



EIGRP 設定ガイド

最終更新：2026年7月8日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



はじめに

ここでは、このマニュアルの表記法、および他資料の入手方法について説明します。また、シスコ製品のマニュアルの最新情報についても説明します。

- [表記法](#) (iii ページ)
- [関連資料](#) (v ページ)
- [マニュアルの入手方法およびテクニカルサポート](#) (v ページ)

表記法

このマニュアルでは、以下の表記法を使用しています。

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 (ここではキーを大文字で表記していますが、小文字で入力してもかまいません)。
太字	コマンド、キーワード、およびユーザーが入力するテキストは 太字 で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する引数は、イタリック体で示しています。
Courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
太字の courier フォント	太字の Courier フォントは、ユーザーが入力しなければならないテキストを示しています。
[x]	角カッコの中の要素は、省略可能です。
...	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ています。

表記法	説明
	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示しています。
[x y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表しています。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string 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string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示しています。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



ヒント 「問題解決に役立つ情報」です。



注意 「要注意」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。



ワンポイントアドバイス

「時間を節約する方法」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

次の一般的な安全上の警告に注意してください。



警告 安全上の重要な注意事項

装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。使用、設置、電源への接続を行う前にインストール手順を読んでください。各警告の冒頭に記載されているステートメント番号を基に、装置の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。



関連資料



(注) デバイスをインストールまたはアップグレードする前に、デバイスのリリースノートを参照してください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、毎月更新される『更新情報』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

『更新情報』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



目次

はじめに :

はじめに iii

表記法 iii

関連資料 v

マニュアルの入手方法およびテクニカル サポート v

第 1 章

EIGRP 1

EIGRP に関する情報 2

EIGRP の主な機能 2

EIGRP の主な利点 3

EIGRP for IPv6 固有の機能 4

EIGRP NSF 4

EIGRP NSF 認識 5

EIGRP NSF の c_Benefits 5

EIGRP NSF の前提条件と考慮事項 6

EIGRP スタブルルーティング 6

EIGRP スタブルルーティングとは 6

EIGRP スタブルルーティング 7

EIGRPv6 スタブルルーティング 8

EIGRPv6 スタブルルーティングとは 8

EIGRPv6 スタブルルーティングの仕組み 9

EIGRPv6 環境の利点 9

EIGRPv6 スタブルルーティングに関する主な考慮事項 10

EIGRP の設定方法 10

EIGRP のデフォルト設定 11

基本的な EIGRP パラメータの設定	13
EIGRP インターフェイスの設定	15
IPv6 の EIGRP の設定	16
明示的なルータ ID の設定	17
EIGRP IPv6 インターフェイスおよびパッシブインターフェイスの設定	17
EIGRP ルート認証の設定	18



第 1 章

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) は、シスコが開発した高度なハイブリッドルーティングプロトコルであり、ディスタンスベクターとリンクステート機能のバランスをとることで、自律システム (AS) 内の高速かつ効率的で拡張可能なルーティングを実現します。

- [EIGRP に関する情報 \(2 ページ\)](#)
- [EIGRP の主な機能 \(2 ページ\)](#)
- [EIGRP の主な利点 \(3 ページ\)](#)
- [EIGRP for IPv6 固有の機能 \(4 ページ\)](#)
- [EIGRP NSF \(4 ページ\)](#)
- [EIGRP NSF 認識 \(5 ページ\)](#)
- [EIGRP NSF の c_Benefits \(5 ページ\)](#)
- [EIGRP NSF の前提条件と考慮事項 \(6 ページ\)](#)
- [EIGRP スタブルルーティング \(6 ページ\)](#)
- [EIGRP スタブルルーティングとは \(6 ページ\)](#)
- [EIGRP スタブルルーティング \(7 ページ\)](#)
- [EIGRPv6 スタブルルーティング \(8 ページ\)](#)
- [EIGRPv6 スタブルルーティングとは \(8 ページ\)](#)
- [EIGRPv6 スタブルルーティングの仕組み \(9 ページ\)](#)
- [EIGRPv6 環境の利点 \(9 ページ\)](#)
- [EIGRPv6 スタブルルーティングに関する主な考慮事項 \(10 ページ\)](#)
- [EIGRP の設定方法 \(10 ページ\)](#)
- [EIGRP のデフォルト設定 \(11 ページ\)](#)
- [基本的な EIGRP パラメータの設定 \(13 ページ\)](#)
- [EIGRP インターフェイスの設定 \(15 ページ\)](#)
- [IPv6 の EIGRP の設定 \(16 ページ\)](#)
- [明示的なルータ ID の設定 \(17 ページ\)](#)
- [EIGRP IPv6 インターフェイスおよびパッシブインターフェイスの設定 \(17 ページ\)](#)
- [EIGRP ルート認証の設定 \(18 ページ\)](#)

EIGRP に関する情報

Enhanced Interior Gateway Routing Protocol (EIGRP) は、シスコシステムズによって開発された高度なルーティングプロトコルです。Diffusing Update Algorithm (DUAL) は、ループフリーのパスと迅速なコンバージェンスを確保するために EIGRP で使用されるコアアルゴリズムです。EIGRP が最適なパス (サクセサ) を見つけ、接続先への事前計算されたバックアップパス (フィージブルサクセサ) を計算できます。プライマリパスで障害が発生した場合、EIGRP はルート全体を再計算することなく、すぐにフィージブルサクセサに切り替えることができます。これにより、ダウンタイムを最小限に抑えることができます。DUAL も可変長サブネットマスク (VLSM) をサポートしています。

EIGRP は、高度なディスタンス ベクター ルーティング プロトコル と見なされ、ディスタンス ベクター と リンクステート ルーティング プロトコルの両方に通常見られる機能が組み込まれているため、ハイブリッドプロトコルと呼ばれることがよくあります。

EIGRP の主な機能

EIGRP の主な機能は次のとおりです。

- **ハイブリッドな性質と効率的な更新** : EIGRP は、ディスタンスベクタープロトコル (ネイバーからルート进行学习) のシンプルさと、通常リンクステートプロトコルに関連付けられる高速コンバージェンスおよびループ回避メカニズムを結合します。従来のディスタンスベクタープロトコルが定期的にルーティングテーブル全体の更新を送信するのとは異なり、EIGRP は部分的かつ限定的な更新を送信します。これは、変更が発生した場合にのみ更新が送信され、影響を受けるルートがその情報を必要とするルータにのみ送信されることを意味し、帯域幅の消費を大幅に削減します。
- **Reliable Transport Protocol (RTP)** : EIGRP は独自の RTP を使用して、EIGRP パケットの信頼性と順序付けられた配信を保証します。信頼性の高い通信のためのシーケンスおよび確認応答番号が含まれます。
- **複数のテーブル** : EIGRP は、ルーティング情報を管理するために 3 つの異なるテーブルを保持します。
 - **ネイバーテーブル** : 隣接関係が形成されている直接接続された EIGRP ルータ (ネイバー) に関する情報を保存します。ネイバー関係は Hello パケットを使用して確立されます。
 - **トポロジテーブル** : ベストパス (サクセサ) とバックアップパス (フィージブルサクセサ) を含む、自律システム内の接続先へのすべての学習済みルートが含まれます。
 - **ルーティングテーブル** : トポロジテーブルから選択された各接続先への最適なパスが含まれています。
- **複合メトリックと複数のネットワーク層プロトコルのサポート** : EIGRP は、帯域幅、遅延、信頼性、負荷などの要因を組み合わせることでメトリックを計算します。デフォルトでは、

負荷と信頼性は動的に変化する可能性があり、ルートの再計算が頻繁に発生するため、メトリックの計算では帯域幅と遅延のみが使用されます。メトリック式には、使用される要因とその影響を決定する「K 値」が組み込まれています。EIGRP は、プロトコル依存モジュール (PDM) を使用して、IPv4、IPv6、IPX、AppleTalk などのさまざまなネットワーク層プロトコルのルーティングをサポートします。

- **ロードバランシングとルート集約**：EIGRP は、等コストと不等コストの両方のロードバランシングをサポートします。これにより、パスのコストが異なっている場合でも、トラフィックを接続先までの複数のパスに分散でき、ネットワークリソースの使用率が最適化されます。EIGRP は、手動と自動のルート集約をサポートしています。これにより、ルーティングテーブルのサイズを削減し、ルーティングの効率と拡張性を向上できます。
- **認証**：EIGRP は認証 (MD5 または SHA-2 など) を使用して、ネイバー間のルーティングの更新を保護でき、ネットワークのセキュリティを強化できます。
- **スタブルルーティング**：EIGRP は、ハブアンドスポークトポロジでのルーティングを最適化するために使用されるスタブルルーティングをサポートしています。スタブルルータは、受信する EIGRP トラフィックとクエリの量を制限します。これにより、ネットワークの安定性が向上し、メモリ消費を削減できます。
- **クラスレスルーティング**：EIGRP はクラスレスルーティングプロトコルであり、可変長サブネットマスク (VLSM) とクラスレス インタードメイン ルーティング (CIDR) をサポートします。
- **アドミニストレーティブ ディスタンス (AD) とホップカウント**：EIGRP のデフォルトのアドミニストレーティブ ディスタンスは、内部ルートが 90、外部ルートが 170 であり、複数のルーティングプロトコルが使用されている場合のルート選択に影響を与えます。メトリックの計算では直接使用されませんが、EIGRP には、ループ防止メカニズムとして機能する設定可能な最大ホップ数 (デフォルトは 100 (最大 255)) が設定されています。

EIGRP の主な利点

EIGRP には、大規模で複雑なネットワークに適した次のような利点があります。

- **インターフェイスベースの設定**：ネットワークコマンドを使用して EIGRP プロセスにネットワークを含める IPv4 用 EIGRP とは異なり、IPv6 用 EIGRP は、実行する必要があるインターフェイスで直接設定されます。これは、EIGRPv6 に「network」コマンドがないことを意味します。代わりに、特定のインターフェイスで EIGRPv6 を有効にします。
- **グローバル IPv6 アドレス要件なし**：EIGRP for IPv6 は、グローバル IPv6 アドレスを必要とせずにインターフェイスで設定できます。主に、ネイバー探索と通信に IPv6 リンクローカルアドレスを使用します。
- **ルータ ID**：EIGRP for IPv6 インスタンスでは、明示的または暗黙的なルータ ID が正しく機能する必要があります。このルータ ID は、32 ビットの数値であり、IPv4 ドット付き 10 進法形式 (例：1.1.1.1) で表示されます。ルータに、ルータ ID の導出元となる IPv4 アドレスがない場合は、手動で設定する必要があります。

- マルチキャストアドレス：EIGRP for IPv6は、メッセージ（Hello パケットや更新など）の送信に IPv6 マルチキャストアドレス FF02::A を使用します。これは、IPv4 用 EIGRP が使用する 224.0.0.10 マルチキャストアドレスの IPv6 に相当します。
- 送信元アドレス：IPv6 メッセージ用 EIGRP は、終了インターフェースの IPv6 リンクローカルアドレスを使用して送信されます。一方、IPv4 用 EIGRP メッセージは、アウトバウンドインターフェースの IPv4 アドレスを使用します。
- 差別化された設定：Diffusing Update Algorithm（DUAL）やメトリック計算などの基本メカニズムは IPv4 用 EIGRP と似ていますが、IPv6 用 EIGRP は個別に設定および管理されます。

EIGRP for IPv6 固有の機能

IPv6 用 Enhanced Interior Gateway Routing Protocol（EIGRP）は、IPv6 ネットワークをサポートするように設計された元の EIGRP をカスタマイズしたものです。EIGRP for IPv4 の多くのコア機能と利点は維持されていますが、IPv6 アドレッシングスキームとその固有の特性に対応するため、特定の拡張機能と動作の違いが組み込まれています。

- インターフェイスベースの設定：EIGRP for IPv6 は、グローバルネットワーク コマンドを使用せずに、インターフェイスで直接設定されます。
- ルータ ID：IPv6 専用環境でも、明示的または暗黙的な 32 ビットのルータ ID が必要です。多くの場合、IPv4 ドット付き 10 進形式で使用されます。
- マルチキャストアドレス：メッセージの送信に IPv6 マルチキャストアドレス FF02::A を使用します。これは、IPv4 の 224.0.0.10 に相当します。
- 送信元アドレス：IPv6 メッセージ用 EIGRP は、終了インターフェースの IPv6 リンクローカルアドレスから送信されます。
- 同様の DUAL およびメトリック計算：IPv4 および IPv6 バージョンの両方で、同じ DUAL アルゴリズムとコンポジットメトリック計算が使用されます。

EIGRP NSF

EIGRP Nonstop Forwarding（NSF）は、ルートプロセッサ（RP）のスイッチオーバーや再起動など、ルータで計画的または計画外のコントロールプレーン障害によるトラフィックの中断を最小限に抑えるように設計された高可用性機能です。これを実現するために、EIGRP NSF はネットワーク内のルータ間で、EIGRP NSF 機能と EIGRP NSF 認識という 2 つの異なるロールまたはサポートレベルに依存しています。

EIGRP NSF 機能

EIGRP NSF 機能を使用して設定されたルータは、パケット転送を中断せずに再起動またはスイッチオーバーを実行するように設計されたデバイスです。このルータは、多くの場合冗長な

コントロールプレーン（Cisco Catalyst 6500 シリーズ スイッチのデュアル RP など）を備えているため、コントロールプレーンが回復中または切り替え中でも、データプレーン（Forwarding Information Base（転送情報ベース）：FIB）を維持し、トラフィックを転送し続けます。

NSF 対応ルータが再起動すると、NSF 機能を EIGRP ネイバーに伝達します。この期間中、通常はネイバーが隣接関係のダウンを宣言する原因となる EIGRP Hello パケットの送信を一時的に停止します。ただし、NSF のため、ネイバーの反応は異なります。

EIGRP NSF 認識

EIGRP NSF 認識ルータ（NSFヘルパーとも呼ばれる）は、NSF 対応ルータからの NSF 固有のシグナリングを理解するネイバー EIGRP ルータです。NSF 認識ルータが NSF 対応ネイバーが再起動していることを検出すると、Hello パケットの受信を停止しても、EIGRP 隣接関係はすぐに切断しません。

代わりに、NSF 対応ルータは、事前定義された「猶予期間」中、再起動（NSF 対応）ルータから受信したルーティング情報を保持します。これにより、ルーティングが防止されます。

シスコ社外秘

隣接関係がドロップされずに済み、ネットワーク全体のルーティングの再コンバージェンスを回避できます。そうしない場合、トラフィック損失につながります。この猶予期間中に、NSF 対応ルータはルーティングテーブルを再構築し、NSF 対応ルータとの完全な EIGRP 隣接関係を再確立します。再起動するルータが完全に回復し、ルーティング情報を同期すると、通常の EIGRP 動作がシームレスに再開されます。

基本的に、EIGRP NSF 機能は、ルータが自身のコントロールプレーンの中断中に転送を維持する機能を指します。一方、EIGRP NSF 認識は、ルーティング隣接関係を維持し、ネットワーク全体の再コンバージェンスをトリガーしないことにより、このプロセスを支援するネイバーの機能を指します。この協力メカニズムにより、コントロールプレーンに障害が発生した場合でも、最小限のダウンタイムと継続的なパケット転送が保証されます。

EIGRP NSF の c_Benefits

- ダウンタイムの最小化：主な利点は、コントロールプレーン障害または計画的なメンテナンス時のネットワーク非可用性とパケット損失が大幅に削減されることです。

•

シームレスな運用：ルーティングインテリジェンスが一時的に使用できない場合でもトラフィックが流れるため、ユーザーは中断のないサービスを提供できます。

•

ネットワークの安定性の向上：NSF は、ルーティング隣接関係のドロップを防ぐことで、ネットワーク全体に広範に及ぶルートの再計算を回避し、全体的な安定性の向上に役立ちます。

EIGRP NSF の前提条件と考慮事項

- SSO と GR の統合 : NSF はスタンドアロン機能ではありません。通常、SSO および GR (または Non-Stop Routing - NSR) と組み合わせて展開することで、完全なノンストップフォワーディング機能を実現できます。
- NSF 対応および NSF 認識デバイス : 関与するすべてのデバイスは、NSF をサポートする必要があり、再起動ルータは NSF 対応で、そのネイバーは NSF 認識です。
- EIGRP タイマー : EIGRP NSF には、グレースフルリスタートページ時間、nsf コンバージ、nsf ルート保留、nsf 信号などの設定可能なタイマーがあり、猶予期間やその他のリカバリ側面を制御します。
- BFD の相互作用 : BFD (双方向転送検出) は高速な異常検出を提供しますが、フェイルオーバー中に BFD の隣接関係が維持されない可能性があるため、BFD を認識しない場合、NSF/SSO と競合する可能性があります。これにより、再コンバージェンスが発生する可能性があります。
- Cisco Express Forwarding (CEF) : NSF は、FIB を維持する CEF に依存して、コントロールプレーンの中断中にラインカードがパケットを転送し続けます。

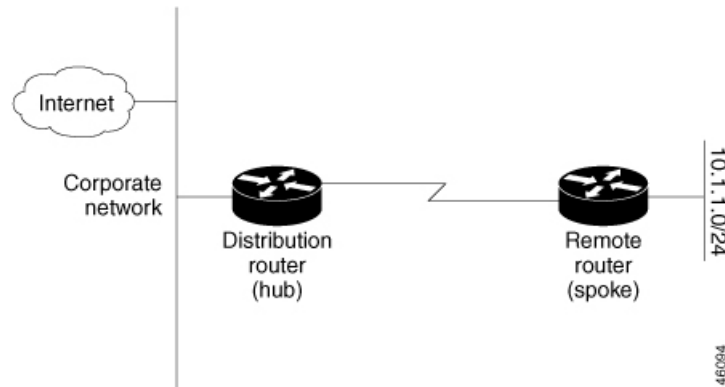
EIGRP スタブルルーティング

EIGRP スタブルルーティングは、特にハブアンドスポークや分散拠点トポロジにおけるネットワークの安定性の向上、リソース使用率 (CPU、メモリ、帯域幅) の削減、およびネットワーク設計の簡素化を目的とした機能です。EIGRP ルーティング更新のフローとネットワーク内のクエリを制御するために使用されます。

EIGRP スタブルルーティングとは

ルータが EIGRP スタブとして設定されると、ルータはスタブルータであることを EIGRP ネイバーに送信します。スタブルータは、通常、特定の方向に自身を超える他の EIGRP ネイバーを持たない EIGRP ドメインのルータです。通常、ハブアンドスポークトポロジのスポークルータ、または単一のアップストリームルータに接続されているルータです。

図 1: 単純なハブアンドスポーク型ネットワーク



EIGRP スタブルーティング

EIGRP スタブルーティングを導入する主な理由は次のとおりです。

- ネットワークの安定性の向上：スタブルーティングは、EIGRP クエリの伝播を制限することにより、トポロジ変更時のルート再計算の範囲を絞り込むことができます。これにより、「スタックインアクティブ」(SIA)の問題が防止され、ネットワークの安定性を保つことができます。
- リソース使用率の削減：スタブルータは、ネットワーク全体の完全なEIGRP トポロジテーブルを維持する必要がありません。これにより、CPUとメモリの使用量が削減されます。さらに、送受信する更新を制御することで、帯域幅を節約できます。
- 簡素化された設定：限られたルートのセットのみをアドバタイズするため、スタブルータでのルーティング設定が簡素化されます。
- セキュリティの強化：スタブルータを通過するトランジットトラフィックを防止することにより、セキュリティ対策として機能し、トラフィックがハブにのみ流れるようにできます。

EIGRP スタブルーティングの仕組み

ルータがスタブとして設定されている場合：

- EIGRP Hello パケットにある特別なスタブフラグがネイバーに送信されます。
- ネイバーはこのフラグを認識し、ルータをネイバーテーブルのスタブとしてマークします。
- 重要なのは、EIGRP ネイバーがスタブルータにクエリパケットを送信しないことです。これは、クエリドメインを制限するための主なメカニズムです。スタブルータが持っている可能性があるルートがネイバーに必要な場合、スタブにはクエリされません。代わりに、スタブにはその接続先へのパスがないことが想定されます。

- スタブルータは、デフォルトでは、直接接続ルートとサマリールートのみをアドバタイズします。他の EIGRP ネイバーから学習したルートはアドバタイズしません。

EIGRPv6 スタブルルーティング

EIGRPv6 スタブルルーティングは、IPv6 ネットワークに特化した EIGRP スタブルルーティング機能の実装です。コアの原則と利点は、IPv4 スタブルルーティング用の EIGRP と同じですが、IPv6 アドレッシングおよび動作コンテキストに合わせて適用されます。

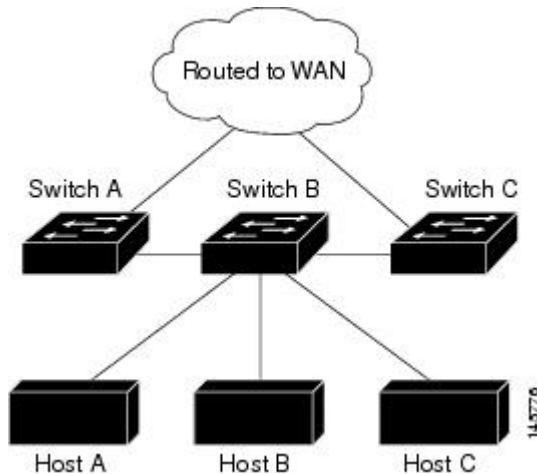
EIGRPv6 スタブルルーティングとは

EIGRPv6 スタブルルーティングは、ネットワークの安定性を向上させ、リソース使用率（CPU、メモリ、帯域幅）を減らし、IPv6 EIGRP ドメインのスタブルータの設定を簡素化するために使用されます。スタブルータは、通常、ハブアンドスポークまたは分散拠点トポロジのエッジデバイスです。通常、ローカル ネットワーク セグメント外に 1 つまたはいくつかのパスしかないルータであり、他の EIGRP ピア間のトラフィックのトランジットポイントになることは想定されていません。

次の図では、スイッチ B は EIGRPv6 スタブルータとして設定されています。スイッチ A および C は、より広範な WAN に接続されています。このセットアップでは、次のようになります。

- スイッチ B は、接続済み、静的、再配布、および要約ルートをスイッチ A および C にアドバタイズします。
- 逆に、スイッチ B はスイッチ A から学習したルートをアドバタイズしません（その逆も同様）。この結果、スイッチ B は EIGRP ドメインにのみローカルルートを挿入し、他の EIGRP ネイバーから学習したルートのトランジットルータとして機能しないようにできます。

図 2: EIGRP スタブルータ設定



EIGRPv6 スタブルルーティングの仕組み

EIGRPv6 スタブルルーティングのメカニズムは、対応する IPv4 とほぼ同じです。

1. Hello パケットのスタブフラグ：EIGRPv6 ルータがスタブとして設定されている場合、EIGRPv6 Hello パケットに特別なスタブフラグが含まれます。これらの Hello は、インターフェイスの IPv6 リンクローカルアドレスと EIGRPv6 マルチキャストアドレス (FF02::A) を使用して送信されます。
2. ネイバーの認識：ネイバーリング EIGRPv6 ルータ（通常はハブルータ）は、これらの Hello を受信し、スタブフラグを認識し、その特定のネイバーをスタブとしてマークします。
3. クエリの抑制：最も重要な点は、EIGRPv6 ネイバーがスタブルータにクエリパケットを送信しないことです。ハブルータがルートを失い、代替パスをネイバーにクエリする必要がある場合、スタブピアにはクエリを実行しません。これにより、クエリフラッドがスタブネットワークに到達するのを防ぎます。これは、潜在的に不安定な場合や、低帯域幅の WAN リンクで有効です。
4. 限定ルートアドバタイズメント：デフォルトでは、EIGRPv6 スタブルータは、直接接続された IPv6 ネットワークとサマリー IPv6 ルートのみを EIGRPv6 ドメインにアドバタイズします。これにより、スタブルータが維持する必要があるルーティングテーブルのサイズと送信するルーティング情報の量が制限されます。

EIGRPv6 環境の利点

- 安定性の向上：EIGRPv6 クエリがスタブネットワークに伝播するのを防ぎ、「スタック インアクティブ」(SIA) 状態を緩和し、トポロジ変更の影響をローカル化します。これは、ネットワークの稼働時間を維持するのに重要です。

- リソース消費の削減：スタブルータでは、完全な EIGRPv6 トポロジテーブルを処理または保存する必要がないため、メモリと CPU が少なく済みます。更新が少なくクエリが送信されないため、スタブへのリンクで消費される帯域幅が少なくなります。
- 設計と管理の簡素化：エッジネットワークのルーティング設計が合理化され、スタブデバイスでの設定が簡素化されます。
- ハブアンドスポークに最適化：スポークルータがネットワークの他の部分に到達するのにデフォルトルート（またはいくつかの固有ルート）のみを必要とする IPv6 ハブアンドスポーク展開に最適です。

EIGRPv6 スタブルルーティングに関する主な考慮事項

- 設定の場所：EIGRPv6 は `ipv6 eigrp [ASN]` を使用してインターフェイスで直接設定され、`eigrp stable` コマンドは EIGRPv6 ルータ コンフィギュレーションモード内で適用されます。
- ルータ ID：EIGRPv6 インスタンスには、IPv6 専用ネットワークであっても、32 ビットのルータ ID（多くの場合 IPv4 ドット付き 10 進形式）が必要です。ルータに IPv4 アドレスが存在しない場合は、明示的に設定する必要があります。
- トランジットトラフィックなし：スタブとして設定されたルータを、他の EIGRPv6 ネイバー間のトラフィックのトランジットポイントとして使用しないでください。使用すると、ルーティングブラックホールが発生する可能性があります。
- デフォルトルートと要約：スタブルルーティングの利点を完全に活用するために、特にリソース保護の観点から、スタブルータにデフォルトの IPv6 ルート (:::0) を送信するようにハブルータを設定することを強く推奨します。また、ハブでルータを集約すると、スタブのルーティングテーブルサイズをさらに小さくできます。

EIGRP の設定方法

デバイスで EIGRP ルーティングプロセスを開始するには、次の手順を実行する必要があります。

手順

- ステップ 1** EIGRP の有効化：これには、通常、グローバル コンフィギュレーション モードで `router eigrp [AS_number]` などのコマンドを入力することによる EIGRP プロセスの開始が含まれます。この場合、`[AS_number]` は、EIGRP ルーティングドメインを定義する自律システム番号です。
- ステップ 2** ネットワークの関連付け：EIGRP を有効にした後、EIGRP がアドバタイズするネットワークと、EIGRP が更新を送信するインターフェイスを指定する必要があります。これは、EIGRP ルータ コンフィギュレーション モード内のネットワークコマンドを使用して実行されます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。イン

ターフェイスのネットワークを指定しなければ、EIGRPのアップデート中にアドバタイズされません。

次のタスク



- (注) ネットワーク上にIGRP用に設定されているデバイスがあり、この設定をEIGRPに変更する場合は、IGRPとEIGRPの両方が設定された移行デバイスを指定する必要があります。この場合は、この次の項に記載されているステップ1～3を実行し、さらに「スプリットホライズンの設定」も参照してください。ルートを自動的に再配信するには、同じAS番号を使用する必要があります。

EIGRP のデフォルト設定

表 1: EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	ディセーブル。
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。 <ul style="list-style-type: none"> • 帯域幅：0 以上の kb/s • 遅延（10 マイクロ秒）：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0～255 の任意の数値（255 の場合は信頼性が 100%） • 負荷：0～255 の数値で表される有効帯域幅（255 の場合は 100% の負荷） • MTU：バイトで表されたルートの MTU サイズ（0 または任意の正の整数）
ディスタンス	内部距離：90 外部距離：170

機能	デフォルト設定
EIGRP ログネイバーの変更	ディセーブル。隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅の割合	50%
IP hello 間隔	低速非ブロードキャスト マルチアクセス (NBMA) ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル。
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリック重み	tos : 0、k1 および k3 : 1、k2、k4、および k5 : 0
ネットワーク	指定なし
ノンストップ フォワーディング (NSF) 認識	Network Advantage ライセンスを実行するスイッチ上で IPv4 に対してイネーブルになっています。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 対応	ディセーブル。 (注) デバイスは EIGRP NSF 対応ルーティングを IPv4 に対してサポートします。
オフセットリスト	ディセーブル。
ルータ EIGRP	ディセーブル。
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分
バリエーション	1 (等コスト ロード バランシング)

基本的な EIGRP パラメータの設定

基本的な EIGRP パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 端末の有効化と設定

特権 EXEC モードを有効にします。要求された場合はパスワードを入力し、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。

例：

```
Device enable
Device# configure terminal
```

ステップ 2 router eigrp autonomoussystem

EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他の EIGRP デバイスへのルートを特定し、ルーティング情報をタグ付けします。

例：

```
Device(config)#router eigrp 10
```

ステップ 3 nsf

(任意) EIGRPNsf をイネーブルにします。アクティブスイッチとそのすべてのピアでこのコマンドを入力します。

例：

```
Device(configrouter)#nsf
```

ステップ 4 network network-number

ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。

例：

```
Device(configrouter)#network 192.168.0.0
```

ステップ 5 eigrp log-neighbor-changes

(任意) EIGRP 隣接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニターします。

例：

```
Device(configrouter)#eigrp logneighbor-changes
```

ステップ 6 metric weights tos k1 k2 k3 k4 k5

(任意) EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するように入念に設定されていますが、調整することも可能です。

(注)

メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。

例：

```
Device(configrouter)#metric weights 0
2 0 2 0 0
```

ステップ7 offset-list [*access-list number name*] { in out } offset [*type number*]

(任意) オフセットリストをルーティングメトリックに適用し、EIGRPによって取得したルートへの着信および発信メトリックを増加します。アクセスリストまたはインターフェイスを使用し、オフセットリストを制限できます。

例：

```
Device(configrouter)#offset-list 21 out 10
```

ステップ8 auto-summary

(任意) ネットワークレベルルートへのサブネットルートの自動サマライズをイネーブルにします。

例：

```
Device(configrouter)# auto-summary
```

ステップ9 interface *interface-id*

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、設定するレイヤ3 インターフェイスを指定し、必要に応じて、サマリー集約を設定します。ip summary-address eigrp *autonomous-systemnumber address mask*

例：

```
Device(configrouter)# interface gigabitethernet 1/0/1
Device(config-if)# ip summary-address eigrp 1 192.168.0.0 255.255.0.0
Device(config-if)# end
```

次のタスク

エントリを確認するには、**show ip protocols** を使用します。

```
Device# show ip protocols
For NSF awareness, the output shows: *** IP Routing is NSF aware *** EIGRP NSF enabled.
```

設定を保存するには、**copy running-config startup-config** コマンドを入力します。

```
Device# copy runningconfig startup-config
```

EIGRP インターフェイスの設定

インターフェイスごとに、他のEIGRPパラメータを任意で設定できます。EIGRP インターフェイスを設定するには、次の手順を実行します。

手順

ステップ1 端末の有効化と設定

特権 EXEC モードを有効にします。要求された場合はパスワードを入力し、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。

例：

```
Device enable  
Device# configure terminal
```

ステップ2 interface *interface-id*

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、設定するレイヤ3 インターフェイスを指定します。

例：

```
Device(config)#interface gigabitethernet 1/0/1
```

ステップ3 ip bandwidth-percent autonomous-system-number eigrp

(任意) インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。

例：

```
Device(config-if)# ip bandwidth-percent autonomous-system-number eigrp 60
```

ステップ4 ip summary-address eigrp *autonomous-systemnumber address mask*

(任意) 指定されたインターフェイスのサマリー集約アドレスを設定します (auto-summary がイネーブルの場合は、通常設定する必要はありません)。

例：

```
Device(config-if)#ip summary-address eigrp 109 192.161.0.0 255.255.0.0
```

ステップ5 ip hello-interval eigrp *autonomous-system-number seconds*

(任意) EIGRP ルーティングプロセスの hello 時間間隔を変更します。指定できる範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。

例 :

```
Device(config-if)#ip hellointerval eigrp 109 10
```

ステップ 6 ip hold-time eigrp autonomous-system-number seconds

(任意) EIGRP ルーティング プロセスのホールド時間間隔を変更します。指定できる範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。

(注)

ホールド タイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。

例 :

```
Device(config-if)#ip holdtime eigrp 109 40
```

ステップ 7 no ip split-horizon eigrp [autonomous-system-number]

(任意) スプリットホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。

例 :

```
Device(config-if)#no ip split-horizon eigrp 109
```

ステップ 8 end

特権 EXEC モードに戻ります。

例 :

```
Device(config)# end
```

次のタスク

show ip eigrp interface を使用して、EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。

```
Device#show ip eigrp interface
```

設定を保存するには、**copy running-config startup-config** コマンドを入力します。

```
Device# copy runningconfig startup-config
```

IPv6 の EIGRP の設定

EIGRPv6 設定の前提条件

IPv6 用 EIGRP を実行するようにスイッチを設定する前に、次のグローバル設定が行われていることを確認します。

1. `ip routing` グローバルコンフィギュレーションコマンドを使用してルーティングをイネーブルにします。EIGRPv6 は IPv6 用ですが、一般にこのコマンドは、シスコデバイスのルーティング機能の前提条件になっています。
2. `ipv6 unicast-routing` グローバルコンフィギュレーションコマンドを使用して IPv6 パケットの転送をイネーブルにします。

```
ipv6 unicast-routing
```
3. レイヤ 3 インターフェイスでの IPv6 の有効化：IPv6 EIGRP を実行する予定のすべてのレイヤ 3 インターフェイスで IPv6 が有効になっていることを確認します。通常、これには、インターフェイスでの IPv6 アドレスの設定が含まれます。

明示的なルータ ID の設定

EIGRP for IPv6 にはルータ ID が必要です。IPv4 アドレスから派生した暗黙的なルータ ID が使用できない場合、または望ましくない場合は、明示的なルータ ID を設定できます。

- `show ipv6 eigrp` コマンドを使用して、現在設定されているルータ ID を表示できます。
- 特定の 32 ビットのルータ ID（多くの場合、IPv4 アドレスのようなドット付き 10 進数形式）を設定するには、EIGRP IPv6 ルータ コンフィギュレーション モード内で `router-id` コマンドを使用します。

EIGRP IPv6 インターフェイスおよびパッシブインターフェイスの設定

IPv4 用 EIGRP と同様に、EIGRP IPv6 プロセスに参加するインターフェイスを指定し、一部をパッシブとして指定できます。

- アクティブなインターフェイス：EIGRP IPv6 プロセスにインターフェイスを含めるには、通常、そのインターフェイスで直接 EIGRP IPv6 を有効にします。
- パッシブインターフェイス：`Passive-interface` コマンド（EIGRP IPv6 ルータ コンフィギュレーションモード内）を使用して、インターフェイスをパッシブにします。パッシブインターフェイスは、接続されたネットワークをアドバタイズすることによって EIGRP プロセスに参加しますが、そのインターフェイスで EIGRP Hello パケットや隣接関係を形成したり、受信したりすることはありません。
- パッシブインターフェイスのアクティブ化：インターフェイスがパッシブになっている場合、特定のインターフェイスでコマンドを使用して再度アクティブにして、EIGRP 隣接関係を形成できるようにします。

```
no passive-interface
```

- パッシブインターフェイスでの設定なし：EIGRP IPv6 は、パッシブインターフェイスで明示的に設定する必要はありません。パッシブインターフェイスコマンドは、EIGRPの動作を制御するだけです。

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

手順

ステップ 1 端末の有効化と設定

特権 EXEC モードを有効にします。要求された場合はパスワードを入力し、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。

例：

```
Device enable
Device# configure terminal
```

ステップ 2 interface *interface-id*

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、設定するレイヤ 3 インターフェイスを指定します。

例：

```
Device(config)#interface gigabitethernet 1/0/1
```

ステップ 3 ip authentication mode eigrp *autonomous-system md5*

IP EIGRP パケットの MD5 認証をイネーブルにします。

例：

```
Device(config-if)# ip authentication mode eigrp 104 md5
```

ステップ 4 ip authentication key-chain eigrp *autonomous-system keychain*

IP EIGRP パケットの認証をイネーブルにします。

例：

```
Device(config-if)#ip authentication key-chain eigrp 105 chain1
```

ステップ 5 exit

グローバル コンフィギュレーション モードに戻ります。

例：

```
Device(config-if)# exit
```

ステップ6 key chainname-of-chain

キーチェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。ステップ4で設定した名前を指定します。

例：

```
Device(config)#key chain chain1
```

ステップ7 key [number]

キーチェーン コンフィギュレーション モードで、キー番号を識別します。キーチェーン コンフィギュレーション モードで、キー スtring を識別します。key-string text を使用します。

例：

```
Device(config-keychain)#key 1  
Device(config-keychainkey)# key-string key1
```

ステップ8 accept-lifetime starttime {infinite | endtime | duration seconds}

(任意) キーを受信できる期間を指定します。

start-time および end-time 構文には、hh:mm:ss Month date year または hh:mm:ss date Month year のいずれかを使用できます。デフォルトは、デフォルトの starttime 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの endtime および duration は infinite です。

例：

```
Device(config-keychainkey)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
```

ステップ9 send-lifetime starttime {infinite | endtime | duration seconds}

(任意) キーを送信できる期間を指定します。

start-time および end-time 構文には、hh:mm:ss Month date year または hh:mm:ss date Month year のいずれかを使用できます。デフォルトは、デフォルトの starttime 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの endtime および duration は infinite です。

例：

```
Device(config-keychainkey)#send-lifetime 14:00:00 Jan 25 2011 duration 3600  
Device (config) # end
```

次のタスク

show key chain を使用して認証キーの情報を表示します。

```
Device# show key chain
```

設定を保存するには、**copy running-config startup-config** コマンドを入力します。

```
Device# copy runningconfig startup-config
```


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。