念を理解しておく必要があります。

- 「BFD エコー モード」 (P.27)
- 「前提条件」 (P.27)
- 「制約事項」 (P.28)

BFD エコー モード

BFD エコー モードを実行する利点

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。

非対称性のないエコー モード

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、**no ip redirects** コマンドを入力して、Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) 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作成](#)」 (P.10) を参照してください。

制約事項

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 リリース 12.4(9)T および 12.2(33)SRA だけで使用できます。

ここでは、BFD エコー モードの次の設定タスクについて説明します。

- 「[BFD 低速タイマーの設定](#)」 (P.28)
- 「[非対称性のない BFD エコー モードのディセーブル化](#)」 (P.28)

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. **configure terminal**
3. **bfd slow-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： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 slow-timer milliseconds 例： Router(config)# bfd slow-timer 12000	BFD の slow timer を設定します。
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。ルータからエコー パケットが送信されず、ルータはネイバー ルータが受信した 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. configure terminal
3. bfd echo
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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 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 echo 例： Router(config)# no bfd echo	BFD エコー モードをイネーブルにします。 • 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 モードを終了して、特権 EXEC モードに戻ります。

BFD の監視とトラブルシューティング

ここでは、メンテナンス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](#)」(P.4) 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 の監視とトラブルシューティングについて説明します。

- 「[Catalyst 7600 シリーズ ルータの監視とトラブルシューティング](#)」(P.29)
- 「[Catalyst 12000 シリーズ ルータの監視とトラブルシューティング](#)」(P.30)
- 「[Cisco 10720 インターネット ルータに対する BFD の監視とトラブルシューティング](#)」(P.32)

Catalyst 7600 シリーズ ルータの監視とトラブルシューティング

Catalyst 7600 シリーズ ルータの監視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. `show bfd neighbors [details]`
3. `debug bfd [packet | event]`

手順の詳細

コマンドまたはアクション	目的
<p>ステップ 1 <code>enable</code></p> <p>例： Router> enable</p>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> • プロンプトが表示されたら、パスワードを入力します。
<p>ステップ 2 <code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>(任意) BFD 隣接関係データベースを表示します。</p> <ul style="list-style-type: none"> • 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。 <p>(注) Cisco 12000 シリーズのルータで show bfd neighbors details 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 show bfd neighbors details コマンドの出力に表示されません。</p>
<p>ステップ 3 <code>debug bfd [packet event]</code></p> <p>例： Router# debug bfd packet</p>	<p>(任意) BFD パケットのデバッグ情報を表示します。</p>

Catalyst 12000 シリーズ ルータの監視とトラブルシューティング

Catalyst 12000 シリーズ ルータの監視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. `show bfd neighbors [details]`
4. `show monitor event-trace bfd [all]`
5. `debug bfd event`
6. `debug bfd packet`
7. `debug bfd ipc-error`
8. `debug bfd ipc-event`
9. `debug bfd oir-error`

10. debug bfd oir-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	<p><code>enable</code></p> <p>例： Router> enable</p>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<p><code>attach slot-number</code></p> <p>例： Router# attach 6</p>	<p>特定のラインカードで監視とトラブルシューティング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。</p> <ul style="list-style-type: none"> 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。 <p>(注) Cisco 12000 シリーズのルータで show bfd neighbors details 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。</p>
ステップ 3	<p><code>show bfd neighbors [details]</code></p> <p>例： Router# show bfd neighbors details</p>	<p>BFD 隣接関係データベースを表示します。</p> <ul style="list-style-type: none"> 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。 <p>(注) ラインカードで入力すると、登録されたプロトコルが show bfd neighbors details コマンドの出力に表示されません。</p>
ステップ 4	<p><code>show monitor event-trace bfd [all]</code></p> <p>例： Router# show monitor event-trace bfd all</p>	<p>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。</p>
ステップ 5	<p><code>debug bfd event</code></p> <p>例： Router# debug bfd event</p>	<p>BFD 状態遷移のデバッグ情報を表示します。</p>
ステップ 6	<p><code>debug bfd packet</code></p> <p>例： Router# debug bfd packet</p>	<p>BFD 制御パケットのデバッグ情報を表示します。</p>
ステップ 7	<p><code>debug bfd ipc-error</code></p> <p>例： Router# debug bfd ipc-error</p>	<p>RP および LC でのデバッグ情報と IPC エラーを表示します。</p>

	コマンドまたはアクション	目的
ステップ 8	<pre>debug bfd ipc-event</pre> <p>例： Router# debug bfd ipc-event</p>	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	<pre>debug bfd oir-error</pre> <p>例： Router# debug bfd oir-error</p>	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	<pre>debug bfd oir-event</pre> <p>例： Router# debug bfd oir-event</p>	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。

Cisco 10720 インターネット ルータに対する BFD の監視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 ルータの監視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. show bfd neighbors [details]
3. debug bfd event
4. debug bfd packet

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<pre>enable</pre> <p>例： Router> enable</p>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<pre>show bfd neighbors [details]</pre> <p>例： Router# show bfd neighbors details</p>	<p>(任意) BFD 隣接関係データベースを表示します。</p> <ul style="list-style-type: none"> • 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。 <p>(注) ラインカードで入力すると、登録されたプロトコルが show bfd neighbors details コマンドの出力に表示されません。</p>

	コマンドまたはアクション	目的
ステップ 3	<code>debug bfd event</code> 例： <code>Router# debug bfd event</code>	(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	<code>debug bfd packet</code> 例： <code>Router# debug bfd packet</code>	(任意) BFD 制御パケットのデバッグ情報を表示します。

双方向フォワーディング検出の設定例

ここでは、次の設定例について説明します。

- 「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 : 例」 (P.33)
- 「OSPF ネットワークでの BFD の設定 : 例」 (P.38)
- 「BGP ネットワークでの BFD の設定 : 例」 (P.42)
- 「IS-IS ネットワークでの BFD の設定 : 例」 (P.45)
- 「HSRP ネットワークでの BFD の設定 : 例」 (P.46)
- 「スタティック ルーティングのための BFD サポートの設定 : 例」 (P.47)

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 : 例

Cisco IOS リリース 12.4(9)T の例

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 0/1 がルータ B のファストイーサネット インターフェイス 0/1 と同じネットワークに接続されます。ルータ B のファストイーサネット インターフェイス 0/1 が、ルータ C のファストイーサネット インターフェイス 0/1 と同じネットワークに接続されます。

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。

図 3 V1 または V0 を実行する 3 台の BFD ネイバーがある EIGRP ネットワーク

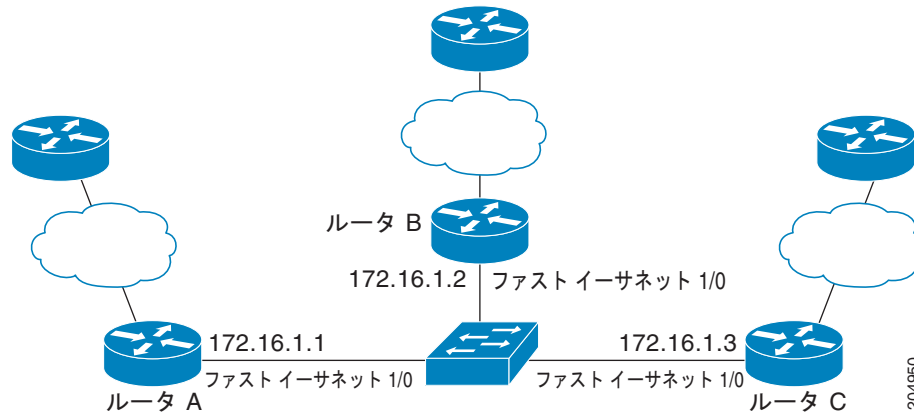


図 3 に、複数のルータがある大規模な EIGRP ネットワークを示します。その中の 3 台は、ルーティングプロトコルとして EIGRP を実行している BFD ネイバーです。

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 FastEthernet0/0
no shutdown
ip address 10.4.9.14 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
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 FastEthernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 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 C の設定

```

!
!
interface FastEthernet0/0
 no shutdown
 ip address 10.4.9.34 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 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 台のすべてのルータで 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。

ルータ A

RouterA# **show bfd neighbors details**

```

OurAddr      NeighAddr    LD/RD  RH/RS   Holddown(mult)  State  Int
172.16.1.1   172.16.1.3    5/3    1(RH)   150 (3 )        Up     Fa0/1
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
Holddown (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   Holddown(mult)  State  Int
172.16.1.1   172.16.1.2    6/1    Up      0 (3 )          Up     Fa0/1
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
Holddown (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 からの **how bfd neighbors details** コマンドの出力で、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。

ルータ B

RouterB# **show bfd neighbors details**

```

OurAddr      NeighAddr      LD/RD  RH/RS  Holddown(mult)  State  Int
172.16.1.2   172.16.1.1     1/6    Up      0 (3)           Up     Fa0/1
    
```

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
Holddown (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  Holddown(mult)  State  Int
172.16.1.2   172.16.1.3     3/6    1(RH)  118 (3)         Up     Fa0/1
    
```

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
Holddown (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
    
```

図 4 ファストイーサネットインターフェイス 0/1 の障害

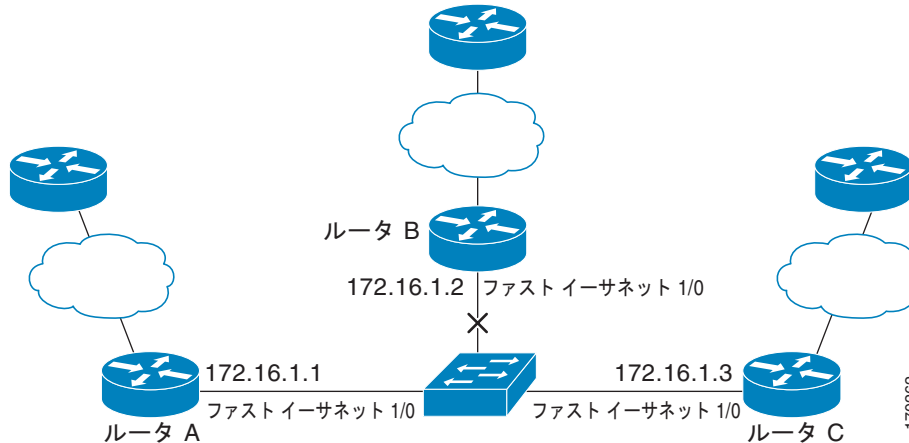


図 4 は、ルータ B でファストイーサネットインターフェイス 0/1 に障害が発生した状態を示しています。このネイバーがなければ、ルータ B からネットワークに到達する方法がありません。

ルータ B のファストイーサネットインターフェイス 0/1 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 0/1 が管理的にシャットダウンされています。

ルータ A での `show bfd neighbors` コマンドからの次の出力では、EIGRP ネットワークのルータ A に対する唯一の BFD ネイバーを示します。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`

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	Fa0/1

ルータ C での `show bfd neighbors` コマンドからの次の出力では、EIGRP ネットワークのルータ C に対する唯一の BFD ネイバーも示します。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。

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	Fa0/1

OSPF ネットワークでの BFD の設定 : 例

Cisco IOS リリース 12.0(31)S

次の例は、ルータ A とルータ B で構成される単純な OSPF ネットワークです。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 がルータ 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ます。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 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 FastEthernet 0/1
ip address 172.16.10.1 255.255.255.0
```

```

bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 コマンドの出力で、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 **show bfd neighbors details** 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。



(注)

ルータ B は Cisco 12000 シリーズ ルータです。 **show bfd neighbors details** コマンドはラインカードで実行する必要があります。 **show bfd neighbors details** コマンドがラインカードで入力された場合、登録されたプロトコルは表示されません。

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!

LC-Slot6> 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
    
```

show ip ospf 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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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 fastethernet 0/1

show ip ospf interface fastethernet 0/1
FastEthernet0/1 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 fastethernet 6/1
```

```

FastEthernet6/1 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)

```

BGP ネットワークでの BFD の設定 : 例

Cisco IOS リリース 12.0(31)S

次の例は、ルータ A とルータ B で構成される単純な BGP ネットワークです。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 がルータ 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ます。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 FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
ip address 172.16.10.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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、BFD セッションが作成され、BFD サポートに対して BGP 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  Holddown(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
Holddown (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 **show bfd neighbors details** 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。



(注)

ルータ B は Cisco 12000 シリーズ ルータです。 **show bfd neighbors details** コマンドはラインカードで実行する必要があります。 **show bfd neighbors details** コマンドがラインカードで入力された場合、登録されたプロトコルは表示されません。

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!
```

```
LC-Slot6> 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
```

show ip bgp neighbors 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
..
```

IS-IS ネットワークでの BFD の設定 : 例

Cisco IOS リリース 12.0(31)S

次の例は、ルータ A とルータ B で構成される単純な IS-IS ネットワークです。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 に対する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ます。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 FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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 FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 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** コマンドは、BFD セッションが作成され、IS-IS が BFD サポートに対して登録されることを確認できます。

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  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 **show bfd neighbors details** 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。



(注)

ルータ B は Cisco 12000 シリーズ ルータです。 **show bfd neighbors details** コマンドはラインカードで実行する必要があります。 **show bfd neighbors details** コマンドがラインカードで入力された場合、登録されたプロトコルは表示されません。

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!
```

```
LC-Slot6> 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
```

HSRP ネットワークでの BFD の設定 : 例

次の例は、ルータ A とルータ B で構成される HSRP ネットワークです。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 に対する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ます。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。



(注) 次の例では、**standby bfd** コマンドと **standby bfd all-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 **bfd interval** 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。**standby bfd** コマンドと **standby bfd all-interfaces** コマンドは、ルータまたはインターフェイスで BFD が手動でディセーブルになっている場合にだけ必要です。

ルータ A

```
ip cef
interface FastEthernet2/0
  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 FastEthernet2/0
  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 FastEthernet2/0
  10.1.0.22
  No active groups
  Standby groups: 1
  BFD enabled !
```

RouterB# **show standby neighbors**

```
HSRP neighbors on FastEthernet2/0
  10.0.0.2
  Active groups: 1
  No standby groups
  BFD enabled !
```

スタティック ルーティングのための BFD サポートの設定：例

次の例は、ルータ A とルータ B で構成されるネットワークです。ルータ A のシリアル インターフェイス 2/0 は、ルータ 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ます。BFD セッションを起動するには、ルータ B を設定する必要があります。

ルータ 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
```

ルータ 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
```

ルータ 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。設定する必要が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。

参考資料

ここでは、BFD 機能に関する参考資料について説明します。

関連資料

関連項目	資料タイトル
BGP の設定と監視	『Cisco IOS IP Routing Protocols Configuration Guide』の「 Cisco BGP Overview 」モジュール
EIGRP の設定と監視	『Cisco IOS IP Routing Protocols Configuration Guide』の「 Configuring EIGRP 」モジュール
HSRP の設定と監視	『Cisco IOS IP Application Services Configuration Guide』の「 Configuring HSRP 」モジュール
IS-IS の設定と監視	『Cisco IOS IP Routing Protocols Configuration Guide』の「 Configuring Integrated IS-IS 」モジュール
OSPF の設定と監視	『Cisco IOS IP Routing Protocols Configuration Guide』の「 Configuring OSPF 」モジュール
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 』

関連項目	資料タイトル
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 』

規格

規格	タイトル
IETF ドラフト	<i>Bidirectional Forwarding Detection</i> , February 2009 (http://www.ietf.org/internet-drafts/draft-ietf-bfd-base-09.txt)
IETF ドラフト	<i>BFD for IPv4 and IPv6 (Single Hop)</i> , February 2009 (http://www.ietf.org/internet-drafts/draft-ietf-bfd-v4v6-1hop-09.txt)

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィードバックの MIB の場所を検索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

RFC

RFC	タイトル
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none">• テクニカル サポートを受ける• ソフトウェアをダウンロードする• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける• ツールおよびリソースへアクセスする• Product Alert の受信登録• Field Notice の受信登録• Bug Toolkit を使用した既知の問題の検索• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する• トレーニング リソースへアクセスする• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>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。</p>	<p>http://www.cisco.com/techsupport</p>

双方向フォワーディング検出の機能情報

表 1 に、この機能のリリース履歴を示します。

一部のコマンドは、お使いの Cisco IOS ソフトウェア リリースで使用できないことがあります。コマンドごとのリリース情報については、コマンドリファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、およびプラットフォームに固有です。プラットフォームのサポートおよびソフトウェア 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 を使用すると、特定のソフトウェア リリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS および Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp> からアクセスしてください。Cisco.com のアカウントは必要ありません。



(注) 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1 双方向フォワーディング検出の機能情報

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)	12.2(18)SXE 12.0(31)S 12.0(32)S 12.4(9)T 12.2(33)SRB 12.4(11)T 12.4(15)T 12.2(33)SXH 12.2(33)SRC	このドキュメントでは、Bidirectional Forwarding Detection (BFD; 双方向フォワーディング検出) 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、複数のルーティング プロトコルの hello メカニズムの可変レートではなく、統一レートで転送パス障害を検出でき、ネットワークのプロファイリングおよび計画が簡単になり、コンバージェンス時間が一貫して予測できます。 リリース 12.0(31)S では、Cisco 12000 シリーズ インターネット ルータのサポートが追加されました。 リリース 12.0(32)S では、Cisco 12000 シリーズ インターネット ルータの Cisco 10720 インターネット ルータおよび IP サービス エンジン (Engine 3) およびエンジン 5 共有ポート アダプタ (SPA) および 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。

表 1 双方向フォワーディング検出の機能情報 (続き)

機能名	リリース	機能情報
BFD エコー モード	12.4(9)T 12.2(33)SRB	<p>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。</p> <p>次の項では、この機能に関する情報について説明します。</p> <ul style="list-style-type: none"> 「BFD エコー モードの設定」 (P.27) 「非対称性のない BFD エコー モードのディセーブル化」 (P.28)
BFD : EIGRP サポート	12.0(31)S 12.4(4)T 12.2(18)SXE 12.2(33)SRA 12.2(33)SRB	<p>EIGRP が BFD で登録されたプロトコルであり、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 BFD を設定できます。</p> <p>EIGRP に対する BFD は、Cisco IOS リリース 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。</p> <p>次の項では、この機能に関する情報について説明します。</p> <ul style="list-style-type: none"> 「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」 (P.11) 「EIGRP に対する BFD サポートの設定」 (P.13) 「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 : 例」 (P.33)
BFD : VRF サポート	12.2(33)SRC 15.0(1)M	<p>BFD 機能のサポートが、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 Routing and Forwarding (VRF; VPN ルーティングおよび転送) 対応に拡張されています。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「VPN Routing and Forwarding (VRF; VPN ルーティングおよび転送) インターフェイスのための BFD サポート」 (P.7)

表 1 双方向フォワーディング検出の機能情報 (続き)

機能名	リリース	機能情報
BFD : WAN インターフェイス サポート	12.2(33)SRC 15.0(1)M	<p>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。</p> <p>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。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「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」 (P.7)
BFD に対する HSRP サポート	12.4(11)T 12.4(15)T 12.2(33)SRC	<p>リリース 12.4(11)T では、HSRP のサポートが追加されました。</p> <p>リリース 12.4(15)T では、BFD が Cisco ルータの Integrated Services Router (ISR; サービス統合型ルータ) 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。</p> <p>リリース 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、BFD 機能が VRF 対応に確証され、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、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。</p> <p>この機能については、次の項に説明があります。</p> <p>「HSRP ネットワークでの BFD の設定 : 例」 (P.46)</p>
IPv4 での BFD に対する IS-IS サポート	12.0(31)S 12.4(4)T 12.2(18)SXE 12.2(33)SRA	<p>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。</p> <p>次の項では、この機能に関する情報について説明します。</p> <ul style="list-style-type: none"> 「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」 (P.11) 「IS-IS に対する BFD サポートの設定」 (P.15) 「IS-IS ネットワークでの BFD の設定 : 例」 (P.45)

表 1 双方向フォワーディング検出の機能情報 (続き)

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 12.4(4)T 12.2(18)SXE 12.2(33)SRA	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 から転送バスの検出障害メッセージを受信します。 次の項では、この機能に関する情報について説明します。 <ul style="list-style-type: none"> 「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」(P.11) 「OSPF に対する BFD サポートの設定」(P.19) 「OSPF ネットワークでの BFD の設定 : 例」(P.38)
SSO : BFD	12.2(33)SXI2 12.2(33)SRE 12.2(33)XNE	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動状態に保つことができます。 この機能については、次の項に説明があります。 <ul style="list-style-type: none"> 「ステートフルスイッチオーバーのための BFD サポート」(P.8)
SSO : BFD (Admin Down)	12.2(33)SRC	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。 この機能については、次の項に説明があります。 <ul style="list-style-type: none"> 「ステートフルスイッチオーバー機能を持つノンストップフォワーディングのための BFD サポート」(P.7)
BFD 用のスタティックルート	12.2(33)SRC 15.0(1)M	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みなされ、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。 次の項では、この機能に関する情報について説明します。 <ul style="list-style-type: none"> 「スタティックルーティングのための BFD サポート」(P.9) 「スタティックルーティングのための BFD サポートの設定」(P.25) 「スタティックルーティングのための BFD サポートの設定 : 例」(P.47)

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2008-2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2010, シスコシステムズ合同会社.
All rights reserved.

