Cisco Nexus 5000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド リリース 5.0(3)N1(1)

2011 年 3 月

Text Part Number: OL-23800-01-J

【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。

Cisco Nexus 5000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド リリース 5.0(3)N1(1)

CONTENTS

はじめに

このマニュアルでは、Cisco Nexus 5000 シリーズ スイッチでの Cisco NX-OS ユニキャスト ルーティングの設定の詳細について説明します。

この章では、次の内容について説明します。

対象読者

このマニュアルを使用するには、IP およびルーティングのテクノロジーに関する詳しい知識が必要です。

サポートされるスイッチ

内容は次のとおりです。

Cisco Nexus 5500 プラットフォーム スイッチ

表 ii-1 に、Cisco Nexus 5500 プラットフォームでサポートされる Cisco スイッチを示します。

（注） これらのスイッチの詳細については、次の URL にある『*Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide*』を参照してください。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

表 ii-1　サポートされる Cisco Nexus 5500 プラットフォーム スイッチ

スイッチ	説明
Cisco Nexus 5548P スイッチ	Cisco Nexus 5548P スイッチは、Cisco Nexus 5500 プラットフォームの最初のスイッチです。このスイッチは、1 Rack-Unit（1 RU）の 10 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）スイッチであり、最大 960 Gbps スループットおよび最大 48 ポートを提供します。
Cisco Nexus 5596P スイッチ	Cisco Nexus 5596P スイッチは、Top-of-Rack の 10 ギガビット イーサネットおよび FCoE スイッチであり、最大 1920 ギガビット スループットおよび最大 96 ポートを提供します。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

タイトル	説明
第 1 章「概要」	ユニキャスト ルーティングの概要と各機能の簡単な説明を示します。
第 2 章「IPv4 の設定」	ARP と ICMP を含む IPv4 を設定し、管理する手順について説明します。
第 3 章「OSPFv2 の設定」	IPv4 ネットワークのための OSPFv2 ルーティング プロトコルを設定する手順について説明します。
第 4 章「EIGRP の設定」	IPv4 ネットワークのための Cisco EIGRP ルーティング プロトコルを設定する手順について説明します。
第 5 章「ベーシック BGP の設定」	IPv4 ネットワークのための BGP ルーティング プロトコルの基本機能を設定する手順について説明します。
第 6 章「拡張 BGP の設定」	ルート再配布とルート集約を含む、IPv4 ネットワークのための BGP ルーティング プロトコルの高度な機能を設定する手順について説明します。
第 7 章「RIP の設定」	IPv4 ネットワークのための RIP ルーティング プロトコルを設定する手順について説明します。
第 8 章「スタティック ルーティングの設定」	IPv4 ネットワークのためのスタティック ルーティングを設定する手順について説明します。
第 9 章「レイヤ 3 仮想化の設定」	レイヤ 3 仮想化を設定する手順について説明します。
第 10 章「ユニキャスト RIB および FIB の管理」	ユニキャスト RIB および FIB を表示および変更する方法について説明します。
第 11 章「Route Policy Manager の設定」	フィルタリングおよび再配布用の IP プレフィクス リストとルート マップを含む Route Policy Manager を設定する手順について説明します。
第 12 章「HSRP の設定」	Hot Standby Routing Protocol を設定する手順について説明します。
第 13 章「VRRP の設定」	Virtual Router Redundancy Protocol を設定する手順について説明します。

タイトル	説明
第 14 章「オブジェクト トラッキングの設定」	オブジェクト トラッキングを設定する手順について説明します。
付録 A「Cisco NX-OS Unicast Features Release 5.0(3)N1(1) がサポートする IETF RFC」	Cisco NX-OS にサポートされている IETF RFC を示します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
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ています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	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。
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。

出力例では、次の表記法を使用しています。

`screen フォント`	スイッチに表示される端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
`イタリック体の screen フォント`	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	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ます。

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」を意味します。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。

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。

関連資料

Cisco Nexus 5000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ Fabric Extender のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

次に、Cisco Nexus 5000 シリーズおよび Cisco Nexus 2000 シリーズ Fabric Extender に関連するマニュアルを示します。

リリース ノート

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes』

『Cisco Nexus 5000 Series Switch Release Notes』

コンフィギュレーション ガイド

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(3)N1(1)』

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)』

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)』

『Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide』

『Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Security Configuration Guide』

『Cisco Nexus 5000 Series NX-OS System Management Configuration Guide』

『Cisco Nexus 5000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド』

『Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide』

『Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)』

『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2』

『Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide』

メンテナンスおよび操作ガイド

『Cisco Nexus 5000 Series NX-OS Operations Guide』

インストレーション ガイドおよびアップグレード ガイド

『Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide』

『Cisco Nexus 2000 Series Hardware Installation Guide』

『Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)』

『Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders』

ライセンス ガイド

『Cisco NX-OS Licensing Guide』

コマンド リファレンス

『Cisco Nexus 5000 Series Command Reference』

テクニカル リファレンス

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference』

エラー メッセージおよびシステム メッセージ

『Cisco NX-OS System Messages Reference』

トラブルシューティング ガイド

『Cisco Nexus 5000 Troubleshooting Guide』

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、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』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/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』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。

新機能と変更された機能

この章では、『Cisco Nexus 5000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド リリース 5.0(3)N1(1)』に記載されている新機能および変更された機能について、リリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

Cisco NX-OS Release 5.x に関するその他の情報については、次のシスコ Web サイトから入手できる『*Cisco Nexus 5000 Series Switch NX-OS Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

表 1 では、Cisco Nexus 5000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド リリース 5.0(3)N1(1) における新機能および変更された機能を要約し、その参照先を示しています。

表 1　　リリース 5.0(3)N1(1) の新機能および変更された機能

機能	説明	変更されたリリース	参照先
IPv4	この機能が導入されました。 次のインターネット プロトコル バージョン 4（IPv4）機能を Cisco NX-OS スイッチに設定できます。 • IPv4 アドレス指定 • アドレス解決プロトコル（ARP） • インターネット制御メッセージ プロトコル（ICMP）	5.0(3)N1(1)	第 2 章「IPv4 の設定」
OSPFv2	この機能が導入されました。 IPv4 ネットワークに対して、次の基本的および高度な Open Shortest Path First Version 2（OSPFv2）機能を設定できます。 • OSPF インスタンス • OSPFv2 認証 • フィルタ リスト • 仮想リンク • スタブ ルート • ルートの再配布	5.0(3)N1(1)	第 3 章「OSPFv2 の設定」
EIGRP	この機能が導入されました。 次の基本的および高度な Enhanced Interior Gateway Routing Protocol（EIGRP）機能を Cisco NX-OS スイッチに設定できます。 • EIGRP インスタンス • スタブ ルーティング • サマリー アドレス • EIGRP 認証 • ルートの再配布	5.0(3)N1(1)	第 4 章「EIGRP の設定」
BGP	この機能が導入されました。 次の基本的および高度なボーダー ゲートウェイ プロトコル（BGP）機能を Cisco NX-OS スイッチに設定できます。 • BGP インスタンス • BGP ピア • テンプレート • プレフィクス ピアリング • BGP 認証 • ネクストホップ アドレス	5.0(3)N1(1)	第 5 章「ベーシック BGP の設定」 第 6 章「拡張 BGP の設定」

表 1　　リリース 5.0(3)N1(1) の新機能および変更された機能 （続き）

機能	説明	変更されたリリース	参照先
RIP	この機能が導入されました。 次の Routing Information Protocol（RIP）機能を Cisco NX-OS スイッチに設定できます。 • RIPv2 認証 • スプリット ホライズン • ルート フィルタリング • ルート集約 • ルートの再配布 • 仮想化	5.0(3)N1(1)	第 7 章「RIP の設定」
スタティック ルーティング	この機能が導入されました。 Cisco NX-OS スイッチにスタティック ルーティングを設定できます。	5.0(3)N1(1)	第 8 章「スタティック ルーティングの設定」
レイヤ 3 仮想化	この機能が導入されました。 Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンス、および VRF-lite を Cisco NX-OS スイッチに設定できます。	5.0(3)N1(1)	第 9 章「レイヤ 3 仮想化の設定」
ユニキャスト RIB および FIB	この機能が導入されました。 Cisco NX-OS スイッチでユニキャスト Routing Information Base（RIB; ルーティング情報ベース）および Forwarding Information Base（FIB; 転送情報ベース）のルートを管理できます。	5.0(3)N1(1)	第 10 章「ユニキャスト RIB および FIB の管理」
Route Policy Manager	この機能が導入されました。 Route Policy Manager を Cisco NX-OS スイッチに設定し、プリフィクス リスト、AS-path リスト、コミュニティ リストを指定できます。	5.0(3)N1(1)	第 11 章「Route Policy Manager の設定」
HSRP	この機能が導入されました。 Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）を Cisco NX-OS スイッチに設定できます。	5.0(3)N1(1)	第 12 章「HSRP の設定」

表 1　　リリース 5.0(3)N1(1) の新機能および変更された機能 （続き）

機能	説明	変更されたリリース	参照先
VRRP	この機能が導入されました。 次の Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）を Cisco NX-OS スイッチに設定できます。 • VRRP グループ • 仮想ルータのプライオリティ • 単純なテキスト認証 • インターフェイスのステート追跡	5.0(3)N1(1)	第 13 章「VRRP の設定」
オブジェクト トラッキング	この機能が導入されました。 Cisco NX-OS スイッチにトラッキングを設定して、インターフェイス ライン プロトコル ステート、IP ルーティング、ルート到達可能性などのスイッチ上の特定のオブジェクトをトラッキングできます。	5.0(3)N1(1)	第 14 章「オブジェクト トラッキングの設定」

CHAPTER 1

概要

この章では、Cisco NX-OS でのレイヤ 3 ユニキャスト ルーティング プロトコルの基盤となる概念を紹介します。

この章では、次の内容について説明します。

レイヤ 3 ユニキャスト ルーティングについて

レイヤ 3 ユニキャスト ルーティングには、最適なルーティング パスの決定とパケットの交換という、2 つの基本的動作があります。ルーティング アルゴリズムを使用すると、ルータから宛先までの最適なパス（経路）を計算できます。この計算方法は、選択したアルゴリズム、ルート メトリック、そしてロード バランシングや代替パスの探索などの考慮事項により異なります。

ここでは、次の内容について説明します。

ルーティングの基本

ルーティング プロトコルは、*メトリック*を使用して、宛先までの最適なパスを調べます。メトリックとは、パス帯域幅などの、ルーティング アルゴリズムが宛先までの最適なパスを決定するために使用する測定基準です。パスを決定しやすいように、ルーティング アルゴリズムは、ルート情報（IP 宛先アドレス、および次のルータまたは*ネクスト ホップ*のアドレスなど）を含むルーティング テーブルを初期化して維持します。宛先とネクストホップの関連付けにより、ルータは、宛先までの途中にあるネクストホップとなる特定のルータにパケットを送信すると、最適なパスで IP 宛先まで届けられることを判定できます。ルータは、着信パケットを受信すると、宛先アドレスをチェックし、このアドレスをネクストホップと関連付けようとします。ルート テーブルの詳細については、「ユニキャスト RIB」（P.1-10）を参照してください。

ルーティング テーブルには、パスの優先度に関するデータなどのその他の情報も含まれる場合があります。ルータはメトリックを比較して、最適なルートを決定します。また、これらのメトリックは、使用されるルーティング アルゴリズムの設計により異なります。「ルーティング メトリック」（P.1-3）を参照してください。

各ルータは互いに通信し、さまざまなメッセージを送信して、そのルーティング テーブルを維持します。ルーティング更新メッセージは、ルーティング テーブルの全部または一部で構成されるメッセージです。ルータは、他のすべてのルータからのルーティング更新情報を分析して、ネットワーク トポロジの詳細な図を構築できます。ルータ間で送信されるもう 1 つのメッセージであるリンクステート アドバタイズメントは、他のルータに、送信側ルータのリンク状態を通知します。リンク情報を使用して、ルータが、ネットワーク宛先までの最適なルートを決定できるようにすることもできます。詳細については、「ルーティング アルゴリズム」（P.1-8）を参照してください。

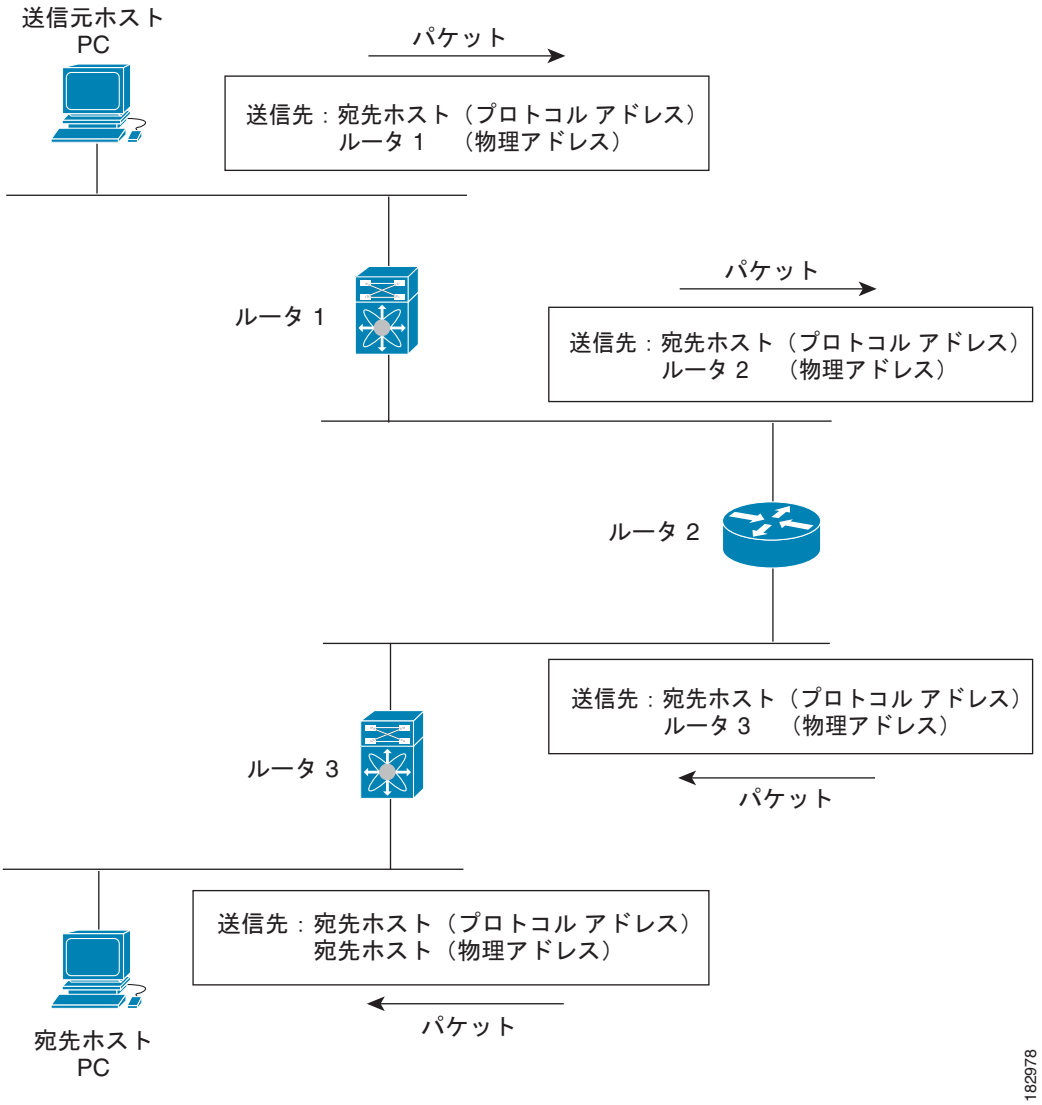
パケット交換

パケット交換では、ホストが、パケットを別のホストに送信する必要があることを決定します。なんらかの方法でルータのアドレスを入手したら、送信元ホストはパケットを明確に、宛先ホストの IP（ネットワーク層）アドレスを含むルータの物理（Media Access Control（MAC）層）アドレス宛てに送信します。

ルータは宛先の IP アドレスを調べ、ルーティング テーブルでその IP アドレスを探します。ルータでパケットの転送方法がわからない場合は、パケットは通常、廃棄されます。パケットの転送方法がわかった場合、ルータは、宛先の MAC アドレスをネクストホップ ルータの MAC アドレスに変更し、パケットを送信します。

ネクストホップが宛先のホストである場合や、同じ交換決定処理を行う別のルータである場合があります。パケットがネットワーク間を移動するにつれ、その物理アドレスは変更されますが、そのプロトコル アドレスは変わりません（図 1-1 を参照）。

図 1-1　ネットワーク上でのパケット ヘッダーの更新



ルーティング メトリック

ルーティング アルゴリズムは、多くの異なるメトリックを使用して最適なルートを決定します。高度なルーティング アルゴリズムは、複数のメトリックに基づいてルートを選択している場合があります。

ここでは、次のメトリックについて説明します。

- 「パス長」（P.1-4）
- 「信頼性」（P.1-4）
- 「ルーティング遅延」（P.1-4）
- 「帯域幅」（P.1-4）
- 「負荷」（P.1-4）
- 「通信コスト」（P.1-4）

パス長

パス長 は、最も一般的なルーティング メトリックです。一部のルーティング プロトコルでは、各ネットワーク リンクに恣意的なコストの割り当てが可能です。この場合、パスの長さは、経由した各リンクに関連付けられたコストの合計となります。それ以外のルーティング プロトコルでは、パケットが送信元から宛先までに経由する必要のある、ルータなどのネットワーク間製品の通過回数を指定するメトリックであるホップ数が定義されます。

信頼性

ルーティング アルゴリズムとの関連における*信頼性*は、各ネットワーク リンクの信頼性（ビット誤り率で示される）です。一部のネットワーク リンクは、他のネットワーク リンクよりダウンする頻度が高い場合があります。ネットワークがダウンしたあと、特定のネットワーク リンクが他のリンクより容易に、または短時間に修復される場合もあります。信頼性のランクを割り当てるときに考慮できる信頼性係数は、一般的にネットワーク リンクに割り当てる任意の数値です。

ルーティング遅延

ルーティングは、*遅延*送信元から宛先に、インターネットワークを通過してパケットを移動するために必要な時間の長さです。遅延は、中間のネットワーク リンクの帯域幅、経由する各ルータでのポート キュー、中間の全ネットワーク リンクでのネットワークの混雑状況、パケットが移動する物理的な距離など、多くの要素に応じて異なります。ルーティング遅延はいくつかの重要な変数の組み合わせであるため、一般的で便利なメトリックです。

帯域幅

帯域幅 は、リンクで使用可能なトラフィック容量です。たとえば、10 ギガビット イーサネット リンクは 1 ギガビット イーサネット リンクより容量が大きく、優れています。帯域幅は、リンクで達成可能な最大スループットですが、帯域幅のより大きいリンクを経由するルートが、帯域幅のより小さいリンクを経由するルートより優れているとは限りません。たとえば、帯域幅の大きいリンクの方が混雑していると、実際には、パケットを宛先に送信するためにさらに長い時間がかかる場合があります。

負荷

*負荷*は、ルータなどのネットワーク リソースの使用状況の程度です。負荷は、CPU 使用状況や処理される 1 秒あたりのパケット数など、さまざまな方法で計算できます。これらのパラメータを継続的にモニタすると、リソースに負担がかかる場合があります。

通信コスト

通信コスト は、リンク上でルーティングするための稼動コストの測定単位です。通信コストは重要なメトリックの 1 つで、特にパフォーマンスより稼動コストの削減が優先される場合に使用されます。たとえば、専用回線での回線遅延が公衆回線より大きくても、使用時間に応じて課金される公衆回線上でなく、自身の専用回線上でパケットを送信できます。

ルータ ID

各ルーティング処理には、*ルータ ID* が関連付けられています。ルータ ID は、システムのあらゆるインターフェイスに設定できます。ルータ ID を設定しないと、Cisco NX-OS が次の基準に基づいて、ルータ ID を選択します。

- Cisco NX-OS は、他のあらゆるインターフェイス上で loopback0 を優先します。loopback0 が存在しない場合、Cisco NX-OS は、他のあらゆるインターフェイス タイプ上で最初のループバックを優先します。
- 設定済みのループバック インターフェイスがない場合、Cisco NX-OS は、コンフィギュレーション ファイル中の最初のインターフェイスをルータ ID として使用します。Cisco NX-OS がルータ ID を選択したあとにいずれかのループバック インターフェイスを設定した場合は、ループバック インターフェイスがルータ ID となります。ループバック インターフェイスが loopback0 ではなく、あとで loopback0 を IP アドレスで設定した場合は、ルータ ID が loopback0 の IP アドレスに変更されます。
- ルータ ID の元であるインターフェイスが変更されると、新しい IP アドレスがルータ ID となります。他のどのインターフェイスの IP アドレスが変更されても、ルータ ID はまったく変更されません。

自律システム

自律システム（AS）とは、単一の技術的管理エンティティにより制御されるネットワークです。AS により、グローバルな外部ネットワークが個々のルーティング ドメインに分割され、これらのドメインでは、ローカルのルーティング ポリシーが適用されます。この構成により、ルーティング ドメインの管理と一貫したポリシー設定が簡素化されます。

各 AS は、ルート *再配布*により動的にルーティング情報を交換する、複数の内部ルーティング プロトコルをサポートできます。地域インターネット レジストリにより、インターネットに直接接続する各公共 AS に一意の番号が割り当てられます。この AS 番号で、ルーティング処理と AS の両方が識別されます。

Cisco NX-OS は、4 バイトの AS 番号をサポートします。表 1-1 は、AS 番号の範囲を示します。

表 1-1　AS 番号

2 バイト番号	AS ドット表記での 4 バイト番号	プレーンテキスト表記での 4 バイト番号	目的
1 ～ 64511	0.1 ～ 0.64511	1 ～ 64511	公共 AS（RIR により割り当てられる）[1]
64512 ～ 65534	0.64512 ～ 0.65534	64512 ～ 65534	専用 AS（ローカルの管理者により割り当てられる）
65535	0.65535	65535	予約済み
N/A	1.0 ～ 65535.65535	65536 ～ 4294967295	公共 AS（RIR により割り当てられる）

1. RIR = 地域インターネット レジストリ（Regional Internet Registries）

専用 AS 番号は内部ルーティング ドメインに使用されますが、インターネット上にルーティングされたトラフィック向けに、ルータにより変換される必要があります。ルーティング プロトコルを、専用 AS 番号が外部ネットワークにアドバタイズされるように設定しないでください。デフォルトでは、Cisco NX-OS は専用 AS 番号をルーティング更新情報から削除しません。

（注）　公共ネットワークおよび専用ネットワークの AS 番号は、Internet Assigned Number Authority（IANA; インターネット割り当て番号局）により管理されています。予約済み番号の割り当てを含む AS 番号の詳細について、または、AS 番号の登録を申請するには、次の URL を参照してください。
http://www.iana.org/

コンバージェンス

ルーティング アルゴリズム測定の鍵となる要素の 1 つは、ルータがネットワーク トポロジの変化に対応するために要する時間です。リンク障害など、なんらかの理由でネットワークの一部が変化すると、さまざまなルータのルーティング情報が一致しなくなる場合があります。変化したトポロジに関する情報が更新されているルータと、古い情報が残っているルータがあるためです。*コンバージェンス*は、ネットワーク内のすべてのルータが更新され、ルーティング情報が一致するまでにかかる時間の長さです。コンバージェンス時間は、ルーティング アルゴリズムによって異なります。コンバージェンスが速い場合は、不正確なルーティング情報によるパッケージ損失の可能性が小さくなります。

ロード バランシングおよび等コスト マルチパス

ルーティング プロトコルでは、*ロード バランシング*または等コスト マルチパス（ECMP）を使用して、複数のパス上のトラフィックを共有できます。ルータは、特定のネットワークへのルートを複数検出すると、最もアドミニストレーティブ ディスタンスの低いルートをルーティング テーブルにインストールします。ルータが、同じアドミニストレーティブ ディスタンスと宛先までのコストを持つ複数のパスを受信し、インストールすると、ロード バランシングが発生する場合があります。ロード バランシングでは、すべてのパス上にトラフィックが配布され、負荷が共有されます。使用されるパスの数は、ルーティング プロトコルによりルーティング テーブルに配置されるエントリの数に制限されます。Cisco NX-OS は、宛先までの 16 のパスをサポートします。

Enhanced Interior Gateway Routing Protocol（EIGRP）は、等コストでないロード バランシングもサポートしています。詳細については、第 4 章「EIGRP の設定」を参照してください。

ルートの再配布

ネットワークに複数のルーティング プロトコルが設定されている場合は、各プロトコルでルート再配布を設定して、ルーティング情報を共有するように設定できます。たとえば、OSPF（Open Shortest Path First）を設定して、Border Gateway Protocol（BGP）で検出したルートをアドバタイズできます。また、スタティック ルートを、どのダイナミック ルーティング プロトコルにも再配布できます。別のプロトコルからのルートを再配布しているルータは、その再配布ルートに対する固定ルート メトリックを設定します。これにより、異なるルーティング プロトコル間で互換性のないルート メトリックの問題が回避されます。たとえば、EIGRP から OSPF に再配布されたルートには、OSPF が認識できる固定リンク コスト メトリックが割り当てられます。

ルート再配布では、アドミニストレーティブ ディスタンス（「アドミニストレーティブ ディスタンス」（P.1-7）を参照）の使用によっても、2 つの異なるルーティング プロトコルで検出されたルートが区別されます。優先ルーティング プロトコルには、より低いアドミニストレーティブ ディスタンスが与えられており、そのルートが、より高いアドミニストレーティブ ディスタンスが割り当てられた他のプロトコルからのルートに優先して選択されます。

アドミニストレーティブ ディスタンス

アドミニストレーティブ ディスタンス は、ルーティング情報の送信元の信頼性のランクです。値が高いほど、信頼性のランクは低くなります。一般的にルートは、複数のプロトコルを通じて検出されます。アドミニストレーティブ ディスタンスは、複数のプロトコルで検出されたルートを区別するために使用されます。最もアドミニストレーティブ ディスタンスが低いルートが IP ルーティング テーブルにインストールされます。

スタブ ルーティング

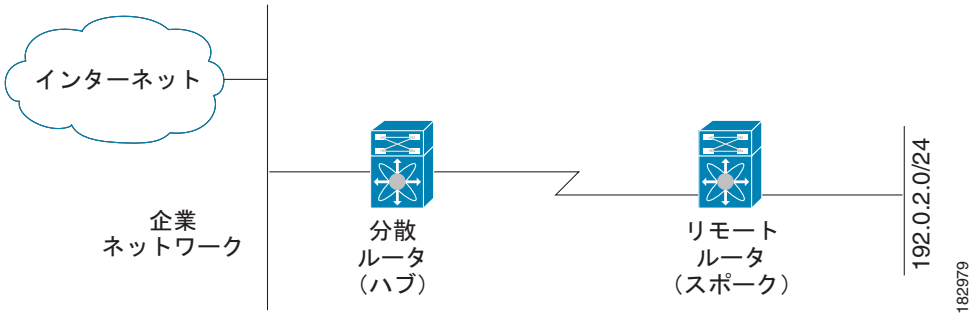
スタブ ルーティングはハブ アンド スポーク型ネットワーク トポロジで使用できます。このトポロジでは、1 つ以上の終端（スタブ）ネットワークが、1 つ以上の分散ルータ（ハブ）に接続されたリモート ルータ（スポーク）に接続されています。リモート ルータは、1 つ以上の分散ルータにのみ隣接しています。リモート ルータへと流れる IP トラフィックのルートは、分散ルータ経由のルートのみです。このタイプの設定は、分散ルータが直接 WAN に接続されている WAN トポロジで使用されるのが一般的です。分散ルータは、さらに多くのリモート ルータに接続できます。分散ルータが 100 台以上のリモート ルータに接続されていることも、よくあります。ハブ アンド スポーク型トポロジでは、リモート ルータがすべての非ローカル トラフィックを分散ルータに転送する必要があります。これにより、リモート ルータが完全なルーティング テーブルを保持する必要はなくなります。通常、分散ルータは、デフォルトのルートのみをリモート ルータに送信します。

指定されたルートのみが、リモート（スタブ）ルータから伝播されます。スタブ ルータは、要約、接続したルート、再配布されたスタティック ルート、外部ルート、内部ルートに対する照会のすべてに、「アクセスできない」メッセージで対応します。スタブとして設定されたルータは、すべての隣接ルータに特別なピア情報パケットを送信して、自身のスタブ ルータとしての状態を報告します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、配布ルータに依存して適切なアップデートをすべてのピアに送信します。

図 1-2 は、単純なハブ アンド スポーク型設定を示します。

図 1-2　単純なハブ アンド スポーク ネットワーク



スタブ ルーティングを使用する場合でも、リモート ルータにルータをアドバタイズできます。図 1-2 は、リモート ルータが、分散ルータのみを使用して企業ネットワークとインターネットにアクセスできることを示しています。この例では、企業ネットワークとインターネットへのパスが常に分散ルータを経由するため、リモート ルータ上の完全なルート テーブルの機能は無意味です。より大規模なルート テーブルを使用しても、リモート ルータに必要なメモリの量が削減されるだけです。使用される帯域幅とメモリは、分散ルータでルートを要約し、フィルタリングすると、削減できます。このネットワーク トポロジでリモート ルータは、他のネットワークから検出されたルートを受信する必要はあり

ません。これは、宛先がどこであっても、リモート ルータは、すべての非ローカル トラフィックを分散ルータに送信する必要があるためです。真のスタブ ネットワークを設定するには、リモート ルータへのデフォルト ルートのみを送信するよう、分散ルータを設定する必要があります。

OSPF はスタブ エリアをサポートしており、EIGRP はスタブ ルータをサポートしています。

ルーティング アルゴリズム

ルーティング アルゴリズムは、ルータが到達可能性の情報を収集し、報告する方法、トポロジの変化に対応する方法、および宛先までの最適なルートを決定する方法を決定します。ルーティング アルゴリズムにはさまざまなタイプがあり、各アルゴリズムがネットワークやルータ リソースに与える影響もさまざまです。ルーティング アルゴリズムは、最適なルートの計算に影響するさまざまなメトリックを使用します。ルーティング アルゴリズムは、スタティックまたはダイナミック、内部または外部など、タイプで分類できます。

ここでは、次の内容について説明します。

スタティック ルートおよびダイナミック ルーティング プロトコル

スタティック ルートは、手動で設定するルート テーブル エントリです。スタティック ルートは、手動で再設定しない限り、変更されません。スタティック ルートは設計が簡単で、ネットワーク トラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。

スタティック ルーティング システムはネットワークの変化に対応できないため、絶えず変化する、今日の大規模ネットワークには使用しないでください。今日のほとんどのルーティング プロトコルは、ダイナミック ルーティング アルゴリズムを使用しています。このアルゴリズムでは、着信ルーティング更新メッセージを分析して、ネットワーク状況の変化に合わせて調整します。メッセージがネットワークの変化を示している場合は、ルーティング ソフトウェアがルートを計算し直して、新しいルーティング更新メッセージを送信します。これらのメッセージがネットワークを通過すると、ルータがそのアルゴリズムを再実行し、それに従ってルーティング テーブルを変更します。

適切であれば、ダイナミック ルーティング アルゴリズムをスタティック ルートで補完することができます。たとえば、各サブネットワークに IP *デフォルト ゲートウェイ*または、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータ）へのスタティック ルートを設定する必要があります。

内部および外部ゲートウェイ プロトコル

ネットワークを、一意のルーティング ドメインまたは AS に分割できます。AS は、管理ガイドラインの特定のセットで規制された共通の管理機関の下の内部ネットワークの一部です。AS 間でのルートを設定するルーティング プロトコルは、外部ゲートウェイ プロトコルまたはドメイン間プロトコルと呼ばれます。BGP は、外部ゲートウェイ プロトコルの例です。1 つの AS 内で使用されるルーティング プロトコルは、内部ゲートウェイ プロトコルまたはドメイン内プロトコルと呼ばれます。EIGRP および OSPF は、内部ゲートウェイ プロトコルの例です。

ディスタンス ベクトル プロトコル

ディスタンス ベクトル プロトコルは*ディスタンス ベクトル*アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれます）を使用します。このアルゴリズムにより、各ルータは、そのルーティング テーブルの一部または全部をネイバー ルータに送信します。ディスタンス ベクトル アルゴリズムでは、ルートが、ディスタンス（宛先までのホップ数など）および方向（ネクストホップ ルータなど）により定義されます。その後、これらのルートは、直接接続されたネイバー ルータにブロードキャストされます。各ルータは、これらの更新情報を使用して、ルーティング テーブルを確認し、更新します。

ルーティング ループを防ぐために、ほとんどのディスタンス ベクトル アルゴリズムは*ポイズン リバースを指定したスプリット ホライズン*を使用します。これは、インターフェイスで検出されたルートを到達不能として設定し、それをそのインターフェイスで、次の定期更新中にアドバタイズするという意味です。この機能により、ルータによるルート更新が、そのルータ自体に返信されなくなります。

ディスタンス ベクトル アルゴリズムは、一定の間隔で更新を送信しますが、ルート メトリックの値の変更に応じて、更新を送信することもできます。このように送信された更新により、ルート コンバージェンス時間の短縮が可能です。Routing Information Protocol（RIP）はディスタンス ベクトル プロトコルの 1 つです。

リンクステート プロトコル

リンクステート プロトコルは、SPF（最短パス優先）とも呼ばれ、情報を隣接ルータと共有します。各ルータはリンクステート アドバタイズメント（LSA）を構築し、ここに、各リンクおよび直接接続されたネイバー ルータに関する情報が含まれます。

各 LSA にはシーケンス番号があります。ルータが LSA を受信し、そのリンクステート データベースを更新すると、LSA がすべての隣接ネイバーにフラッディングされます。ルータが同じシーケンス番号の 2 つの LSA（同じルータからの）を受信した場合は、LSA 更新ループを防ぐために、ルータは最後に受信した LSA をネイバー ルータにフラッディングしません。ルータは、受信直後に LSA をフラッディングするため、リンクステート プロトコルのコンバージェンス時間は最小となります。

ネイバー ルータの探索と隣接関係の確立は、リンクステート プロトコルの重要な部分です。ネイバー ルータは、特別な hello パケットを使用して探索されます。このパケットは、各ネイバー ルータのキープアライブ通知としても機能します。隣接関係は、ネイバー ルータ間のリンクステート プロトコルの一般的な動作パラメータ セットで確立されます。

ルータが受信した LSA は、そのリンクステート データベースに追加されます。各エントリは、次のパラメータで構成されます。

- ルータ ID（LSA を構築したルータの）
- ネイバー ID
- リンク コスト
- LSA のシーケンス番号
- LSA エントリの作成時からの経過時間

ルータは、リンクステート データベース上で SPF アルゴリズムを実行し、そのルータの最短パス ツリーを構築します。この SPF ツリーを使用して、ルーティング テーブルにデータが入力されます。

リンクステート アルゴリズムでは、各ルータがそのルーティング テーブル内に、ネットワーク全体の図を構築します。リンクステート アルゴリズムが小さな更新を全体的に送信するのに対し、ディスタンス ベクトル アルゴリズムは、より大きな更新を隣接ルータのみに送信します。

リンクステート アルゴリズムは、より短時間でコンバージェンスするため、ディスタンス ベクトル アルゴリズムより、ルーティング ループがやや発生しにくくなっています。ただし、リンクステート アルゴリズムはディスタンス ベクトル アルゴリズムより、大きな CPU パワーとメモリを必要とします。リンクステート アルゴリズムは、実装とサポートにより多くの費用がかかる場合があります。リンクステート プロトコルは通常、ディスタンス ベクトル プロトコルよりスケーラブルです。

OSPF は、リンクステート プロトコルの一例です。

レイヤ 3 仮想化

Cisco NX-OS は、複数の Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンス、および複数の Routing Information Base（RIB）をサポートしているため、複数のアドレス ドメインがサポートされます。各 VRF は RIB と関連付けられ、この情報が Forwarding Information Base（FIB; 転送情報ベース）により収集されます。VRF は、レイヤ 3 アドレス指定ドメインを表します。各レイヤ 3 インターフェイス（論理または物理）は、1 つの VRF に属します。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

Cisco NX-OS 転送アーキテクチャ

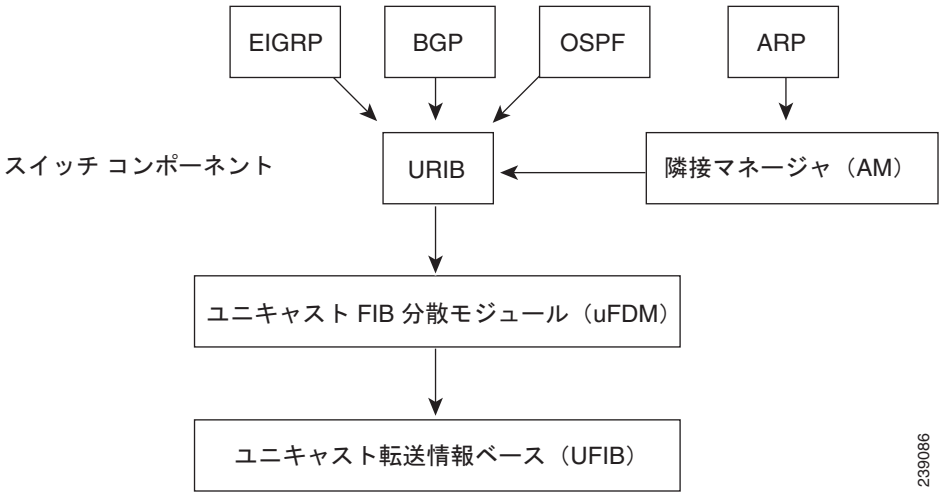
Cisco NX-OS フォワーディング アーキテクチャは、スイッチにおけるすべてのルーティング アップデートの処理および転送情報の入力を担います。

ここでは、次の内容について説明します。

ユニキャスト RIB

Cisco NX-OS 転送アーキテクチャは、図 1-3 に示すように、複数のコンポーネントで構成されます。

図 1-3　Cisco NX-OS 転送アーキテクチャ



ユニキャスト RIB は、直接接続のルート、スタティック ルート、ダイナミック ユニキャスト ルーティング プロトコルで検出されたルートを含むルーティング テーブルを維持しています。また、アドレス解決プロトコル（ARP）などの送信元から、隣接情報を収集します。ユニキャスト RIB は、ルートに最適なネクストホップを決定し、さらにユニキャスト FIB Distribution Module（FDM; FIB 分散モジュール）のサービスを使用して、ユニキャスト Forwarding Information Base（FIB; 転送情報ベース）にデータを入力します。

各ダイナミック ルーティング プロトコルは、タイム アウトしたあらゆるルートについて、ユニキャスト RIB を更新する必要があります。そのあと、ユニキャスト RIB はそのルートを削除し、そのルートに最適なネクストホップを再計算します（代わりに使用できるパスがある場合）。

隣接マネージャ

隣接マネージャは、ARP、Open Shortest Path First version 2（OSPFv2）、Neighbor Discovery Protocol（NDP; ネイバー探索プロトコル）、静的な設定を含む、異なるプロトコルの隣接情報を維持しています。最も基本的な隣接情報は、これらのプロトコルで探索されたレイヤ 3 からレイヤ 2 へのアドレス マッピングです。発信レイヤ 2 パケットは、隣接情報を使用して、レイヤ 2 ヘッダーの作成を終了します。

隣接マネージャは、ARP 要求による、レイヤ 3 からレイヤ 2 への特定のマッピングの探索をトリガーできます。新しいマッピングは、対応する ARP 返信を受信し、処理すると、使用できるようになります。

ユニキャスト転送分散モジュール

ユニキャスト転送分散モジュールは、ユニキャスト RIB およびその他の送信元からの転送パス情報を配布します。ユニキャスト RIB は、ユニキャスト FIB がハードウェア転送テーブルにプログラムする転送情報を生成します。また、ユニキャスト転送分散モジュールは、新規挿入されたモジュールへの FIB 情報のダウンロードも行います。

ユニキャスト転送分散モジュールは、隣接情報を収集し、ユニキャスト FIB でのルートの更新時に、この情報およびその他のプラットフォーム依存の情報を書き直し（リライトし）ます。隣接情報およびリライト情報には、インターフェイス、ネクストホップ、およびレイヤ 3 からレイヤ 2 へのマッピング情報が含まれています。インターフェイスとネクストホップの情報は、ユニキャスト RIB からのルート更新情報で受信します。レイヤ 3 からレイヤ 2 へのマッピングは、隣接マネージャから受信します。

FIB

ユニキャスト FIB は、ハードウェア転送エンジンに使用される情報を作成します。ユニキャスト FIB は、ユニキャスト転送分散モジュールからルート更新情報を受信し、ハードウェア転送エンジンにプログラミングされるよう、この情報を送信します。ユニキャスト FIB は、ルート、パス、隣接関係の追加、削除、変更を管理します。

ユニキャスト FIB は、VRF ごとおよびアドレス ファミリごとに維持されます。ルート更新メッセージに基づいて、ユニキャスト FIB は、VRF ごとのプレフィクスとネクストホップ隣接情報データベースを維持します。ネクストホップ隣接データ構造には、ネクストホップの IP アドレスとレイヤ 2 リライト情報が含まれます。同じネクストホップ隣接情報構造を複数のプレフィクスで使用できます。

またユニキャスト FIB は、インターフェイスごとのユニキャスト Reverse Path Forwarding（RPF; リバース パス転送）チェックをイネーブルまたはディセーブルにします。Cisco Nexus 5548 スイッチは、各入力側インターフェイスに設定される、次の 2 つの RPF モードをサポートします。

- RPF Strict チェック：ルータ転送テーブルで検証可能な送信元アドレスを持たないパケット、または送信元へのリターン パスに到着しないパケットはドロップされます。
- RPF Loose チェック：パケットはルータ転送テーブルで検証可能な送信元アドレスを持ち、送信元は物理インターフェイスを通じて到達可能です。パケットを受信する入力側インターフェイスは、FIB 内のインターフェイスに一致する必要はありません。

ハードウェア転送

Cisco NX-OS は、分散パケット転送をサポートします。入力ポートは、パケット ヘッダーから該当する情報を取得し、その情報をローカル スイッチング エンジンに渡します。ローカル スイッチング エンジンはレイヤ 3 ルックアップを行い、この情報を使って、パケット ヘッダーをリライトします。入力モジュールは、パケットを出力ポートに転送します。出力ポートが別のモジュール上にある場合は、スイッチ ファブリックを使って、パケットが出力モジュールに転送されます。出力モジュールは、レイヤ 3 転送決定には関与しません。

また、**show platform fib** または **show platform forwarding** コマンドを使用すると、ハードウェア転送の詳細が表示されます。

ソフトウェア転送

Cisco NX-OS のソフトウェア転送パスは、主に、ハードウェアでサポートされない機能、またはハードウェア処理中に発生したエラーへの対処に使用されます。通常、IP オプション付きのパケットまたはフラグメンテーションの必要なパケットは CPU に渡されます。ユニキャスト RIB および隣接マネージャは、ソフトウェアでスイッチされるかまたは終了されるパケットに基づいて転送を決定します。

ソフトウェア転送は、コントロール プレーン ポリシーおよびレート リミッタによって管理されます。

レイヤ 3 ユニキャスト ルーティング機能のまとめ

ここでは、Cisco NX-OS でサポートされるレイヤ 3 ユニキャスト機能およびプロトコルを簡単に説明します。

ここでは、次の内容について説明します。

IPv4

Layer 3 は、IPv4 プロトコルを使用します。詳細については、第 2 章「IPv4 の設定」を参照してください。

IP サービス

IP サービスには、DHCP クライアントおよび Domain Name System（DNS; ドメイン ネーム システム）クライアントがあります。詳細については、Chapter 3, “Configuring DNS.” を参照してください。

OSPF

OSPF プロトコルは、AS 内のネットワーク到達可能性情報の交換に使用されるリンクステート ルーティング プロトコルです。各 OSPF ルータは、そのアクティブなリンクに関する情報をネイバー ルータにアドバタイズします。リンク情報には、リンク タイプ、リンク メトリック、およびリンクに接続されたネイバー ルータが含まれます。このリンク情報を含むアドバタイズメントは、リンクステート アドバタイズメントと呼ばれます。詳細については、第 3 章「OSPFv2 の設定」を参照してください。

EIGRP

EIGRP プロトコルは、ディスタンス ベクトルとリンクステートの両ルーティング プロトコルの特徴を備えたユニキャスト ルーティング プロトコルです。これは、シスコ専用ルーティング プロトコルである IGRP の改良バージョンです。EIGRP は、典型的なディスタンス ベクトル ルーティング プロトコルのように、ルートを提供するためにネイバー ルータを必要とします。また、リンクステート プロトコルのように、ネイバー ルータからアドバタイズされたルートからネットワーク トポロジを構築し、この情報を使用して、ループの発生しない、宛先までのパスを選択します。詳細については、第 4 章「EIGRP の設定」を参照してください。

BGP

BGP は AS 間ルーティング プロトコルです。BGP ルータは、信頼性の高い転送メカニズムとして Transmission Control Protocol（TCP）を使用し、他の BGP ルータにネットワーク到達可能性情報をアドバタイズします。ネットワーク到達可能性情報には、宛先ネットワーク プレフィクス、宛先に到達するまでに通過する必要のある AS のリスト、およびネクストホップ ルータが含まれます。到達可能性情報には、ルートの優先度、ルートの始点、コミュニティなどの詳細なパス属性が含まれます。詳細については、第 5 章「ベーシック BGP の設定」および第 6 章「拡張 BGP の設定」を参照してください。

RIP

RIP は、ホップ数をメトリックとして使用するディスタンス ベクトル プロトコルです。RIP は、世界中のインターネットでトラフィックのルーティングに広く使用されています。また、IGP であるため、単一の AS 内でルーティングを行います。詳細については、第 7 章「RIP の設定」を参照してください。

スタティック ルーティング

スタティック ルーティングを使用して、宛先までの一定のルートを入力できます。この機能は、単純なトポロジの小規模ネットワークでは便利です。また、スタティック ルーティングは、他のルーティング プロトコルとともに、デフォルト ルートおよびルート配布の管理に使用されます。詳細については、第 8 章「スタティック ルーティングの設定」を参照してください。

レイヤ 3 仮想化

仮想化を使用すると、複数の管理ドメインにわたる物理リソースを共有できます。

Cisco NX-OS は、VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）を含むレイヤ 3 仮想化をサポートしています。VRF では、レイヤ 3 ルーティング プロトコルを設定するための別のアドレス ドメインが提供されます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

Route Policy Manager

Route Policy Manager は、Cisco NX-OS でルート フィルタリング機能を提供します。Route Policy Manager はルートマップを使用して、さまざまなルーティング プロトコルや、特定のルーティング プロトコル内のさまざまなエンティティ間で配布されたルートをフィルタリングします。フィルタリングは、特定の一致基準に基づいて行われます。これは、アクセス コントロール リストによるパケット フィルタリングに似ています。詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

ファーストホップ冗長プロトコル

First-hop Redundancy Protocol（FHRP; ファーストホップ冗長プロトコル）は、ホストへの冗長接続を可能にします。アクティブなファーストホップ ルータがダウンした場合は、それの機能を引き継ぐスタンバイ ルータが、FHRP により自動的に選択されます。アドレスは仮想のものであり、FHRP グループ内の各ルータ間で共有されているため、ホストを新しい IP アドレスで更新する必要はありませ

ん。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）の詳細については、第 12 章「HSRP の設定」を参照してください。Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）の詳細については、第 13 章「VRRP の設定」を参照してください。

オブジェクト トラッキング

オブジェクト トラッキングを使用すると、インターフェイス回線プロトコル状態、IP ルーティング、ルート到達可能性などの、ネットワーク上の特定のオブジェクトを追跡し、追跡したオブジェクトの状態が変化したときに対処することができます。この機能により、ネットワークのアベイラビリティが向上し、オブジェクトがダウン状態となった場合の回復時間が短縮されます。詳細については、第 14 章「オブジェクト トラッキングの設定」を参照してください。

関連資料

次のシスコ マニュアルは、レイヤ 3 機能に関連するものです。

- 『*Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide, Release 5.0(3)N1(1)*』
- AS 番号の詳細については、次のページを参照してください。
  http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

PART 1

IP

CHAPTER 2

IPv4 の設定

この章では、Cisco NX-OS スイッチ上でのインターネット プロトコル バージョン 4（IPv4）（アドレス指定を含む）、アドレス解決プロトコル（ARP）、およびインターネット制御メッセージ プロトコル（ICMP）の設定方法を説明します。

この章では、次の内容について説明します。

IPv4 について

スイッチで IP を設定して、IP アドレスをネットワーク インターフェイスに割り当てられます。IP アドレスを割り当てると、インターフェイスがイネーブルになり、そのインターフェイス上のホストと通信できるようになります。

IP アドレスは、スイッチ上でプライマリまたはセカンダリとして設定できます。インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ アドレスを設定できます。スイッチが生成したパケットは、常にプライマリ IPv4 アドレスを使用するため、インターフェイス上のすべてのネットワーキング スイッチは、同じプライマリ IP アドレスを共有する必要があります。各 IPv4 パケットは、送信元または宛先の IP アドレスからの情報に基づいています。「複数の IPv4 アドレス」（P.2-2）を参照してください。

サブネットを使用して、IP アドレスをマスクできます。マスクは、IP アドレスがどのサブネットに属するかを決定するために使用されます。IP アドレスは、ネットワーク アドレスとホスト アドレスで構成されています。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネット マスクと呼ばれます。サブネット マスクは 32 ビット値で、これにより IP パケットの受信者は、IP アドレスのネットワーク ID 部分とホスト ID 部分を区別できます。

Cisco NX-OS システムの IP 機能は、IPv4 パケットの処理と IPv4 パケットの転送を行う役割があります。これには、IPv4 ユニキャスト/マルチキャスト ルート検索、Reverse Path Forwarding（RPF; リバース パス転送）チェック、およびソフトウェア Access Control List（ACL; アクセス コントロール リスト）転送が含まれます。IP 機能は、ネットワーク インターフェイスの IP アドレス設定、重複アドレス チェック、スタティック ルート、IP クライアントのパケット送信/受信インターフェイスも管理します。

ここでは、次の内容について説明します。

複数の IPv4 アドレス

Cisco NX-OS システムは、インターフェイスごとに複数の IP アドレスをサポートしています。さまざまな状況に備え、いくつでもセカンダリ アドレスを指定できます。最も一般的な状況は次のとおりです。

- 特定のネットワーク インターフェイスのホスト IP アドレスの数が不足している場合。たとえば、サブネット化により、論理サブネットごとに 254 までのホストを使用できるが、物理サブネットの 1 つに 300 のホスト アドレスが必要な場合は、ルータ上またはアクセス サーバ上でセカンダリ IP アドレスを使用して、1 つの物理サブネットで 2 つの論理サブネットを使用できます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。別のネットワークによって物理的に分離された複数のサブネットから、セカンダリ アドレスを使用して、1 つのネットワークを作成できます。このような場合、最初のネットワークは、2 番めのネットワークの上に拡張されます。つまり、上の階層となります。サブネットは、ルータの複数のアクティブなインターフェイス上に同時に表示できません。

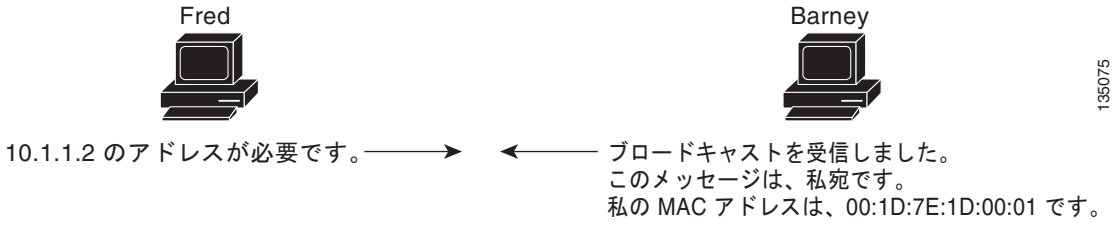
（注）　ネットワーク セグメント上のいずれかのスイッチがセカンダリ IPv4 アドレスを使用している場合は、同じネットワーク インターフェイス上の他のすべてのスイッチも、同じネットワークまたはサブネットからのセカンダリ アドレスを使用する必要があります。ネットワーク セグメント上で、一貫性のない方法でセカンダリ アドレスを使用すると、ただちにルーティング ループが発生する可能性があります。

アドレス解決プロトコル

ネットワーク スイッチおよびレイヤ 3 スイッチは、アドレス解決プロトコル（ARP）を使用して、IP（ネットワーク層）アドレスを Media Access Control（MAC; メディア アクセス コントロール）レイヤ アドレスにマップし、IP パケットのネットワーク間の送信を可能にします。スイッチは、別のスイッチにパケットを送信する前に、独自の ARP キャッシュを調べて、宛先スイッチの MAC アドレスおよび対応する IP アドレスがあるかどうかを確認します。エントリがない場合、発信元のスイッチは、ネットワーク上のすべてのスイッチにブロードキャスト メッセージを送信します。

各スイッチは、IP アドレスをそれぞれ自身の IP アドレスと比較します。一致する IP アドレスを持つスイッチだけが、スイッチの MAC アドレスを含むパケットとともにデータを送信したスイッチに返信します。送信元スイッチは、以降の参照用に宛先スイッチの MAC アドレスを自身の ARP テーブルに追加し、データリンク ヘッダーの作成とパケットをカプセル化するトレーラの作成を行った後、データ転送を開始します。図 2-1 は、ARP ブロードキャストと応答処理を示します。

図 2-1　ARP 処理



宛先スイッチが別のスイッチの背後のリモートネットワークにある場合、データを送信するスイッチがデフォルト ゲートウェイの MAC アドレスに対する ARP 要求を送信する場合を除いてプロセスは同じです。アドレスが解決され、デフォルト ゲートウェイがパケットを受信したあとに、デフォルト ゲートウェイは、接続されているネットワーク上で宛先の IP アドレスをブロードキャストします。宛先スイッチのネットワーク上のスイッチは、ARP を使用して宛先スイッチの MAC アドレスを取得し、パケットを配信します。ARP はデフォルトでイネーブルにされています。

デフォルトのシステム定義 CoPP ポリシーは、ARP ブロード キャスト パケットのレート制限を行います。デフォルトのシステム定義 CoPP ポリシーは、ARP ブロードキャスト ストームによるコントロール プレーン トラフィックへの影響を防止し、ブリッジド パケットに影響しません。

ARP キャッシング

ARP キャッシングにより、ブロードキャストが最小になり、無駄に使用されるネットワーク リソースが制限されます。IP アドレスの MAC アドレスへのマッピングは、インターネットワークを送信される各パケットに対しネットワーク上のホップ（スイッチ）ごとに発生します。そのため、ネットワーク パフォーマンスに影響を与えます。

ARP キャッシングでは、ネットワーク アドレスとそれに関連付けられたデータリンク アドレスが一定の期間、メモリに格納されるため、パケットが送信されるたびに同じアドレスを求めてブロードキャストする場合の、貴重なネットワーク リソースの使用が最小限となります。キャッシュ エントリは、定期的に失効するよう設定されているため、保守が必要です。これは、古い情報が無効となる場合があるためです。ネットワーク上のすべてのスイッチは、アドレスがブロードキャストされるとそれぞれのテーブルを更新します。

ARP キャッシュのスタティック エントリおよびダイナミック エントリ

スタティック ルートの使用時には、各スイッチの各インターフェイスの IP アドレス、サブネット マスク、ゲートウェイ、および対応する MAC アドレスを手動で設定する必要があります。スタティック ルーティングを使用すると、管理を強化できますが、より多くのルート テーブル保守作業が必要となります。ルートを追加または変更するたびに、テーブルの更新が必要となるためです。

ダイナミック ルーティングは、ネットワーク内のスイッチが相互にルーティング テーブルの情報を交換できるプロトコルを使用します。ダイナミック ルーティングは、キャッシュに制限時間を追加しない限り、ルート テーブルが自動更新されるため、スタティック ルーティングより効率的です。デフォルトの制限時間は 25 分ですが、キャッシュから追加および削除されるルートがネットワークに数多く存在する場合は、制限時間を変更します。

ARP を使用しないデバイス

ネットワークが 2 つのセグメントに分割されると、ブリッジによりセグメントが結合され、各セグメントへのトラフィックが MAC アドレスに基づいてフィルタリングされます。スイッチとは対照的に MAC アドレスだけを使用するブリッジは、独自のアドレス テーブルを作成します。このテーブルには IP アドレスおよび対応する MAC アドレスを含む ARP キャッシュがあります。

パッシブ ハブは、ネットワーク内の他のスイッチを物理的に接続する中央接続スイッチです。これは、そのすべてのポートからスイッチに対してメッセージを送信し、レイヤ 1 で動作しますが、アドレス テーブルは維持しません。

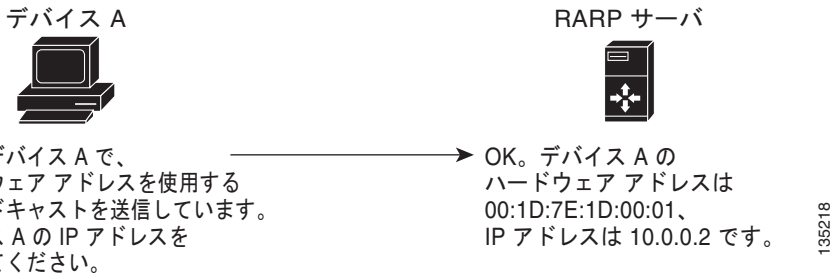
レイヤ 2 スイッチは、すべてのポートからメッセージを送信するハブとは異なり、メッセージの宛先であるデバイスに接続されるポートを決定し、そのポートにだけ送信します。ただし、レイヤ 3 スイッチは、ARP キャッシュ（テーブル）を作成するスイッチです。

Reverse ARP

RFC 903 で定義された Reverse ARP（RARP）は ARP と同様に機能しますが、RARP 要求パケットが MAC アドレスではなく、IP アドレスを要求する点が異なります。RARP は多くの場合、ディスクレス ワークステーションで使用されます。これは、このタイプのデバイスには、起動時に使用する IP アドレスを格納する手段がないためです。認識できるアドレスは MAC アドレスだけで、これはハードウェアに焼き付けられているためです。

RARP を使用するには、ルータ インターフェイスとして、同じネットワーク セグメント上に RARP サーバが必要です。図 2-2 は、RARP の機能を図示したものです。

図 2-2　Reverse ARP



RARP には、いくつかの制限があります。これらの制限により、ほとんどの企業では、DHCP を使用してダイナミックに IP アドレスを割り当てています。DHCP は、RARP よりコスト効率が高く、必要な保守作業も少ないためです。最も重要な制限は次のとおりです。

- RARP はハードウェア アドレスを使用するため、多くの物理ネットワークを含む大規模なネットワークの場合は、各セグメント上に、冗長性のための追加サーバを備えた RARP サーバが必要です。各セグメントに 2 台のサーバを保持すると、コストがかかります。
- 各サーバは、ハードウェア アドレスと IP アドレスのスタティック マッピングのテーブルで設定する必要があります。IP アドレスの保守は困難です。
- RARP は、ホストの IP アドレスだけを提供し、サブネット マスクもデフォルト ゲートウェイも提供しません。

プロキシ ARP

プロキシ ARP によって、あるネットワーク上に物理的に存在するスイッチが、同じスイッチまたはファイアウォールに接続された別の物理ネットワークの論理的な一部であることが可能になります。プロキシ ARP によって、ルータの背後のプライベート ネットワーク上のスイッチをパブリック IP アドレスを使用して隠すことができ、さらに、ルータの手前のパブリック ネットワークにあるように見せることができます。ルータはそのアイデンティティを隠すことにより、実際の宛先までパケットをルーティングする役割を担います。プロキシ ARP を使用すると、サブネット上のスイッチは、ルーティングもデフォルト ゲートウェイも設定せずにリモート サブネットまで到達できます。

スイッチが同じデータリンク層ネットワークには存在しないが、同じ IP ネットワークに存在する場合、それらのスイッチはローカル ネットワーク上に存在するものとして、相互にデータ送信を試みます。ただし、これらのスイッチを隔てるルータは、ブロードキャスト メッセージを送信しません。これは、ルータがハードウェア レイヤのブロードキャストを渡さず、アドレスが解決されないためです。

スイッチでプロキシ ARP をイネーブルにし、ARP 要求を受信すると、プロキシ ARP はこれを、ローカル LAN 上にないシステムに対する要求と見なします。スイッチは、ブロードキャストがアドレス指定されたリモートの宛先であるかのように、そのスイッチの MAC アドレスをリモートの宛先の IP アドレスと関連付ける ARP 応答で応答します。ローカル スイッチは、宛先に直接接続されていると確信しますが、実際には、パケットはローカル スイッチによってローカル サブネットワークから宛先サブネットワークへ転送されます。デフォルトでは、プロキシ ARP はディセーブルになっています。

ローカル プロキシ ARP

ローカル Proxy ARP を使用すると、通常ルーティングが必要ないサブネット内の IP アドレスを求める ARP 要求に対し、スイッチが応答するようにできます。ローカル プロキシ ARP をイネーブルにすると、ARP は、サブネット内の IP アドレスを求めるすべての ARP 要求に応答し、サブネット内のホスト間ですべてのトラフィックを転送します。この機能は、接続先スイッチ上での設定により、意図的にホスト間の直接的なコミュニケーションが禁止されているサブネットについてだけ使用してください。

Gratuitous ARP

Gratuitous ARP は、送信元 IP アドレスと宛先 IP アドレスが同じである要求を送信し、重複する IP アドレスを検出します。Cisco NX-OS Release 5.0(3) は、Gratuitous ARP 要求または ARP キャッシュ アップデートのイネーブルまたはディセーブルをサポートします。

ICMP

ICMP を使用して、IP 処理に関連するエラーおよびその他の情報を報告するメッセージ パケットを提供できます。ICMP は、ICMP 宛先到達不能メッセージ、ICMP エコー要求（2 つのホスト間でパケットを往復送信する）、およびエコー返信メッセージなどのエラー メッセージを生成します。ICMP は多くの診断機能も備えており、ホストへのエラー パケットの送信およびリダイレクトが可能です。デフォルトでは、ICMP がイネーブルにされています。

次に示すのは、ICMP メッセージ タイプの一部です。

- ネットワーク エラー メッセージ
- ネットワーク混雑メッセージ
- トラブルシューティング情報
- タイムアウト告知

（注）　ICMP リダイレクトは、ローカル プロキシ ARP 機能がイネーブルであるインターフェイス上ではディセーブルにされています。

仮想化のサポート

IPv4 は、Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング/転送インスタンス）をサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

IPv4 のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IPv4 にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IPv4 の前提条件

IPv4 には、次の前提条件があります。

- IPv4 はレイヤ 3 インターフェイス上だけで設定可能です。

注意事項および制約事項

IPv4 設定時の注意事項および制約事項は、次のとおりです。

- セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にだけ設定できます。

デフォルト設定

表 2-1 に、IP パラメータのデフォルト設定を示します。

表 2-1　デフォルト IP パラメータ

パラメータ	デフォルト
ARP タイムアウト	1500 秒
プロキシ ARP	ディセーブル

IPv4 の設定

ここでは、次の内容について説明します。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

IPv4 アドレス指定の設定

ネットワーク インターフェイスにプライマリ IP アドレスを割り当てることができます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*
3. **no switchport**
4. **ip address** *ip-address/length* [**secondary**]
5. （任意）**show ip interface**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *number* **Example:** switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip address** *ip-address/length* [**secondary**] **Example:** switch(config-if)# ip address 192.2.1.1 255.0.0.0	インターフェイスにプライマリまたはセカンダリ IPv4 アドレスを指定します。 • ネットワーク マスクは、ドットで 4 つの部分に分けられている 10 進数のアドレスです。たとえば、255.0.0.0 は、1 に等しい各ビットが、ネットワーク アドレスに属した対応するアドレス ビットを意味することを示します。 • ネットワーク マスクは、スラッシュ（/）および数字、つまり、プレフィクス長として示される場合もあります。プレフィクス長は、プレフィクスを構成するアドレスの上位の連続ビット（アドレスのネットワーク部分）の桁数を示す 10 進数の値です。スラッシュは 10 進数値の前に置かれ、IP アドレスとスラッシュの間にスペースは入りません。
ステップ 5	**show ip interface** **Example:** switch(config-if)# show ip interface	（任意）IPv4 に設定されたインターフェイスを表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip address 192.2.1.1 255.0.0.0
switch(config-if)# copy running-config startup-config
```

複数の IP アドレスの設定

セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にだけ追加できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*
3. **no switchport**
4. **ip address** *ip-address/length* [**secondary**]
5. （任意）**show ip interface**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *number*
	
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip address** *ip-address/length* [**secondary**] **Example:** `switch(config-if)# ip address 192.2.1.1 255.0.0.0 secondary`	設定したアドレスをセカンダリ IPv4 アドレスとして指定します。
ステップ 5	**show ip interface** **Example:** `switch(config-if)# show ip interface`	（任意）IPv4 に設定されたインターフェイスを表示します。
ステップ 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

スタティック ARP エントリの設定

スイッチ上に、IP アドレスを MAC ハードウェア アドレス（スタティック マルチキャスト MAC アドレスを含む）にマップするスタティック ARP エントリを設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*
3. **no switchport**
4. **ip arp** *ipaddr mac_addr*
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *number* **Example:** switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip arp** *ipaddr mac_addr* **Example:** switch(config-if)# ip arp 192.2.1.1 0019.076c.1a78	IP アドレスを MAC アドレスにスタティック エントリとして関連付けます。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、スタティック ARP エントリを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip arp 192.2.1.1 0019.076c.1a78
switch(config-if)# copy running-config startup-config
```

プロキシ ARP の設定

スイッチで、別のネットワークまたはサブネット上のホストのメディア アドレス定義する Proxy ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*
3. **no switchport**
4. **ip proxy-arp**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *number* **Example:** switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip proxy-arp** **Example:** switch(config-if)# ip proxy-arp	インターフェイス上でプロキシ ARP をイネーブルにします。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip proxy-arp
switch(config-if)# copy running-config startup-config
```

ローカル プロキシ ARP の設定

スイッチ上でローカル プロキシ ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*

3. **no switchport**
4. **ip local-proxy-arp**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *number* **Example:** switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip local-proxy-arp** **Example:** switch(config-if)# ip local-proxy-arp	インターフェイス上でローカル プロキシ ARP をイネーブルにします。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ローカル プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip local-proxy-arp
switch(config-if)# copy running-config startup-config
```

Gratuitous ARP の設定

インターフェイス上で Gratuitous ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *number*
3. **no switchport**
4. **ip arp gratuitous** {**request** | **update**}
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *number* **Example:** switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip arp gratuitous** {**request** | **update**} **Example:** switch(config-if)# ip arp gratuitous request	インターフェイス上で Gratuitous ARP をイネーブルにします。イネーブルがデフォルトです。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、Gratuitous ARP 要求をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# no ip arp gratuitous request
switch(config-if)# copy running-config startup-config
```

ダイレクト ブロードキャストの設定

IP ダイレクト ブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

宛先サブネットに直接接続されていないスイッチは、ユニキャスト IP パケットをそのサブネット上のホストに転送するのと同じ方法で、IP ダイレクト ブロードキャストを転送します。ダイレクト ブロードキャスト パケットが、宛先サブネットに直接接続されたスイッチに到着すると、宛先サブネット上のブロードキャストとして「展開」されます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。

あるインターフェイスでダイレクト ブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクト ブロードキャストとして識別されると、そのパケットはそのサブネット上にブロードキャストとして展開されます。

IP ダイレクト ブロードキャストをイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip directed-broadcast	ダイレクト ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。

IPv4 設定の確認

IPv4 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hardware forwarding ip verify	IP パケット検証の設定を表示します。
show ip adjacency	隣接関係テーブルを表示します。
show ip arp	ARP テーブルを表示します。
show ip interface	IP 関連のインターフェイス情報を表示します。
show ip arp statistics [**vrf** *vrf-name*]	ARP 統計情報を表示します。

IPv4 の設定例

次に、IPv4 アドレスを設定する例を示します。

```
configure terminal
 interface ethernet 1/2
  no switchport
  ip address 192.2.1.1/16
```

その他の関連資料

IP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.2-15）
- 「標準」（P.2-15）

関連資料

関連項目	マニュアル名
IP CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

IP 機能の履歴

表 2-1 は、この機能のリリースの履歴です。

表 2-2　IP 機能の履歴

機能名	リリース	機能情報
IP	5.0(3)N1(1)	この機能が導入されました。

PART 2

ルーティング

CHAPTER 3

OSPFv2 の設定

この章では、IPv4 ネットワーク向けの OSPFv2（Open Shortest Path First version 2）の設定方法を説明します。

この章では、次の内容について説明します。

OSPFv2 について

OSPFv2 は、IPv4 ネットワーク用 IETF リンクステート プロトコルです（「リンクステート プロトコル」（P.1-9）を参照）。OSPFv2 ルータは、*hello パケット*と呼ばれる特別なメッセージを各 OSPF 対応インターフェイスに送信して、他の OSPFv2 ネイバー ルータを探索します。ネイバー ルータが発見されると、この 2 台のルータは hello パケットの情報を比較して、両者の設定に互換性があるかどうかを判定します。これらのネイバー ルータは*隣接関係*を確立しようとします。つまり、両者のリンクステート データベースを同期させて、確実に同じ OSPFv2 ルーティング情報を持つようにします。隣接ルータは、各リンクの稼動状態に関する情報、リンクのコスト、およびその他のあらゆるネイバー情報を含む*リンクステート アドバタイズメント*（LSA）を共有します。これらのルータはその後、受信した LSA をすべての OSPF 対応インターフェイスにフラッディングします。これにより、すべての OSPFv2 ルータのリンクステート データベースが最終的に同じになります。すべての OSPFv2 ルータのリンクステート データベースが同じになると、ネットワークは *収束* されます（「コンバージェンス」（P.1-6）を参照）。その後、各ルータは、ダイクストラの最短パス優先（SPF）アルゴリズムを使用して、自身のルート テーブルを構築します。

OSPFv2 ネットワークは、複数のエリアに分割できます。ルータは、ほとんどの LSA を 1 つのエリア内だけに送信するため、OSPF 対応ルータの CPU とメモリの要件が緩やかになります。

OSPFv2 は IPv4 をサポートしています。

ここでは、次の内容について説明します。

hello パケット

OSPFv2 ルータは、すべての OSPF 対応インターフェイスに hello パケットを定期的に送信します。ルータがこの hello パケットを送信する頻度は、インターフェイスごとに設定された *hello 間隔*により決定されます。OSPFv2 は、hello パケットを使用して、次のタスクを実行します。

- ネイバー探索
- キープアライブ
- 指定ルータの選定（「指定ルータ」（P.3-3）を参照）

hello パケットには、リンクの OSPFv2 コスト割り当て、hello 間隔、送信元ルータのオプション機能など、送信元の OSPFv2 インターフェイスとルータに関する情報が含まれます。これらの hello パケットを受信する OSPFv2 インターフェイスは、設定に受信インターフェイスの設定との互換性があるかどうかを判定します。互換性のあるインターフェイスはネイバーと見なされ、ネイバー テーブルに追加されます（「ネイバー」（P.3-2）を参照）。

hello パケットには、送信元インターフェイスが通信したルータのルータ ID のリストも含まれます。受信インターフェイスが、このリストで自身の ID を見つけた場合は、2 つのインターフェイス間で双方向通信が確立されます。

OSPFv2 は、hello パケットをキープアライブ メッセージとして使用して、ネイバーが通信を継続中であるかどうかを判定します。ルータが設定された *デッド間隔*（通常は hello 間隔の倍数）で hello パケットを受信しない場合、そのネイバーはローカル ネイバー テーブルから削除されます。

ネイバー

ネイバーと見なされるためには、OSPFv2 インターフェイスがリモート インターフェイスとの互換性を持つように設定されている必要があります。この 2 つの OSPFv2 インターフェイスで、次の基準が一致している必要があります。

- hello 間隔
- デッド間隔
- エリア ID（「エリア」（P.3-4）を参照）

- 認証
- オプション機能

一致する場合は、次の情報がネイバー テーブルに入力されます。

- ネイバー ID：ネイバーのルータ ID。
- プライオリティ：ネイバーのプライオリティ。プライオリティは、指定ルータの選定（「指定ルータ」（P.3-3）を参照）に使用されます。
- 状態：ネイバーから通信があったか、双方向通信の確立処理中であるか、リンクステート情報を共有しているか、または完全な隣接関係が確立されたかを示します。
- デッド タイム：このネイバーから最後の hello パケットを受信したあとに経過した時間を示します。
- IP アドレス：ネイバーの IP アドレス。
- 指定ルータ：ネイバーが指定ルータ、またはバックアップ指定ルータとして宣言されたかどうかを示します（「指定ルータ」（P.3-3）を参照）。
- ローカル インターフェイス：このネイバーの hello パケットを受信したローカル インターフェイス。

隣接関係

すべてのネイバーが隣接関係を確立するわけではありません。ネットワーク タイプと確立された指定ルータに応じて、完全な隣接関係を確立して、すべてのネイバーと LSA を共有するものと、そうでないものがあります。詳細については、「指定ルータ」（P.3-3）を参照してください。

隣接関係は、OSPF のデータベース説明パケット、リンク状態要求パケット、およびリンク状態更新パケットを使用して確立されます。データベース説明パケットに含まれるのは、ネイバーのリンクステート データベースからの LSA ヘッダーだけです（「リンクステート データベース」（P.3-7）を参照）。ローカル ルータは、これらのヘッダーを自身のリンクステート データベースと比較して、新規の LSA か、更新された LSA かを判定します。ローカル ルータは、新規または更新の情報を必要とする各 LSA について、リンク状態要求パケットを送信します。これに対し、ネイバーはリンク状態更新パケットを返信します。このパケット交換は、両方のルータのリンクステート情報が同じになるまで継続します。

指定ルータ

複数のルータを含むネットワークは、OSPF 特有の状況です。すべてのルータがネットワークで LSA をフラッディングした場合は、同じリンクステート情報が複数の送信元から送信されます。ネットワークのタイプに応じて、OSPFv2 は*指定ルータ*（*DR*）という 1 台のルータを使用して、LSA のフラッディングを制御し、OSPFv2 の残りの部分に対してネットワークを代表する場合があります（「エリア」（P.3-4）を参照）。DR がダウンした場合、OSPFv2 は*バックアップ指定ルータ*（BDR）を選定します。DR がダウンすると、OSPFv2 はこの BDR を使用します。

ネットワーク タイプは次のとおりです。

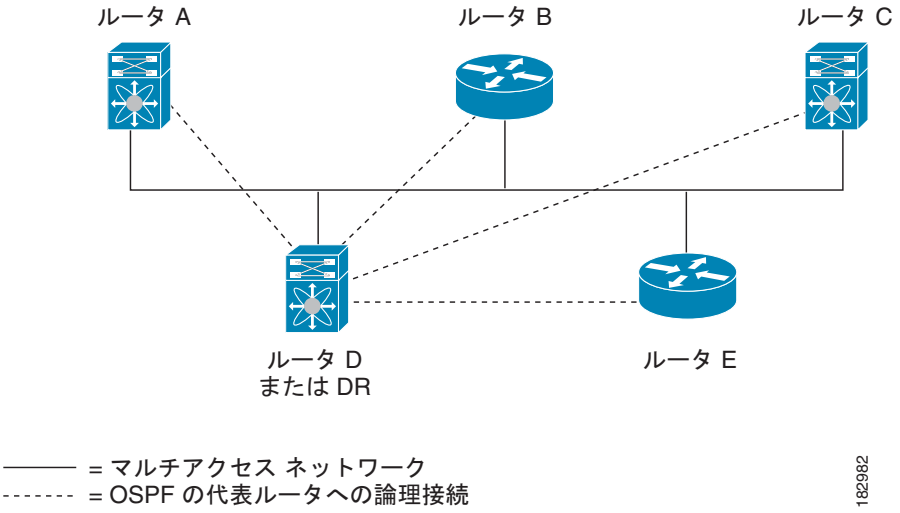
- ポイントツーポイント：2 台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。
- ブロードキャスト：ブロードキャスト トラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv2 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッディングを制御します。OSPFv2 は、よく知られている IPv4 マルチキャスト アドレス 224.0.0.5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

DR と BDR は、hello パケット内の情報に基づいて選択されます。インターフェイスは hello パケットの送信時に、どれが DR および BDR かわかっている場合は、優先フィールドと、DR および BDR フィールドを設定します。ルータは、hello パケットの DR および BDR フィールドで宣言されたルータと優先フィールドに基づいて、選定手順を実行します。最終的に OSPFv2 は、最も大きいルータ ID を DR および BDR として選択します。

他のルータはすべて DR および BDR と隣接関係を確立し、IPv4 マルチキャスト アドレス 224.0.0.6 を使用して、LSA 更新情報を DR と BDR に送信します。図 3-1 は、すべてのルータと DR の間のこの隣接関係を示します。

DR は、ルータ インターフェイスに基づいています。1 つのネットワークの DR であるルータは、別のインターフェイス上の他のネットワークの DR となることはできません。

図 3-1　マルチアクセス ネットワークの DR



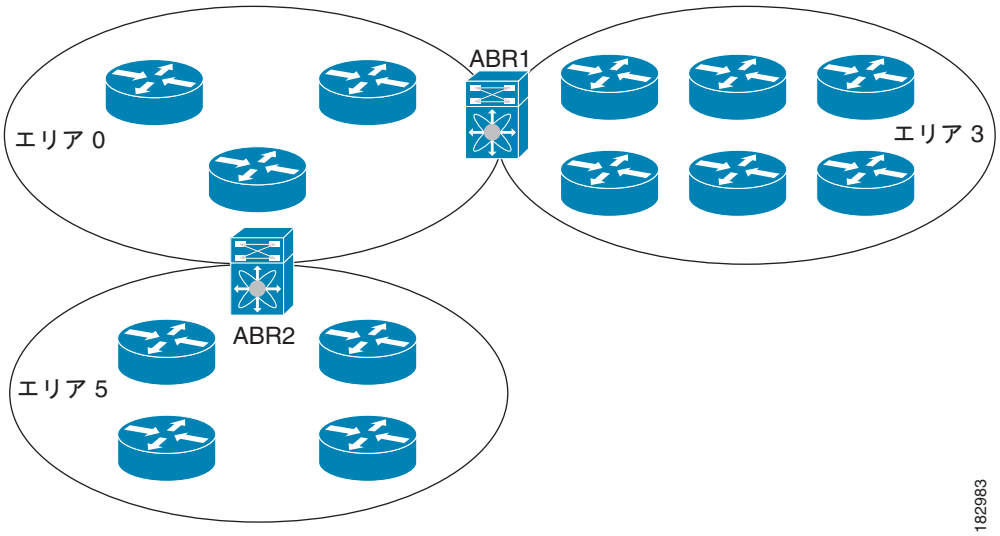
エリア

OSPFv2 ネットワークを複数の*エリア*に分割すると、ルータに要求される OSPFv2 の CPU とメモリに関する要件を制限できます。 エリアとは、ルータの論理的な区分で、OSPFv2 ドメイン内にリンクして別のサブドメインを作成します。LSA フラッディングはエリア内でのみ発生し、リンクステート データベースはエリア内のリンクにのみ制限されます。定義されたエリア内のインターフェイスには、エリア ID を割り当てることができます。エリア ID は、10.2.3.1 などの、数字またはドット付き 10 進表記で入力できる 32 ビット値です。

Cisco NX-OS は常にドット付き 10 進表記でエリアを表示します。

OSPFv2 ネットワーク内に複数のエリアを定義する場合は、0 という予約されたエリア ID を持つバックボーン エリアも定義する必要があります。エリアが複数ある場合は、1 台以上のルータが*エリア境界ルータ*（ABR）となります。ABR は、バックボーン エリアと他の 1 つ以上の定義済みエリアの両方に接続します（図 3-2 を参照）。

図 3-2　OSPFv2 エリア



ABR には、接続するエリアごとに個別のリンクステート データベースがあります。ABR は、接続したエリアの 1 つからバックボーン エリアにネットワーク集約（タイプ 3）LSA（「ルート集約」（P.3-10）を参照）を送信します。バックボーン エリアは、1 つのエリアに関する集約情報を別のエリアに送信します。図 3-2 では、エリア 0 が、エリア 5 に関する集約情報をエリア 3 に送信しています。

OSPFv2 では、自律システム境界ルータ（ASBR）という、もう 1 つのルータ タイプも定義されています。このルータは、OSPFv2 エリアを別の自律システムに接続します。自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。OSPFv2 は、そのルーティング情報を別の自律システムに再配布したり、再配布されたルートを別の自律システムから受信したりできます。詳細については、「高度な機能」（P.3-8）を参照してください。

リンクステート アドバタイズメント

OSPFv2 は Link State Advertisement（LSA; リンクステート アドバタイズメント）を使用して、自身のルーティング テーブルを構築します。

ここでは、次の内容について説明します。

LSA タイプ

表 3-1 は、Cisco NX-OS でサポートされる LSA タイプを示します。

表 3-1　LSA タイプ

タイプ	名前	説明
1	ルータ LSA	すべてのルータが送信する LSA。この LSA には、すべてのリンクの状態とコスト、およびリンク上のすべての OSPFv2 ネイバーの一覧が含まれます。ルータ LSA は SPF 再計算をトリガーします。ルータ LSA はローカル OSPFv2 エリアにフラッディングされます。
2	ネットワーク LSA	DR が送信する LSA。この LSA には、マルチアクセス ネットワーク内のすべてのルータの一覧が含まれます。ネットワーク LSA は SPF 再計算をトリガーします。「指定ルータ」（P.3-3）を参照してください。
3	ネットワーク集約 LSA	ABR が、ローカル エリア内の宛先ごとに外部エリアに送信する LSA。この LSA には、ABR からローカルの宛先へのリンク コストが含まれます。「エリア」（P.3-4）を参照してください。
4	ASBR 集約 LSA	ABR が外部エリアに送信する LSA。この LSA は、リンク コストを ASBR のみにアドバタイズします。「エリア」（P.3-4）を参照してください。
5	AS 外部 LSA	ASBR が生成する LSA。この LSA には、外部 AS 宛先へのリンク コストが含まれます。AS 外部 LSA は、AS 全体にわたってフラッディングされます。「エリア」（P.3-4）を参照してください。
7	NSSA 外部 LSA	ASBR が Not-So-Stubby Area（NSSA）内で生成する LSA。この LSA には、外部 AS 宛先へのリンク コストが含まれます。NSSA 外部 LSA は、ローカル NSSA 内のみでフラッディングされます。「エリア」（P.3-4）を参照してください。
9–11	不透明 LSA	OSPF の拡張に使用される LSA。「不透明 LSA」（P.3-7）を参照してください。

リンク コスト

各 OSPFv2 インターフェイスには、*リンク コスト*が割り当てられます。このコストは任意の数字です。デフォルトでは、Cisco NX-OS が、設定された参照帯域幅をインターフェイス帯域幅で割った値をコストとして割り当てます。デフォルトでは、参照帯域幅は 40 Gbps です。リンク コストは各リンクに対して、LSA 更新情報で伝えられます。

フラッディングと LSA グループ ペーシング

OSPFv2 ルータは、LSA を受信すると、その LSA をすべての OSPF 対応インターフェイスに転送し、OSPFv2 エリアをこの情報でフラッディングします。この LSA フラッディングにより、ネットワーク内のすべてのルータが同じルーティング情報を持つことが保証されます。LSA フラッディングは、OSPFv2 エリアの設定により異なります（「エリア」（P.3-4）を参照）。LSA は、*リンクステート リフレッシュ*時間に基づいて（デフォルトでは 30 分ごとに）フラッディングされます。各 LSA には、リンクステート リフレッシュ時間が設定されています。

ネットワークの LSA 更新情報のフラッディング レートは、LSA グループ ペーシング機能を使用して制御できます。LSA グループ ペーシングにより、CPU またはバッファの使用率を低下させることができます。この機能により、同様のリンクステート リフレッシュ時間を持つ LSA がグループ化されるため、OSPFv2 で、複数の LSA を 1 つの OSPFv2 更新メッセージにまとめることが可能となります。

デフォルトでは、相互のリンクステート リフレッシュ時間が 4 分以内の LSA が同じグループに入れられます。この値は、大規模なリンクステート データベースでは低く、小規模のデータベースでは高くして、ネットワーク上の OSPFv2 負荷を最適化する必要があります。

リンクステート データベース

各ルータは、OSPFv2 ネットワーク用のリンクステート データベースを維持しています。このデータベースには、収集されたすべての LSA が含まれ、ネットワークを通過するすべてのルートに関する情報が格納されます。OSPFv2 は、この情報を使用して、各宛先への最適なパスを計算し、この最適なパスをルーティング テーブルに入力します。

MaxAge と呼ばれる設定済みの時間間隔で受信された LSA 更新情報がまったくない場合は、リンクステート データベースから LSA が削除されます。ルータは、LSA を 30 分ごとに繰り返してフラッディングし、正確なリンクステート情報が期限切れで削除されるのを防ぎます。Cisco NX-OS は、すべての LSA が同時にリフレッシュされるのを防ぐために、LSA グループ機能をサポートしています。詳細については、「フラッディングと LSA グループ ペーシング」（P.3-6）を参照してください。

不透明 LSA

不透明 LSA により、OSPF 機能の拡張が可能となります。不透明 LSA は、標準 LSA ヘッダーと、それに続くアプリケーション固有の情報で構成されます。この情報は、OSPFv2 または他のアプリケーションにより使用される場合があります。次のような 3 種類の不透明 LSA タイプが定義されています。

- LSA タイプ 9：ローカル ネットワークにフラッディングされます。
- LSA タイプ 10：ローカル エリアにフラッディングされます。
- LSA タイプ 11：ローカル AS にフラッディングされます。

OSPFv2 とユニキャスト RIB

OSPFv2 は、リンクステート データベースでダイクストラの SPF アルゴリズムを実行します。このアルゴリズムにより、パス上の各リンクのリンク コストの合計に基づいて、各宛先への最適なパスが選択されます。そして、選択された各宛先への最短パスが OSPFv2 ルート テーブルに入力されます。OSPFv2 ネットワークが収束すると、このルート テーブルはユニキャスト RIB にデータを提供します。OSPFv2 はユニキャスト RIB と通信し、次の動作を行います。

- ルートの追加または削除
- 他のプロトコルからのルートの再配布への対応
- 変更されていない OSPFv2 ルートの削除およびスタブ ルータ アドバタイズメントを行うためのコンバージェンス更新情報の提供（「OSPFv2 スタブ ルータ アドバタイズメント」（P.3-11）を参照）

さらに OSPFv2 は、変更済みダイクストラ アルゴリズムを実行して、集約および外部（タイプ 3、4、5、7）LSA の変更の高速再計算を行います。

認証

OSPFv2 メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。Cisco NX-OS は、次の 2 つの認証方式をサポートしています。

- 簡易パスワード認証
- MD5 認証ダイジェスト

OSPFv2 認証は、OSPFv2 エリアに対して、またはインターフェイスごとに設定できます。

簡易パスワード認証

簡易パスワード認証では、OSPFv2 メッセージの一部として送信された単純なクリア テキストのパスワードを使用します。受信 OSPFv2 ルータが OSPFv2 メッセージを有効なルート更新情報として受け入れるには、同じクリア テキスト パスワードで設定されている必要があります。パスワードがクリア テキストであるため、ネットワーク上のトラフィックをモニタできるあらゆるユーザがパスワードを入手できます。

MD5 認証

OSPFv2 メッセージを認証するには、MD5 認証を使用する必要があります。そのためには、ローカル ルータとすべてのリモート OSPFv2 ネイバーが共有するパスワードを設定します。Cisco NX-OS は各 OSPFv2 メッセージに対して、メッセージと暗号化されたパスワードに基づく MD5 一方向メッセージ ダイジェストを作成します。インターフェイスはこのダイジェストを OSPFv2 メッセージとともに送信します。受信する OSPFv2 ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合はダイジェストの計算が同一であるため、OSPFv2 メッセージは有効と見なされます。

MD5 認証には、ネットワークでのメッセージの再送を防ぐための、各 OSPFv2 メッセージのシーケンス番号が含まれます。

高度な機能

Cisco NX-OS は、ネットワークでの OSPFv2 の可用性やスケーラビリティを向上させる数多くの高度な OSPFv2 機能をサポートしています。ここでは、次の内容について説明します。

- 「スタブ エリア」（P.3-8）
- 「Not-So-Stubby エリア」（P.3-9）
- 「仮想リンク」（P.3-9）
- 「ルートの再配布」（P.3-10）
- 「ルート集約」（P.3-10）
- 「OSPFv2 スタブ ルータ アドバタイズメント」（P.3-11）
- 「複数の OSPFv2 インスタンス」（P.3-11）
- 「SPF 最適化」（P.3-11）
- 「仮想化のサポート」（P.3-11）

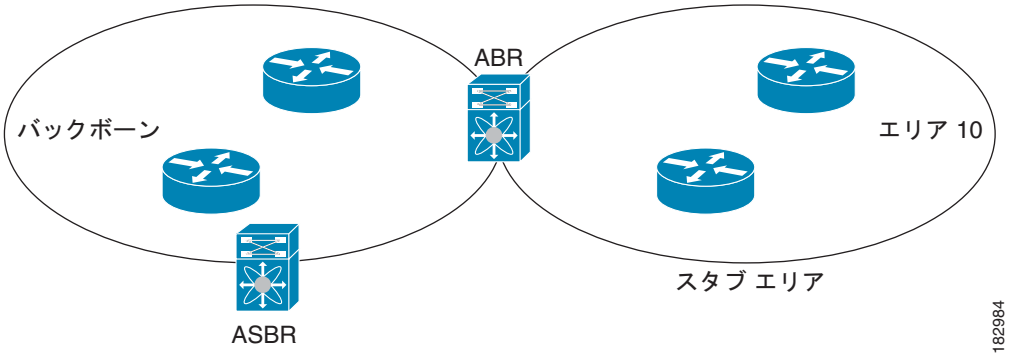
スタブ エリア

エリアを *スタブ エリア*にすると、エリアでフラッディングされる外部ルーティング情報の量を制限できます。スタブ エリアとは、AS 外部（タイプ 5）LSA（「リンクステート アドバタイズメント」（P.3-5）を参照）が許可されないエリアです。これらの LSA は通常、外部ルーティング情報を伝播するためにローカル AS 全体でフラッディングされます。スタブ エリアには、次の要件があります。

- スタブ エリア内のすべてのルータはスタブ ルータです。「スタブ ルーティング」（P.1-7）を参照してください。
- スタブ エリアには ASBR ルータは存在しません。
- スタブ エリアには仮想リンクを設定できません。

図 3-3 は、外部 AS に到達するためにエリア 0.0.0.10 内のすべてのルータが ABR を通過する必要のある OSPFv2 AS の例を示します。エリア 0.0.0.10 は、スタブ エリアとして設定できます。

図 3-3　スタブ エリア



スタブ エリアは、外部 AS へのバックボーン エリアを通過する必要のあるすべてのトラフィックにデフォルト ルートを使用します。IPv4 の場合のデフォルト ルートは 0.0.0.0 です。

Not-So-Stubby エリア

Not-So-Stubby Area（*NSSA*）はスタブ エリアに似ていますが、NSSA では、再配布を使用して NSSA 内で AS 外部ルートをインポートできる点が異なります。NSSA ASBR はこれらのルートを再配布し、NSSA 外部（タイプ 7）LSA を生成して NSSA 全体でフラッディングします。または、NSSA を他のエリアに接続する ABR を設定することにより、この NSSA 外部 LSA を AS 外部（タイプ 5）LSA に変換することもできます。こうすると、ABR は、これらの AS 外部 LSA を OSPFv2 AS 全体にフラッディングします。変換時には、集約およびフィルタリングがサポートされます。NSSA 外部 LSA の詳細については、「リンクステート アドバタイズメント」（P.3-5）を参照してください。

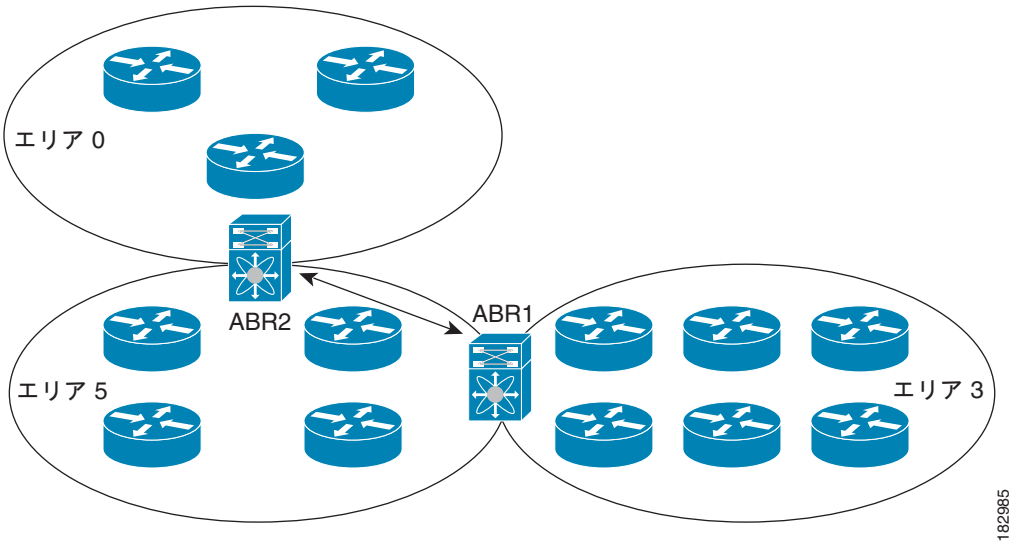
たとえば、OSPFv2 を使用する中央サイトを、異なるルーティング プロトコルを使用するリモート サイトに接続するときに NSSA を使用すると、管理作業を簡素化できます。リモート サイトへのルートはスタブ エリア内に再配布できないため、NSSA を使用する前に、企業サイトの境界ルータとリモート ルータの間の接続を OSPFv2 スタブ エリアとして実行できません。NSSA を使用すると、企業のルータとリモート ルータ間のエリアを NSSA として定義する（「NSSA の設定」（P.3-26）を参照）ことで、OSPFv2 を拡張してリモート接続性をサポートできます。

バックボーン エリア 0 を NSSA にできません。

仮想リンク

仮想リンクを使用すると、物理的に直接接続できない場合に、OSPFv2 エリア ABR をバックボーン エリア ABR に接続できます。図 3-4 は、エリア 3 をエリア 5 経由でバックボーン エリアに接続する仮想リンクを示します。

図 3-4　仮想リンク



また、仮想リンクを使用して、分割エリアから一時的に回復できます。分割エリアは、エリア内のリンクがダウンしたために隔離された一部のエリアで、ここからはバックボーン エリアへの代表 ABR に到達できません。

ルートの再配布

OSPFv2 は、ルート再配布を使用して、他のルーティング プロトコルからルートを学習できます。「ルートの再配布」（P.1-6）を参照してください。リンク コストをこれらの再配布されたルートに割り当てるか、またはデフォルト リンク コストを再配布されたすべてのルートに割り当てるように、OSPFv2 を設定します。

ルート再配布では、ルートマップを使用して、再配布する外部ルートを管理します。ルート マップの設定の詳細については、第 11 章「Route Policy Manager の設定」を参照してください。ルートマップを使用して、これらの外部ルートがローカル OSPFv2 AS でアドバタイズされる前に AS 外部（タイプ 5）LSA および NSSA 外部（タイプ 7）LSA のパラメータを変更できます。

ルート集約

OSPFv2 は、学習したすべてのルートを、すべての OSPF 対応ルータと共有するため、ルート集約を使用して、すべての OSPF 対応ルータにフラッディングされる一意のルートの数を削減した方がよい場合があります。ルート集約により、より具体的な複数のアドレスが、すべての具体的なアドレスを表す 1 つのアドレスに置き換えられるため、ルート テーブルが簡素化されます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

一般的には、ABR の境界ごとに集約します。集約は 2 つのエリアの間でも設定できますが、バックボーンの方向に集約する方が適切です。こうすると、バックボーンがすべての集約アドレスを受信し、すでに集約されているそれらのアドレスを他のエリアに投入できるためです。集約には、次の 2 タイプがあります。

- エリア間ルート集約
- 外部ルート集約

エリア間ルート集約は ABR 上で設定し、AS 内のエリア間のルートを集約します。集約の利点を生かすには、これらのアドレスを 1 つの範囲内にまとめることができるように、連続するネットワーク番号をエリア内で割り当てる必要があります。

外部ルート集約は、ルート再配布を使用して OSPFv2 に投入される外部ルートに特有のルート集約です。集約する外部の範囲が連続していることを確認する必要があります。異なる 2 台のルータからの重複範囲を集約すると、誤った宛先にパケットが送信される原因となる場合があります。外部ルート集約は、ルートを OSPF に再配布している ASBR で設定してください。

集約アドレスの設定時に Cisco NX-OS は、ルーティング ブラック ホールおよびルート ループを防ぐために、集約アドレスの廃棄ルートを自動的に設定します。

OSPFv2 スタブ ルータ アドバタイズメント

OSPFv2 スタブ ルータ アドバタイズメント機能を使用して、OSPFv2 インターフェイスをスタブ ルータとして機能するように設定できません。この機能は、ネットワークに新規ルータを機能制限付きで導入する場合や、過負荷になっているルータの負荷を制限する場合など、このルータ経由の OSPFv2 トラフィックを制限するときに使用します。また、この機能は、さまざまな管理上またはトラフィック エンジニアリング上の理由により使用される場合もあります。

OSPFv2 スタブ ルータ アドバタイズメントは、OSPFv2 ルータをネットワーク トポロジから削除しませんが、他の OSPFv2 ルータがこのルータを使用して、ネットワークの他の部分にトラフィックをルーティングできないようにします。このルータを宛先とするトラフィック、またはこのルータに直接接続されたトラフィックだけが送信されます。

OSPFv2 スタブ ルータ アドバタイズメントは、すべてのスタブ リンク（ローカル ルータに直接接続された）を、ローカル OSPFv2 インターフェイスのコストとしてマークします。すべてのリモート リンクは、最大のコスト（0xFFFF）としてマークされます。

複数の OSPFv2 インスタンス

Cisco NX-OS は、同じノード上で動作する、OSPFv2 プロトコルの複数インスタンスをサポートしています。同一インターフェイスには複数のインスタンスを設定できません。デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。複数のインスタンスが同じ OSPFv2 AS にある場合は、各インスタンスのルータ ID を手動で設定する必要があります。

SPF 最適化

Cisco NX-OS は、次の方法で SPF アルゴリズムを最適化します。

- ネットワーク（タイプ 2）LSA、ネットワーク集約（タイプ 3）LSA、および AS 外部（タイプ 5）LSA 用の部分的 SPF：これらの LSA のいずれかが変更されると、Cisco NX-OS は、全体的な SPF 計算ではなく、高速部分計算を実行します。
- SPF タイマー：さまざまなタイマーを設定して、SPF 計算を制御できます。これらのタイマーには、後続の SPF 計算の幾何バックオフが含まれます。幾何バックオフにより、複数の SPF 計算による CPU 負荷が制限されます。

仮想化のサポート

OSPFv2 は、Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング / 転送インスタンス）をサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。各 OSPFv2 インスタンスは、システム制限値の範囲で複数の VRF をサポートできます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

OSPFv2 のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	OSPFv2 には、LAN Base Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、*『Cisco NX-OS Licensing Guide』を参照してください。*

OSPFv2 の前提条件

OSPFv2 には、次の前提条件があります。

- OSPF を設定するための、ルーティングの基礎に関する詳しい知識がある。
- スイッチにログインしている。
- リモート OSPFv2 ネイバーと通信可能な IPv4 用インターフェイスが 1 つ以上設定されている。
- LAN Base Services ライセンスがインストールされている。
- OSPFv2 ネットワーク戦略と、ネットワークのプランニングが完成している。たとえば、複数のエリアが必要かどうかを決定する必要があります。
- OSPF 機能がイネーブルにされている（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

注意事項および制約事項

OSPFv2 設定時の注意事項および制約事項は次のとおりです。

- Cisco NX-OS は、ユーザがエリアを 10 進表記で入力するか、ドット付き 10 進表記で入力するかに関係なく、ドット付き 10 進表記でエリアを表示します。
- vPC 環境で OSPF を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピアリンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch(config-router)# timers throttle spf 1 50 50
switch(config-router)# timers lsa-arrival 10
```

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

デフォルト設定

表 3-2 に、OSPFv2 パラメータのデフォルト設定を示します。

表 3-2　デフォルトの OSPFv2 パラメータ

パラメータ	デフォルト
hello 間隔	10 秒
デッド間隔	40 秒
OSPFv2 機能	ディセーブル
スタブ ルータ アドバタイズメントの宣言期間	600 秒
リンク コスト計算の参照帯域幅	40 Gbps
LSA 最小到着時間	1000 ミリ秒
LSA グループ ペーシング	240 秒
SPF 計算初期遅延時間	0 ミリ秒
SPF 計算ホールド タイム	5000 ミリ秒
SPF 計算初期遅延時間	0 ミリ秒

基本的 OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計したあとに設定します。

ここでは、次の内容について説明します。

OSPFv2 機能のイネーブル化

OSPFv2 を設定するには、その前に OSPFv2 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature ospf**
3. （任意）**show feature**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**feature ospf** **Example:** switch(config)# feature ospf	OSPFv2 機能をイネーブルにします。
ステップ 3	**show feature** **Example:** switch(config)# show feature	（任意）イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

OSPFv2 機能をディセーブルにし、関連付けられた設定をすべて削除するには、**no feature ospf** コマンドを使用します。

コマンド	目的
no feature ospf **Example:** switch(config)# no feature ospf	OSPFv2 機能をディセーブルにして、関連付けられた設定をすべて削除します。

OSPFv2 インスタンスの作成

OSPFv2 設定の最初のステップは OSPFv2 インスタンスの作成です。作成した OSPFv2 インスタンスには、一意のインスタンス タグを割り当てます。インスタンス タグは任意の文字列です。

OSPFv2 インスタンス パラメータの詳細については、「拡張 OSPFv2 の設定」（P.3-23）を参照してください。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

show ip ospf *instance-tag* コマンドを使用して、インスタンス タグが使用されていないことを確認します。

OSPFv2 がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順の概要

1. **configure terminal**

2. **router ospf** *instance-tag*
3. （任意）**router-id** *ip-address*
4. （任意）**show ip ospf** *instance-tag*
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**router-id** *ip-address* **Example:** switch(config-router)# router-id 192.0.2.1	（任意）OSPFv2 ルータ ID を設定します。この IP アドレスにより、この OSPFv2 インスタンスが識別されます。このアドレスは、システムの設定済みインターフェイス上に存在する必要があります。
ステップ 4	**show ip ospf** *instance-tag* **Example:** switch(config-router)# show ip ospf 201	（任意）OSPF 情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

OSPFv2 インスタンスと、関連付けられた設定をすべて削除するには、**no router ospf** コマンドを使用します。

コマンド	目的
no router ospf *instance-tag* **Example:** switch(config)# no router ospf 201	OSPF インスタンスと、関連付けられた設定を削除します。

（注）　このコマンドは、インターフェイス モードでは OSPF 設定を削除しません。インターフェイス モードで設定された OSPFv2 コマンドはいずれも、手動で削除する必要があります。

OSPFv2 インスタンス上のオプション パラメータの設定

OSPF のオプション パラメータを設定できます。

OSPFv2 インスタンス パラメータの詳細については、「拡張 OSPFv2 の設定」（P.3-23）を参照してください。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

OSPFv2 がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順の詳細

ルータ コンフィギュレーション モードで、次の OSPFv2 用オプション パラメータを設定できます。

コマンド	目的
distance *number* **Example:** `switch(config-router)# distance 25`	この OSPFv2 インスタンスのアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトは 110 です。

log-adjacency-changes [**detail**]
 	
Example:
`switch(config-router)#`
`log-adjacency-changes`
	ネイバーの状態が変化するたびに、システム メッセージを生成します。

maximum-paths *path-number* **Example:** `switch(config-router)# maximum-paths 4`	ルート テーブル内の宛先への同じ OSPFv2 パスの最大数を設定します。このコマンドはロード バランシングに使用されます。指定できる範囲は 1 ～ 16 です。デフォルトは 8 です。

次の例は、OSPFv2 インスタンスを作成する方法を示しています。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# copy running-config startup-config
```

OSPFv2 でのネットワークの設定

ルータがこのネットワークへの接続に使用するインターフェイスを介して、OSPFv2 へのネットワークを関連付けることで、このネットワークを設定できます（「ネイバー」（P.3-2）を参照）。すべてのネットワークをデフォルト バックボーン エリア（エリア 0）に追加したり、任意の 10 進数または IP アドレスを使用して新規エリアを作成したりできます。

（注） すべてのエリアは、バックボーン エリアに直接、または仮想リンク経由で接続する必要があります。

（注） インターフェイスに有効な IP アドレスを設定するまでは、OSPF はインターフェイス上でイネーブルにされません。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **ip address** *ip-prefix/length*
5. **ip router ospf** *instance-tag* **area** *area-id* [**secondaries none**]
6. （任意）**show ip ospf** *instance-tag* **interface** *interface-type slot/port*
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip address** *ip-prefix/length* **Example:** `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	**ip router ospf** *instance-tag* **area** *area-id* [**secondaries none**] **Example:** `switch(config-if)# ip router ospf 201 area 0.0.0.15`	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。

	コマンド	目的
ステップ 6	**show ip ospf** *instance-tag* **interface** *interface-type slot/port* **Example:** `switch(config-if)# show ip ospf 201 interface ethernet 1/2`	（任意）OSPF 情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

インターフェイス コンフィギュレーション モードで、省略可能な次の OSPFv2 パラメータを設定できます。

コマンド	目的
ip ospf cost *number* **Example:** `switch(config-if)# ip ospf cost 25`	このインターフェイスの OSPFv2 コスト メトリックを設定します。デフォルトでは、参照帯域幅とインターフェイス帯域幅に基づいて、コスト メトリックが計算されます。有効な範囲は 1 ～ 65535 です。
ip ospf dead-interval *seconds* **Example:** `switch(config-if)# ip ospf dead-interval 50`	OSPFv2 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
ip ospf hello-interval *seconds* **Example:** `switch(config-if)# ip ospf hello-interval 25`	OSPFv2 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルト値は 10 秒です。
ip ospf mtu-ignore **Example:** `switch(config-if)# ip ospf mtu-ignore`	OSPFv2 で、ネイバーとのあらゆる IP MTU 不一致が無視されるように設定します。デフォルトでは、ネイバー MTU がローカル インターフェイス MTU が不一致の場合には、隣接関係が確立されません。
ip ospf passive-interface **Example:** `switch(config-if)# ip ospf passive-interface`	インターフェイス上でルーティングが更新されないようにします。
ip ospf priority *number* **Example:** `switch(config-if)# ip ospf priority 25`	エリアの DR の決定に使用される OSPFv2 プライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。「指定ルータ」（P.3-3）を参照してください。
ip ospf shutdown **Example:** `switch(config-if)# ip ospf shutdown`	このインターフェイス上の OSPFv2 インスタンスをシャットダウンします。

次に、OSPFv2 インスタンス 201 にネットワーク エリア 0.0.0.10 を追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

インターフェイス設定を確認するには、**show ip ospf interface** コマンドを使用します。このインターフェイスのネイバーを確認するには、**show ip ospf neighbor** コマンドを使用します。

エリアの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のキーチェーンを作成します。*『Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(3)N1(1)』を参照してください。*

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **area** *area-id* **authentication** [**message-digest**]
4. **interface** *interface-type slot/port*
5. **no switchport**
6. （任意）**ip ospf authentication-key** [**0** | **3**] *key*
   または
   （任意）**ip ospf message-digest-key** *key-id* **md5** [**0** | **3**] *key*
7. （任意）**show ip ospf** *instance-tag* **interface** *interface-type slot/port*
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **authentication** [**message-digest**] **Example:** switch(config-router)# area 0.0.0.10 authentication	エリアの認証モードを設定します。
ステップ 4	**interface** *interface-type slot/port* **Example:** switch(config-router)# interface ethernet 1/2 switch(config-if)#	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	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 6	**ip ospf authentication-key** [**0** | **3**] *key* **Example:** switch(config-if)# ip ospf authentication-key 0 mypass	（任意）このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージ ダイジェストにも設定されていない場合は、このコマンドを使用します。0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パスワードを 3DES 暗号化として設定します。
	ip ospf message-digest-key *key-id* **md5** [**0** | **3**] *key* **Example:** switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass	（任意）このインターフェイスにメッセージ ダイジェスト認証を設定します。認証がメッセージ ダイジェストに設定されている場合は、このコマンドを使用します。key-id の範囲は 1 ～ 255 です。MD5 オプションが 0 の場合はパスワードがクリア テキストで設定され、3 の場合はパス キーが 3DES 暗号化として設定されます。
ステップ 7	**show ip ospf** *instance-tag* **interface** *interface-type slot/port* **Example:** switch(config-if)# show ip ospf 201 interface ethernet 1/2	（任意）OSPF 情報を表示します。
ステップ 8	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

インターフェイスの認証の設定

エリア内の個々のインターフェイスに認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のキーチェーンを作成します。*『Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(3)N1(1)』を参照してください。*

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **ip ospf authentication** [**message-digest**]
5. （任意）**ip ospf authentication key-chain** *key-id*
6. （任意）**ip ospf authentication-key** [**0** | **3**] *key*
7. （任意）**ip ospf message-digest-key** *key-id* **md5** [**0** | **3**] *key*
8. （任意）**show ip ospf** *instance-tag* **interface** *interface-type slot/port*
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip ospf authentication** [**message-digest**] **Example:** `switch(config-if)# ip ospf authentication`	OSPFv2 のインターフェイス認証モードをクリアテキスト タイプとメッセージ ダイジェスト タイプのどちらかでイネーブルにします。このインターフェイスのエリアに基づく認証が無効になります。すべてのネイバーが、この認証タイプを共有する必要があります。

	コマンド	目的
ステップ 5	**ip ospf authentication key-chain** *key-name* **Example:** switch(config-if)# ip ospf authentication key-chain Test1	（任意）OSPFv2 のキーチェーンを使用するようにインターフェイス認証を設定します。キーチェーンの詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(3)N1(1)*』を参照してください。
ステップ 6	**ip ospf authentication-key** [**0** | **3** | **7**] *key* **Example:** switch(config-if)# ip ospf authentication-key 0 mypass	（任意）このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージ ダイジェストにも設定されていない場合は、このコマンドを使用します。 オプションは次のとおりです。 • 0：パスワードをクリア テキストで設定します。 • 3：パス キーを 3DES 暗号化として設定します。 • 7：パス キーを Cisco タイプ 7 暗号化として設定します。
ステップ 7	**ip ospf message-digest-key** *key-id* **md5** [**0** | **3** | **7**] *key* **Example:** switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass	（任意）このインターフェイスにメッセージ ダイジェスト認証を設定します。認証がメッセージ ダイジェストに設定されている場合は、このコマンドを使用します。key-id の範囲は 1 ～ 255 です。MD5 オプションは次のとおりです。 • 0：パスワードをクリア テキストで設定します。 • 3：パス キーを 3DES 暗号化として設定します。 • 7：パス キーを Cisco タイプ 7 暗号化として設定します。
ステップ 8	**show ip ospf** *instance-tag* **interface** *interface-type slot/port* **Example:** switch(config-if)# show ip ospf 201 interface ethernet 1/2	（任意）OSPF 情報を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、インターフェイスに暗号化されていない簡単なパスワードを設定し、イーサネット インターフェイス 1/2 のパスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip ospf authentication
switch(config-if)# ip ospf authentication-key 0 mypass
switch(config-if)# copy running-config startup-config
```

拡張 OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計したあとに設定します。

ここでは、次の内容について説明します。

境界ルータのフィルタ リストの設定

OSPFv2 ドメインを、関連性のある各ネットワークを含む一連のエリアに分離できます。すべてのエリアは、ABR 経由でバックボーン エリアに接続している必要があります。OSPFv2 ドメインは、*自律システム境界ルータ*（ASBR）を介して、外部ドメインにも接続可能です。「エリア」（P.3-4）を参照してください。

ABR には、省略可能な次の設定パラメータがあります。

- Area range：エリア間のルート集約を設定します。
- Filter list：ABR 上で、外部エリアから受信したネットワーク集約（タイプ 3）LSA をフィルタリングします。

ASBR もフィルタ リストをサポートしています。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

フィルタ リストが、着信または発信ネットワーク集約（タイプ 3）LSA の IP プレフィクスのフィルタリングに使用するルートマップを作成します。第 11 章「Route Policy Manager の設定」を参照してください。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **area** *area-id* **filter-list route-map** *map-name* {**in** | **out**}
4. （任意）**show ip ospf policy statistics**

5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **filter-list route-map** *map-name* {**in** | **out**} **Example:** switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in	ABR 上で着信または発信ネットワーク集約（タイプ 3）LSA をフィルタリングします。
ステップ 4	**show ip ospf policy statistics area** *id* **filter-list** {**in** | **out**} **Example:** switch(config-if)# show ip ospf policy statistics area 0.0.0.10 filter-list in	（任意）OSPF ポリシー情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、エリア 0.0.0.10 でフィルタ リストを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router)# copy running-config startup-config
```

スタブ エリアの設定

OSPFv2 ドメインの、外部トラフィックが不要な部分にスタブ エリアを設定できます。スタブ エリアは AS 外部（タイプ 5）LSA をブロックし、不要な、選択したネットワークへの往復のルーティングを制限します。「スタブ エリア」（P.3-8）を参照してください。また、すべての集約ルートがスタブ エリアを経由しないようブロックすることもできます。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

設定されるスタブ エリア内に、仮想リンクと ASBR のいずれも含まれないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **area** *area-id* **stub**
4. （任意）**area** *area-id* **default-cost** *cost*
5. （任意）**show ip ospf** *instance-tag*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **stub** **Example:** switch(config-router)# area 0.0.0.10 stub	このエリアをスタブ エリアとして作成します。
ステップ 4	**area** *area-id* **default-cost** *cost* **Example:** switch(config-router)# area 0.0.0.10 default-cost 25	（任意）このスタブ エリアに送信されるデフォルト集約ルートのコスト メトリックを設定します。指定できる範囲は 0 ～ 16777215 です。デフォルトは 1 です。
ステップ 5	**show ip ospf** *instance-tag* **Example:** switch(config-if)# show ip ospf 201	（任意）OSPF 情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、スタブ エリアを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 stub
switch(config-router)# copy running-config startup-config
```

Totally Stubby エリアの設定

Totally Stubby エリアを作成して、すべての集約ルート更新がスタブ エリアを経由しないようにすることができます。

Totally Stubby エリアを作成するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
area *area-id* **stub no-summary** **Example:** `switch(config-router)# area 20 stub no-summary`	このエリアを Totally Stubby エリアとして作成します。

NSSA の設定

OSPFv2 ドメインの、ある程度の外部トラフィックが必要な部分に NSSA を設定できます。「Not-So-Stubby エリア」（P.3-9）を参照してください。また、この外部トラフィックを AS 外部（タイプ 5）LSA に変換して、このルーティング情報で OSPFv2 ドメインをフラッディングすることもできます。NSSA は、省略可能な次のパラメータで設定できます。

- No redistribution：再配布されたルートが NSSA をバイパスして、OSPFv2 AS 内の他のエリアに再配布されます。このオプションは、NSSA ASBR が ABR も兼ねているときに使用します。
- Default information originate：外部 AS へのデフォルト ルートの NSSA 外部（タイプ 7）LSA を生成します。このオプションは、ASBR のルーティング テーブルにデフォルト ルートが含まれる場合に NSSA ASBR 上で使用します。このオプションは、ASBR のルーティング テーブルにデフォルト ルートが含まれるかどうかに関係なく、NSSA ASBR 上で使用できます。
- Route map：目的のルートだけが NSSA および他のエリア全体でフラッディングされるように、外部ルートをフィルタリングします。
- Translate：NSSA 外のエリア向けに、NSSA 外部 LSA を AS 外部 LSA に変換します。再配布されたルートを OSPFv2 AS 全体でフラッディングするには、このコマンドを NSSA ABR 上で使用します。また、これらの AS 外部 LSA の転送アドレスを無効にすることもできます。このオプションを選択した場合は、転送アドレスが 0.0.0.0 に設定されます。
- No summary：すべての集約ルートが NSSA でフラッディングされないようにします。このオプションは NSSA ABR 上で使用します。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

設定する NSSA 上に仮想リンクがないことと、この NSSA がバックボーン エリアでないことを確認します。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*

3. **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**route-map** *map-name*]] [**no-summary**] [**translate type7** {**always** | **never**} [**suppress-fa**]]
4. （任意）**area** *area-id* **default-cost** *cost*
5. （任意）**show ip ospf** *instance-tag*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**] [**route-map** *map-name*]] [**no-summary**] [**translate type7** {**always**	**never**} [**suppress-fa**]] **Example:** switch(config-router)# area 0.0.0.10 nssa	このエリアを NSSA として作成します。
ステップ 4	**area** *area-id* **default-cost** *cost* **Example:** switch(config-router)# area 0.0.0.10 default-cost 25	（任意）この NSSA に送信されるデフォルト集約ルートのコスト メトリックを設定します。
ステップ 5	**show ip ospf** *instance-tag* **Example:** switch(config-if)# show ip ospf 201	（任意）OSPF 情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

次に、デフォルト ルートを生成する NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

次に、外部ルートをフィルタリングし、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

次に、常に NSSA 外部（タイプ 5）LSA を AS 外部（タイプ 7）LSA に変換する NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

仮想リンクの設定

仮想リンクは、隔離されたエリアを、中継エリア経由でバックボーン エリアに接続します。「仮想リンク」（P.3-9）を参照してください。仮想リンクには、省略可能な次のパラメータを設定できます。

- Authentication：簡単なパスワード認証または MD5 メッセージ ダイジェスト認証、および関連付けられたキーを設定します。
- Dead interval：ローカル ルータがデッドであることを宣言し、隣接関係を解消する前に、ネイバーが hello パケットを待つ時間を設定します。
- Hello interval：連続する hello パケット間の時間間隔を設定します。
- Retransmit interval：連続する LSA 間の推定時間間隔を設定します。
- Transmit delay：LSA をネイバーに送信する推定時間を設定します。

（注）　リンクがアクティブになる前に、関与する両方のルータで仮想リンクを設定する必要があります。

スタブ エリアには仮想リンクを追加できません。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **area** *area-id* **virtual-link** *router-id*
4. （任意）**show ip ospf virtual-link [brief]**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **virtual-link** *router-id* **Example:** switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3 switch(config-router-vlink)#	リモート ルータへの仮想リンクの端を作成します。仮想リンクをリモート ルータ上に作成して、リンクを完成させる必要があります。
ステップ 4	**show ip ospf virtual-link** [**brief**] **Example:** switch(config-router-vlink)# show ip ospf virtual-link	（任意）OSPF 仮想リンク情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-router-vlink)# copy running-config startup-config	（任意）この設定の変更を保存します。

仮想リンク コンフィギュレーション モードで、省略可能な次のコマンドを設定できます。

コマンドまたはアクション	目的
authentication [**key-chain** *key-id* | **message-digest** | **null**] **Example:** switch(config-router-vlink)# authentication message-digest	（任意）これにより、エリアに基づくこの仮想リンクの認証が無効となります。
authentication-key [**0** | **3**] *key* **Example:** switch(config-router-vlink)# authentication-key 0 mypass	（任意）この仮想リンクに簡易パスワードを設定します。認証が、キーチェーンにもメッセージ ダイジェストにも設定されていない場合は、このコマンドを使用します。0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パスワードを 3DES 暗号化として設定します。
dead-interval *seconds* **Example:** switch(config-router-vlink)# dead-interval 50	（任意）OSPFv2 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。

コマンドまたはアクション	目的
hello-interval *seconds* **Example:** switch(config-router-vlink)# hello-interval 25	（任意）OSPFv2 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルト値は 10 秒です。
message-digest-key *key-id* **md5** [**0** | **3**] *key* **Example:** switch(config-router-vlink)# message-digest-key 21 md5 0 mypass	（任意）この仮想リンクにメッセージ ダイジェスト認証を設定します。認証がメッセージ ダイジェストに設定されている場合は、このコマンドを使用します。0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。
retransmit-interval *seconds* **Example:** switch(config-router-vlink)# retransmit-interval 50	（任意）OSPFv2 再送間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 です。
transmit-delay *seconds* **Example:** switch(config-router-vlink)# transmit-delay 2	（任意）OSPFv2 送信遅延を秒単位で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

次に、2 つの ABR 間に簡単な仮想リンクを作成する例を示します。

ABR 1（ルータ ID 27.0.0.55）の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3
switch(config-router-vlink)# copy running-config startup-config
```

ABR 2（ルータ ID 10.1.2.3）の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 101
switch(config-router)# area 0.0.0.10 virtual-link 27.0.0.55
switch(config-router-vlink)# copy running-config startup-config
```

再配布の設定

他のルーティング プロトコルから学習したルートを、ASBR 経由で OSPFv2 AS に再配布できます。

OSPF でのルート再配布には、省略可能な次のパラメータを設定できます。

- Default information originate : 外部 AS へのデフォルト ルートの AS 外部（タイプ 5）LSA を生成します。

（注） Default information originate はオプションのルート マップ内の **match** 文を無視します。

- Default metric : すべての再配布ルートに同じコスト メトリックを設定します。

（注） スタティック ルートを再配布する場合は、Cisco NX-OS でもデフォルト スタティック ルートが再配布されます。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

再配布で使用する、必要なルートマップを作成します。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name*
4. **default-information originate** [**always**] [**route-map** *map-name*]
5. **default-metric** *cost*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name* **Example:** switch(config-router)# redistribute bgp 64496 route-map FilterExternalBGP	設定したルートマップ経由で、選択したプロトコルを OSPF に再配布します。 **（注）** スタティック ルートを再配布する場合は、Cisco NX-OS でもデフォルト スタティック ルートが再配布されます。
ステップ 4	**default-information originate** [**always**] [**route-map** map-name] **Example:** switch(config-router)# default-information-originate route-map DefaultRouteFilter	デフォルト ルートが RIB に存在する場合は、この OSPF ドメインにデフォルト ルートを作成します。次の省略可能なキーワードを使用します。 • **always**：ルートが RIB に存在しない場合でも、常にデフォルト ルートの 0.0.0. を生成します。 • **route-map**：ルート マップが true を返す場合にデフォルト ルートを生成します。 **（注）** このコマンドは、ルート マップの **match** 文を無視します。

	コマンド	目的
ステップ 5	**default-metric** *cost* **Example:** switch(config-router)# default-metric 25	再配布されたルートのコスト メトリックを設定します。これは、直接接続されたルートには適用されません。ルート マップを使用して、直接接続されたルートのデフォルトのメトリックを設定します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ボーダー ゲートウェイ プロトコル（BGP）を OSPF に再配布する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布によって、OSPFv2 ルート テーブルに多くのルートが追加される可能性があります。外部プロトコルから受け取るルートの数に最大制限を設定できます。OSPFv2 には、再配布ルートの制限を設定するために次のオプションが用意されています。

- Fixed limit：OSPFv2 が設定された最大値に達したときにメッセージを記録します。OSPFv2 は以降の再配布ルートを受け取りません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv2 がこのしきい値を超えたときに警告を記録するようにすることもできます。
- Warning only：OSPFv2 が最大値に達したときに警告だけを記録します。OSPFv2 は引き続き再配布ルートを受け取ります。
- Widthdraw：OSPFv2 が最大に達した場合に、設定済みのタイムアウト期間を開始します。このタイムアウト期間後、現在の再配布されたルート数が最大制限より少なければ、OSPFv2 はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、OSPFv2 はすべての再配布されたルートを取り消します。OSPFv2 が追加の再配布されたルートを受け付ける前に、この状況を解消する必要があります。
  任意で、タイムアウト期間を設定できます。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **redistribute** {**bgp** *id* | **direct**| **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name*
4. **redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]]
5. （任意）**show running-config ospf**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name* **Example:** switch(config-router)# redistribute bgp route-map FilterExternalBGP	設定したルートマップ経由で、選択したプロトコルを OSPF に再配布します。
ステップ 4	**redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]] **Example:** switch(config-router)# redistribute maximum-prefix 1000 75 warning-only	OSPFv2 で配布する最大プレフィクス数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • *threshold*：警告メッセージをトリガーする最大プレフィクスの割合。 • **warning-only**：プレフィクスの最大数を超えたときに警告メッセージを記録します。 • **withdraw**：再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。*num-retries* の範囲は 1 ～ 12 です。*timeout* は 60 ～ 600 秒です。デフォルト値は 300 秒です。すべてのルートが取り消された場合は、**clear ip ospf redistribution** を使用してください。
ステップ 5	**show running-config ospf** **Example:** switch(config-router)# show running-config ospf	（任意）OSPFv2 の設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、OSPF に再配布されるルートの数を制限する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

ルート集約の設定

集約されたアドレス範囲を設定して、エリア間ルートのルート集約を設定できます。また、ASBR 上のこれらのルートの集約アドレスを設定して、外部の再配布されたルートのルート集約を設定することもできます。「ルート集約」（P.3-10）を参照してください。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **area** *area-id* **range** *ip-prefix/length* [**no-advertise**]
4. **summary-address** *ip-prefix/length* [**no-advertise** | **tag** *tag-id*]
5. （任意）**show ip ospf summary-address**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**area** *area-id* **range** *ip-prefix/length* [**no-advertise**] **Example:** switch(config-router)# area 0.0.0.10 range 10.3.0.0/16	一定の範囲のアドレスの集約アドレスを ABR 上に作成します。この集約アドレスをネットワーク集約（タイプ 3）LSA にアドバタイズしないようにすることもできます。
ステップ 4	**summary-address** *ip-prefix/length* [**no-advertise** | **tag** tag] **Example:** switch(config-router)# summary-address 10.5.0.0/16 tag 2	一定の範囲のアドレスの集約アドレスを ABR 上に作成します。ルートマップによる再配布で使用できるよう、この集約アドレスにタグを割り当てることもできます。

	コマンド	目的
ステップ 5	**show ip ospf summary-address** **Example:** switch(config-router)# show ip ospf summary-address	（任意）OSPF 集約アドレスに関する情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ABR 上のエリア間の集約アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 range 10.3.0.0/16
switch(config-router)# copy running-config startup-config
```

次に、ABR 上の集約アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# summary-address 10.5.0.0/16
switch(config-router)# copy running-config startup-config
```

スタブ ルート アドバタイズメントの設定

短期間だけ、このルータ経由の OSPFv2 トラフィックを制限する場合は、スタブ ルート アドバタイズメントを使用します。「OSPFv2 スタブ ルータ アドバタイズメント」（P.3-11）を参照してください。

スタブ ルート アドバタイズメントは、省略可能な次のパラメータで設定できます。

- On startup：指定した宣言期間だけ、スタブ ルート アドバタイズメントを送信します。
- Wait for BGP：BGP がコンバージェンスするまで、スタブ ルート アドバタイズメントを送信します。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **max-metric router-lsa** [**on-startup** [*announce-time*] [**wait-for bgp** *tag*]]
4. （任意）**copy running-config startup-config**

（注）　ルータの実行コンフィギュレーションがグレースフル シャットダウンを行うよう設定されている場合は、その実行コンフィギュレーションを保存しないでください。保存すると、ルータが、リロード後に最大メトリックをアドバタイズし続けることになります。

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**max-metric router-lsa** [**on-startup** [*announce-time*] [**wait-for bgp** *tag*]] **Example:** switch(config-router)# max-metric router-lsa	OSPFv2 スタブ ルート アドバタイズメントを設定します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、起動時にスタブ ルータ アドバタイズメント機能を、デフォルトの 600 秒間イネーブルにする例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# max-metric router-lsa on-startup
switch(config-router)# copy running-config startup-config
```

デフォルト タイマーの変更

OSPFv2 には、プロトコル メッセージの動作および SPF 計算を制御する数多くのタイマーが含まれます。OSPFv2 には、省略可能な次のタイマー パラメータが含まれます。

- LSA arrival time：ネイバーから着信する LSA 間で許容される最小間隔を設定します。この時間より短時間で到着する LSA はドロップされます。
- Pacing LSAs：LSA が集められてグループ化され、リフレッシュされて、チェックサムが計算される間隔、つまり期限切れとなる間隔を設定します。このタイマーは、LSA 更新が実行される頻度を制御し、LSA 更新メッセージで送信される LSA 更新の数を制御します（「フラッディングと LSA グループ ペーシング」（P.3-6）を参照）。
- Throttle LSAs：LSA 生成のレート制限を設定します。このタイマーは、トポロジが変更されない場合に LSA が生成される頻度を制御します。
- Throttle SPF calculation：SPF 計算の実行頻度を制御します。

インターフェイス レベルでは、次のタイマーも制御できます。

- Retransmit interval：連続する LSA 間の推定時間間隔を設定します。
- Transmit delay：LSA をネイバーに送信する推定時間を設定します。

hello 間隔とデッド タイマーに関する情報の詳細については、「OSPFv2 でのネットワークの設定」（P.3-16）を参照してください。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **timers lsa-arrival** *msec*
4. **timers lsa-group-pacing** *seconds*
5. **timers throttle lsa** *start-time hold-interval max-time*
6. **timers throttle spf** *delay-time hold-time*
7. **interface** *type slot/port*
8. **no switchport**
9. **ip ospf hello-interval** *seconds*
10. **ip ospf dead-interval** *seconds*
11. **ip ospf retransmit-interval** *seconds*
12. **ip ospf transmit-delay** *seconds*
13. （任意）**show ip ospf**
14. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router ospf** *instance-tag*
	
	Example:
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**timers lsa-arrival** *msec* **Example:** `switch(config-router)# timers lsa-arrival 2000`	LSA 到着時間をミリ秒で設定します。指定できる範囲は 10 ～ 600000 です。デフォルトは 1000 ミリ秒です。

	コマンド	目的
ステップ 4	**timers lsa-group-pacing** *seconds* **Example:** `switch(config-router)# timers lsa-group-pacing 1800`	LSA がグループ化される間隔を秒で設定します。指定できる範囲は 1 ～ 1800 です。デフォルトは 240 秒です。
ステップ 5	**timers throttle lsa** *start-time hold-interval max-time* **Example:** `switch(config-router)# timers throttle lsa 3000 6000 6000`	次のタイマーを使用して、LSA 生成のレート制限をミリ秒で設定します。 *start-time*：指定できる範囲は 50 ～ 5000 ミリ秒です。デフォルト値は 50 ミリ秒です。 *hold-interval*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 *max-time*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 6	**timers throttle spf** *delay-time hold-time max-wait* **Example:** `switch(config-router)# timers throttle spf 3000 2000 4000`	SPF 最適パス スケジュール初期遅延時間と、各 SPF 最適パス計算間の最小ホールド タイム（秒単位）を設定します。指定できる範囲は 1 ～ 600000 です。デフォルトは、遅延時間なし、およびホールド タイム 5000 ミリ秒です。

ステップ 7	**interface** *type slot/port*
	
	Example:
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		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 8	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 9	**ip ospf hello-interval** *seconds* **Example:** `switch(config-if)# ip ospf retransmit-interval 30`	このインターフェイスの hello 間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 です。
ステップ 10	**ip ospf dead-interval** *seconds* **Example:** `switch(config-if)# ip ospf dead-interval 30`	このインターフェイスのデッド間隔を設定します。有効な範囲は 1 ～ 65535 です。
ステップ 11	**ip ospf retransmit-interval** *seconds* **Example:** `switch(config-if)# ip ospf retransmit-interval 30`	このインターフェイスから送信される各 LSA 間の推定時間間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 です。

ステップ 12	**ip ospf transmit-delay** *seconds*
	
	Example:
	`switch(config-if)# ip ospf transmit-delay 450`
	`switch(config-if)#`
		LSA をネイバーに送信する推定時間間隔を秒で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

	コマンド	目的
ステップ 13	**show ip ospf** **Example:** switch(config-if)# show ip ospf	（任意）OSPF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、lsa-group-pacing オプションで LSA フラッディングを制御する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

OSPFv2 インスタンスの再起動

OSPFv2 インスタンスを再起動できます。再起動すると、インスタンスのすべてのネイバーが消去されます。

OSPFv2 インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

コマンド	目的
restart ospf instance-tag **Example:** switch(config)# restart ospf 201	OSPFv2 インスタンスを再起動して、すべてのネイバーを削除します。

仮想化による OSPFv2 の設定

複数の VRF を作成できます。また、各 VRF で同じ OSPFv2 インスタンスを使用することも、複数の OSPFv2 インスタンスを使用することも可能です。VRF には OSPFv2 インターフェイスを割り当てます。

（注）　インターフェイスの VRF を設定したあとに、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

はじめる前に

OSPF 機能がイネーブルにされていることを確認します（「OSPFv2 機能のイネーブル化」（P.3-13）を参照）。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf_name*

3. **router ospf** *instance-tag*
4. **vrf** *vrf-name*
5. **maximum-paths** *paths*
6. **interface** *interface-type slot/port*
7. **no switchport**
8. **vrf member** *vrf-name*
9. **ip-address** *ip-prefix/length*
10. **ip router ospf** *instance-tag* **area** *area-id*
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF 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** *instance-tag* **Example:** switch(config-vrf)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 4	**vrf** *vrf-name* **Example:** switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	VRF 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	**maximum-paths** *paths* **Example:** switch(config-router-vrf)# maximum-paths 4	（任意）この VRF のルート テーブル内の宛先への、同じ OSPFv2 パスの最大数を設定します。ロード バランシングに使用されます。
ステップ 6	**interface** *interface-type slot/port* **Example:** switch(config-router-vrf)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

	コマンド	目的
ステップ 8	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 9	**ip address** *ip-prefix/length* **Example:** switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 10	**ip router ospf** *instance-tag* **area** *area-id* **Example:** switch(config-if)# ip router ospf 201 area 0	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 11	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config)# router ospf 201
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# vrf member NewVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config)# copy running-config startup-config
```

OSPFv2 設定の確認

OSPFv2 の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip ospf	OSPFv2 設定を表示します。
show ip ospf border-routers [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 境界ルータ設定を表示します。
show ip ospf database [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 リンクステート データベースの要約を表示します。
show ip ospf interface *number* [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 インターフェイス設定を表示します。
show ip ospf lsa-content-changed-list *interface-type number*	変更された OSPFv2 LSA を表示します。

コマンド	目的
show ip ospf neighbors [*neighbor-id*] [**detail**] [*interface-type number*] [**vrf** {*vrf-name* | **all** | **default** | **management**}] [**summary**]	OSPFv2 ネイバーの一覧を表示します。
show ip ospf request-list *neighbor-id* [*interface-type number*]	OSPFv2 リンクステート要求の一覧を表示します。
show ip ospf retransmission-list *neighbor-id* [*interface-type number*]	OSPFv2 リンクステート再送の一覧を表示します。
show ip ospf route [*ospf-route*] [**summary**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]	内部 OSPFv2 ルートを表示します。
show ip ospf summary-address [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 集約アドレスに関する情報を表示します。
show ip ospf virtual-links [**brief**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 仮想リンクに関する情報を表示します。
show ip ospf vrf {*vrf-name* | **all** | **default** | **management**}	VRF ベースの OSPFv2 設定に関する情報を表示します。
show running-configuration ospf	現在実行中の OSPFv2 設定を表示します。

OSPFv2 統計情報の表示

OSPFv2 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip ospf policy statistics area *area-id* **filter-list** {**in** | **out**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]	エリアの OSPFv2 ルート ポリシー統計情報を表示します。
show ip ospf policy statistics redistribute {**bgp** *id*| **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} *vrf* {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 ルート ポリシー統計情報を表示します。
show ip ospf statistics [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 イベント カウンタを表示します。
show ip ospf traffic [*interface-type number*] [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv2 パケット カウンタを表示します。

OSPFv2 の設定例

次に、OSPFv2 を設定する例を示します。

```
feature ospf
router ospf 201
 router-id 290.0.2.1
```

```
interface ethernet 1/2
 no switchport
 ip router ospf 201 area 0.0.0.10
 ip ospf authentication
 ip ospf authentication-key 0 mypass
```

その他の関連資料

OSPF の実装に関する詳細情報については、次のページを参照してください。

- 「関連資料」（P.3-43）
- 「MIB」（P.3-43）

関連資料

関連項目	マニュアル名
OSPFv2 CLI コマンド	『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』
ルート マップ	第 11 章「Route Policy Manager の設定」

MIB

管理情報ベース（MIB）	MIB のリンク
• OSPF-MIB • OSPF-TRAP-MIB	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

OSPFv2 機能の履歴

表 3-3 は、この機能のリリースの履歴です。

表 3-3　OSPFv2 機能の履歴

機能名	リリース	機能情報
OSPFv2	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 4

EIGRP の設定

この章では、Cisco NX-OS スイッチに Enhanced Interior Gateway Routing Protocol（*EIGRP*）を設定する方法について説明します。

この章では、次の内容について説明します。

EIGRP について

EIGRP は、リンクステート プロトコルの機能にディスタンス ベクトル プロトコルの利点を組み合わせたプロトコルです。EIGRP は、定期的に Hello メッセージを送信してネイバーを探索します。EIGRP は、新規ネイバーを検出すると、すべてのローカル EIGRP ルートおよびルート メトリックに対する 1 回限りの更新を送信します。受信側の EIGRP ルータは、受信したメトリックと、その新規ネイバーにローカルで割り当てられたリンクのコストに基づいて、ルート ディスタンスを計算します。この最初の全面的なルート テーブルの更新後は、ルート変更の影響を受けるネイバーにのみ、差分更新が EIGRP により送信されます。この処理により、コンバージェンスにかかる時間が短縮され、EIGRP が使用する帯域幅が最小限になります。

ここでは、次の内容について説明します。

EIGRP のコンポーネント

EIGRP には、次の基本コンポーネントがあります。

Reliable Transport Protocol

Reliable Transport Protocol により、すべてのネイバーへの EIGRP パケットの配信が保証されます。（「ネイバー探索およびネイバー回復」（P.4-2）を参照）。Reliable Transport Protocol は、マルチキャスト パケットとユニキャスト パケットの混合伝送をサポートしています。この転送は信頼性が高く、未確認パケットが保留されているときにも、マルチキャスト パケットの迅速な送信が可能です。この方式により、さまざまな速度のリンクでも短いコンバージェンス時間が維持されるようになります。マルチキャスト パケットとユニキャスト パケットの送信を制御するデフォルト タイマーの変更の詳細については、「高度な EIGRP の設定」（P.4-14）を参照してください。

Reliable Transport Protocol には、次のメッセージ タイプが含まれます。

- Hello：ネイバー探索およびネイバー回復に使用されます。EIGRP はデフォルトでは、定期的なマルチキャスト Hello メッセージをローカル ネットワーク上に、設定された *hello 間隔*で送信します。デフォルトの hello 間隔は 5 秒です。
- 確認：更新、照会、返信を確実に受信したことを確認します。
- 更新：ルーティング情報が変更されると、その影響を受けるネイバーに送信されます。更新には、ルートの宛先、アドレス マスク、および遅延や帯域幅などのルート メトリックが含まれます。更新情報は EIGRP トポロジ テーブルに格納されます。
- 照会および返信：必要に応じて、EIGRP が使用する DUAL の一部として送信されます。

ネイバー探索およびネイバー回復

EIGRP は、Reliable Transport Protocol からの Hello メッセージを使用して、直接接続されたネットワーク上のネイバー EIGRP ルータを探索します。EIGRP により、ネイバー テーブルにネイバーが追加されます。ネイバー テーブルの情報には、ネイバー アドレス、検出されたインターフェイス、および*ホールド タイム*が含まれています。ホールド タイムは、ネイバー到達不能を宣言する前に EIGRP が待機する時間を示します。デフォルトのホールド タイムは、hello 間隔の 3 倍または 15 秒です。

EIGRP は、ローカル EIGRP ルーティング情報を共有するために、一連の更新メッセージを新規ネイバーに送信します。このルート情報は EIGRP トポロジ テーブルに格納されます。このように EIGRP ルート情報全体を最初に送信したあとは、ルーティングが変更されたときにのみ、EIGRP により更新メッセージが送信されます。これらの更新メッセージは新情報または更新情報のみを含んでおり、変更の影響を受けるネイバーにのみ送信されます。「EIGRP ルート更新」（P.4-3）を参照してください。

EIGRP はネイバーへのキープアライブとして、Hello メッセージも使用します。Hello メッセージを受信している限り、Cisco NX-OS は、ネイバーがダウンせずに機能していると判定します。

拡散更新アルゴリズム

拡散更新アルゴリズム（DUAL）により、トポロジ テーブルの宛先ネットワークに基づいてルーティング情報が計算されます。トポロジ テーブルには、次の情報が含まれます。

- IPv4 アドレス/マスク：この宛先のネットワーク アドレスおよびネットワーク マスク。
- サクセサ：すべての*フィジブル サクセサ*または、現在の *フィジブル ディスタンス*よりも短いディスタンスをアドバタイズするネイバーの IP アドレスおよびローカル インターフェイス接続。
- Feasibility Distance（FD; フィジブル ディスタンス）：計算された、宛先までの最短ディスタンス。フィジブル ディスタンスは、ネイバーがアドバタイズした距離に、そのネイバーへのリンク コストを加えた合計です。

DUAL は、ディスタンス メトリックを使用して、ループが発生しない効率的なパスを選択します。DUAL はルートを選択し、フィジブル サクセサに基づいてユニキャスト Routing Information Base（RIB; ルーティング情報ベース）に挿入します。トポロジが変更されると、DUAL は、トポロジ テーブルでフィジブル サクセサを探します。フィジブル サクセサが見つかった場合、DUAL は、最短のフィジブル ディスタンスを持つフィジブル サクセサを選択して、それをユニキャスト RIB に挿入します。これにより、再計算が不要となります。

フィジブル サクセサが存在しないが、宛先をアドバタイズするネイバーが存在する場合は、DUAL がパッシブ状態からアクティブ状態へと移行し、新しいサクセサまたは宛先へのネクストホップ ルータを決定する再計算をトリガーします。ルートの再計算に必要な時間はコンバージェンス時間に影響します。EIGRP は照会メッセージをすべてのネイバーに送信し、フィジブル サクセサを探します。フィジブル サクセサを持つネイバーは、その情報を含む返信メッセージを送信します。フィジブル サクセサを持たないネイバーは、DUAL の再計算をトリガーします。

EIGRP ルート更新

トポロジが変更されると、EIGRP は、変更されたルーティング情報のみを含む更新メッセージを、影響を受けるネイバーに送信します。更新メッセージには、新規の、または更新されたネットワーク宛先へのディスタンス情報が含まれます。

EIGRP でのディスタンス情報は、帯域幅、遅延、負荷使用状況、リンクの信頼性などの使用可能なルート メトリックの組み合わせとして表現されます。各メトリックには重みが関連付けられており、これにより、メトリックがディスタンスの計算に含まれるかどうかが決定します。このメトリックの重みは設定することができます。特性を微調整して最適なパスを完成することもできますが、設定可能なメトリックの大部分でデフォルト設定を使用することを推奨します。

ここでは、次の内容について説明します。

- 「内部ルート メトリック」（P.4-3）
- 「外部ルート メトリック」（P.4-4）
- 「EIGRP とユニキャスト RIB」（P.4-4）

内部ルート メトリック

内部ルートとは、同じ EIGRP 自律システム内のネイバー間のルートです。これらのルートには、次のメトリックがあります。

- ネクストホップ：ネクストホップ ルータの IP アドレス。
- 遅延：宛先ネットワークへのルートを形成するインターフェイス上で設定された遅延の合計。10 マイクロ秒単位で設定されます。

- 帯域幅：宛先へのルートの一部であるインターフェイスで設定された最小帯域幅から計算されます。

（注）　デフォルト帯域幅の値の使用を推奨します。この帯域幅パラメータは EIGRP でも使用されます。

- MTU：宛先へのルート上の最大伝送単位の最小値。
- ホップ カウント：宛先までにルートが通過するホップまたはルータの数。このメトリックは、DUAL 計算で直接には使用されません。
- 信頼性：宛先までのリンクの信頼性を示します。
- 負荷：宛先までのリンク上のトラフィック量を示します。

デフォルトで EIGRP は、帯域幅と遅延のメトリックを使用して、宛先までのディスタンスを計算します。計算に他のメトリックが含まれるように、メトリックの重みを変更できます。

外部ルート メトリック

外部ルートとは、異なる EIGRP AS にあるネイバー間のルートです。これらのルートには、次のメトリックがあります。

- ネクストホップ：ネクストホップ ルータの IP アドレス。
- ルータ ID：このルートを EIGRP に再配布したルータのルータ ID。
- AS 番号：宛先の AS の番号。
- プロトコル ID：宛先へのルートを学習したルーティング プロトコルを表すコード。
- タグ：ルートマップで使用可能な任意のタグ。
- メトリック：外部ルーティング プロトコルの、このルートのルート メトリック。

EIGRP とユニキャスト RIB

EIGRP は、学習したルートをすべて、EIGRP トポロジ テーブルとユニキャスト RIB に追加します。トポロジが変更されると、EIGRP は、これらのルートを使用してフィジブル サクセサを探します。EIGRP は、他のルーティング プロトコルから EIGRP に再配布されたあらゆるルートの変更についてのユニキャスト RIB からの通知も待ち受けます。

高度な EIGRP

EIGRP の高度な機能を使用して、EIGRP の設定を最適化できます。

ここでは、次の内容について説明します。

- 「スプリット ホライズン」（P.4-7）
- 「仮想化のサポート」（P.4-7）

アドレス ファミリ

EIGRP は、IPv4 アドレス ファミリをサポートします。

アドレス ファミリ コンフィギュレーション モードには、次の EIGRP 機能が含まれます。

- 認証
- AS 番号
- デフォルト ルート
- メトリック
- ディスタンス
- グレースフル リスタート
- ロギング
- ロード バランシング
- 再配布
- ルータ ID
- スタブ ルータ
- タイマー

複数のコンフィギュレーション モードで同じ機能を設定できません。たとえばルータ コンフィギュレーション モードでデフォルト メトリックを設定すると、アドレス ファミリ モードでデフォルト メトリックを設定できません。

認証

EIGRP メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。EIGRP 認証は MD5 認証ダイジェストをサポートしています。

認証キーのキーチェーン管理を使用して、Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスごと、またはインターフェイスごとに EIGRP 認証を設定できます。キーチェーン管理を使用すると、MD5 認証ダイジェストが使用する認証キーへの変更を管理できます。キーチェーンの作成については、*『Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)』*を参照してください。

MD5 認証を行うには、ローカル ルータとすべてのリモート EIGRP ネイバーで同一のパスワードを設定します。EIGRP メッセージが作成されると、Cisco NX-OS は、そのメッセージ自体と暗号化されたパスワードに基づいて MD5 一方向メッセージ ダイジェストを作成し、このダイジェストを EIGRP メッセージとともに送信します。受信する EIGRP ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合は計算が同一であるため、EIGRP メッセージは有効と見なされます。

MD5 認証には各 EIGRP メッセージのシーケンス番号も含まれており、これにより、ネットワークでのメッセージの再送が防止されます。

スタブ ルータ

EIGRP スタブ ルーティング機能を使用して、ネットワークの安定性を向上させ、リソースの使用を削減し、スタブ ルータ設定を簡素化することができます。スタブ ルータは、リモート ルータ経由で EIGRP ネットワークに接続します。「スタブ ルーティング」（P.1-7）を参照してください。

EIGRP スタブ ルーティングを使用すると、EIGRP を使用するように配布とリモート ルータを設定し、リモート ルータのみをスタブとして設定する必要があります。EIGRP スタブ ルーティングで、分散ルータでの集約が自動的にイネーブルになるわけではありません。ほとんどの場合、分散ルータでの集約の設定が必要です。

EIGRP スタブ ルーティングを使用しない場合は、分散ルータからリモート ルータに送信されたルートがフィルタリングまたは集約されたあとでも、問題が発生することがあります。たとえば、ルートが企業ネットワーク内のどこかで失われた場合に、EIGRP が分散ルータに照会を送信することがあります。分散ルータは、ルートが集約されている場合でも、リモート ルータに照会を送信することがあります。分散ルータとリモート ルータの間の WAN リンク上の通信に問題が発生した場合は、EIGRP がアクティブ状態のままとなり、ネットワークの他の場所が不安定となる場合があります。EIGRP スタブ ルーティングを使用すると、リモート ルータに照会が送信されなくなります。

ルート集約

指定したインターフェイスにサマリー集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

より具体的なアドレスがルーティング テーブルにある場合、EIGRP は、より具体的なルートの最小メトリックに等しいメトリックを持つインターフェイスからの集約アドレスをアドバタイズします。

（注）　EIGRP は、自動ルート集約をサポートしていません。

ルートの再配布

EIGRP を使用して、ダイレクト ルート、スタティック ルート、他の EIGRP AS から学習したルート、または他のプロトコルからのルートを再配布できます。再配布を含むルート マップを設定して、どのルートが EIGRP に渡されるかを制御します。ルート マップを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。第 11 章「Route Policy Manager の設定」を参照してください。

インポートされた EIGRP へのすべてのルートに使用されるデフォルト メトリックも設定できます。

ロード バランシング

ロード バランシングを使用すると、ルータによって、宛先アドレスから同じ距離にあるすべてのルータ ネットワーク ポートにトラフィックが分散されます。ロード バランシングにより、ネットワーク セグメントの使用率が向上し、それによってネットワーク帯域幅の効率も向上します。

Cisco NX-OS は、EIGRP ルート テーブルおよびユニキャスト RIB 中の 16 までの等コスト パスを使用する Equal Cost Multiple Path（ECMP; 等コスト マルチパス）機能をサポートしています。これらのパスの一部または全部に対してトラフィックのロード バランスを行うよう、EIGRP を設定できます。

（注）　Cisco NX-OS の EIGRP は、等コストでないロード バランシングをサポートしていません。

スプリット ホライズン

スプリット ホライズンを使用して、EIGRP が、ルートを伝えたインターフェイスからそのルートをアドバタイズしないようにすることができます。

スプリット ホライズンは、EIGRP 更新パケットおよび EIGRP 照会パケットの送信を制御する方式です。インターフェイスでスプリット ホライズンをイネーブルにすると、Cisco NX-OS は、このインターフェイスから学習された宛先への更新パケットも照会パケットも送信しません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループの可能性が低くなります。

ポイズン リバースによるスプリット ホライズンにより、EIGRP は、EIGRP がルートを学習したインターフェイス経由で、そのルートを到達不能としてアドバタイズするよう設定されます。

EIGRP は、次のシナリオでスプリット ホライズン、またはポイズン リバースによるスプリット ホライズンを使用します。

- スタートアップ モードで、2 台のルータ間で初めてトポロジ テーブルを交換する。
- トポロジ テーブルの変更をアドバタイズする。
- 照会メッセージを送信する。

デフォルトでは、スプリット ホライズン機能がすべてのインターフェイスでイネーブルになっています。

仮想化のサポート

Cisco NX-OS は、同じシステム上で動作する、EIGRP プロトコルの複数インスタンスをサポートしています。EIGRP は、Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスをサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。第 9 章「レイヤ 3 仮想化の設定」を参照してください。

デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。インスタンスごとに一意のルータ ID を設定することもできます。

EIGRP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	EIGRP には、LAN Base Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、*『Cisco NX-OS Licensing Guide』を参照してください。*

EIGRP の前提条件

EIGRP を使用するには、次の前提条件を満たしている必要があります。

- EIGRP 機能がイネーブルにされている（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

注意事項および制約事項

EIGRP 設定時の注意事項および制約事項は次のとおりです。

- 他のプロトコル、接続されたルータ、またはスタティック ルートからの再配布には、メトリック設定（デフォルト メトリック設定オプションまたはルート マップによる）が必要です（第 11 章「Route Policy Manager の設定」を参照）。
- グレースフル スタートについては、NSF 認識ルータが動作中であり、ネットワークで完全に収束している場合にのみ、このルータが NSF 対応ルータのグレースフル リスタート動作を支援できます。
- グレースフル リスタートについては、グレースフル リスタートに関係する隣接スイッチが NSF-aware、または NSF-capable である必要があります。
- Cisco NX-OS EIGRP は Cisco IOS ソフトウェアの EIGRP と互換性があります。
- 妥当な理由がない限り、メトリックの重みを変更しないでください。メトリックの重みを変更した場合は、同じ AS 内のすべての EIGRP ルータに、それを適用する必要があります。
- 大規模ネットワークの場合は、スタブの使用を検討してください。
- EIGRP ベクトル メトリックは維持されないため、異なる EIGRP AS 間での再配布は避けてください。
- **no ip next-hop-self** コマンドは、ネクスト ホップの到達可能性を保証しません。
- **ip passive-interface eigrp** コマンドを使用すると、ネイバーが形成されなくなります。
- Cisco NX-OS は IGRP も、IGRP および EIGRP クラウドの接続もサポートしていません。
- 自動集約は、デフォルトではイネーブルにされていません。
- Cisco NX-OS は IP のみをサポートしています。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

デフォルト設定

表 4-1 は、各 EIGRP パラメータに対するデフォルト設定を示します。

表 4-1　デフォルト EIGRP パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	• 内部ルート：90 • 外部ルート：170
帯域幅の割合	50%
再配布されたルートのデフォルトのメトリック	• bandwidth：100000 kbps • delay：100（10 マイクロ秒単位） • reliability：255 • loading：1 • MTU：1500

表 4-1　デフォルト EIGRP パラメータ （続き）

パラメータ	デフォルト
EIGRP 機能	ディセーブル
hello 間隔	5 秒
ホールド タイム	15 秒
等コスト パス	8
メトリック重み	1 0 1 0 0
アドバタイズされたネクストホップ アドレス	ローカル インターフェイスの IP アドレス
NSF コンバージェンス時間	120
NSF ルート保留時間	240
NSF 信号送信時間	20
再分配	ディセーブル
スプリット ホライズン	イネーブル

基本的 EIGRP の設定

ここでは、次の内容について説明します。

EIGRP 機能のイネーブル化

EIGRP を設定するには、その前に EIGRP 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature eigrp**
3. （任意）**show feature**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**feature eigrp** **Example:** switch(config)# feature eigrp	EIGRP 機能をイネーブルにします。
ステップ 3	**show feature** **Example:** switch(config)# show feature	（任意）イネーブルにされた機能の情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

EIGRP 機能をディセーブルにし、関連付けられた設定をすべて削除するには、**no feature eigrp** コマンドを使用します。

コマンド	目的
no feature eigrp **Example:** switch(config)# no feature eigrp	EIGRP 機能をディセーブルにして、関連付けられたコンフィギュレーションをすべて削除します。

EIGRP インスタンスの作成

EIGRP インスタンスを作成して、そのインスタンスにインターフェイスを関連付けることができます。この EIGRP プロセスに一意の AS 番号を割り当てます（「自律システム」（P.1-5）を参照）。ルート再配布をイネーブルにしていない限り、他の AS からルートがアドバタイズされることも、受信されることもありません。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

EIGRP がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

AS 番号であると認められていないインスタンス タグを設定する場合は、AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

手順の概要

1. **configure terminal**

2. **router eigrp** *instance-tag*
3. （任意）**autonomous-system** *as-number*
4. （任意）**log-adjacency-changes**
5. （任意）**log-neighbor-warnings [***seconds***]**
6. **interface** *interface-type slot/port*
7. **no switchport**
8. **ip router eigrp** *instance-tag*
9. **show ip eigrp interfaces**
10. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp Test1 switch(config-router)#	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	**autonomous-system** *as-number* **Example:** switch(config-router)# autonomous-system 33	（任意）この EIGRP インスタンスに一意の AS 番号を設定します。有効な範囲は 1 ～ 65535 です。
ステップ 4	**log-adjacency-changes** **Example:** switch(config-router)# log-adjacency-changes	（任意）。隣接関係の状態が変化するたびに、システム メッセージを生成します。このコマンドは、デフォルトでイネーブルにされています。
ステップ 5	**log-neighbor-warnings** [*seconds*] **Example:** switch(config-router)# log-neighbor-warnings	（任意）ネイバー警告が発生するたびに、システム メッセージを生成します。警告メッセージの時間間隔を、1 ～ 65535 の秒数で設定できます。デフォルト値は 10 秒です。このコマンドは、デフォルトでイネーブルにされています。
ステップ 6	**interface** *interface-type slot/port* **Example:** switch(config-router)# interface ethernet 1/2 switch(config-if)#	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。**?** を使用すると、スロットおよびポートの範囲を確認できます。

	コマンド	目的
ステップ 7	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 8	**ip router eigrp** *instance-tag* **Example:** switch(config-if)# ip router eigrp Test1	このインターフェイスを、設定された EIGRP プロセスに関連付けます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 9	**show ip eigrp interfaces** **Example:** switch(config-if)# show ip eigrp interfaces	EIGRP インターフェイスに関する情報を表示します。
ステップ 10	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

EIGRP プロセスと、関連付けられた設定を削除するには、**no router eigrp** コマンドを使用します。

コマンド	目的
no router eigrp *instance-tag* **Example:** switch(config)# no router eigrp Test1	EIGRP プロセスと、関連付けられたすべての設定を削除します。

（注）　EIGRP プロセスを削除する場合は、インターフェイス モードで設定された EIGRP コマンドも削除する必要があります。

次に、EIGRP プロセスを作成し、EIGRP のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

その他の EIGRP パラメータの詳細については、「高度な EIGRP の設定」（P.4-14）を参照してください。

EIGRP インスタンスの再起動

EIGRP インスタンスは再起動できます。再起動すると、インスタンスのすべてのネイバーが消去されます。

EIGRP インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

コマンド	目的
flush-routes **Example:** switch(config)# flush-routes	（任意）この EIGRP インスタンスを再起動するときに、ユニキャスト RIB のすべての EIGRP ルートをフラッシュします。
restart eigrp instance-tag **Example:** switch(config)# restart eigrp Test1	EIGRP インスタンスを再起動して、すべてのネイバーを削除します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

EIGRP インスタンスのシャットダウン

EIGRP インスタンスを正常にシャットダウンできます。これにより、すべてのルートと隣接関係が削除されますが、EIGRP 設定は保持されます。

EIGRP インスタンスをディセーブルにするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config-router)# **shutdown** **Example:** switch(config-router)# shutdown	この EIGRP インスタンスをディセーブルにします。EIGRP ルータ設定は残ります。

EIGRP の受動インターフェイスの設定

EIGRP の受動インターフェイスを設定できます。受動インターフェイスは、EIGRP 隣接関係に参加しませんが、このインターフェイスのネットワーク アドレスは EIGRP トポロジ テーブルに残ります。

EIGRP の受動インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip passive-interface eigrp *instance-tag*	EIGRP hello を抑制します。これにより、EIGRP インターフェイス上でネイバーがルーティング アップデートを形成および送信することを防ぎます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

インターフェイスでの EIGRP のシャットダウン

インターフェイスで EIGRP を正常にシャットダウンできます。これにより、すべての隣接関係が削除され、このインターフェイスで EIGRP トラフィックが停止しますが、EIGRP 設定は保持されます。

インターフェイスで EIGRP をディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的

`switch(config-if)# ip eigrp instance-tag shutdown`
 	
Example:
`switch(config-router)# ip eigrp Test1 shutdown`
	このインターフェイスで EIGRP をディセーブルにします。EIGRP インターフェイス設定は残ります。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

高度な EIGRP の設定

ここでは、次の内容について説明します。

EIGRP での認証の設定

EIGRP のネイバー間での認証を設定できます。「認証」（P.4-5）を参照してください。

EIGRP プロセスまたは個々のインターフェイスに対応する EIGRP 認証を設定できます。インターフェイスの EIGRP 認証設定は、EIGRP プロセスレベルの認証設定よりも優先します。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

EIGRP プロセスのすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のキーチェーンを作成します。『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。

手順の概要

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **address-family ipv4 unicast**
4. **authentication key-chain** *key-chain*
5. **authentication mode md5**
6. **interface** *interface-type slot/port*
7. **no switchport**
8. **ip router eigrp** *instance-tag*
9. **ip authentication key-chain eigrp** *instance-tag key-chain*
10. **ip authentication mode eigrp** *instance-tag* **md5**
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router eigrp** *instance-tag*
	
	Example:
	`switch(config)# router eigrp Test1`
	`switch(config-router)#`
		インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
		
		AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

ステップ 3	**address-family ipv4 unicast**
	
	Example:
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		アドレス ファミリ コンフィギュレーション モードを開始します。IPv4 の場合、このコマンドはオプションです。

ステップ 4	**authentication key-chain** *key-chain* **Example:** `switch(config-router-af)# authentication key-chain routeKeys`	この VRF の EIGRP プロセスにキーチェーンを関連付けます。キー チェーン名は、大文字と小文字が区別される 20 文字以下の任意の英数字文字列にできます。
ステップ 5	**authentication mode md5** **Example:** `switch(config-router-af)# authentication mode md5`	この VRF の MD5 メッセージ ダイジェスト認証モードを設定します。

	コマンド	目的
ステップ 6	**interface** *interface-type slot/port* **Example:** switch(config-router-af) interface ethernet 1/2 switch(config-if)#	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。**?** を使用すると、サポートされているインターフェイスを調べることができます。
ステップ 7	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 8	**ip router eigrp** *instance-tag* **Example:** switch(config-if)# ip router eigrp Test1	このインターフェイスを、設定された EIGRP プロセスに関連付けます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 9	**ip authentication key-chain eigrp** *instance-tag key-chain* **Example:** switch(config-if)# ip authentication key-chain eigrp Test1 routeKeys	このインターフェイスの EIGRP プロセスにキーチェーンを関連付けます。この設定は、ルータの VRF モードで設定された認証設定よりも優先します。 インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 10	**ip authentication mode eigrp** *instance-tag* **md5** **Example:** switch(config-if)# ip authentication mode eigrp Test1 md5	このインターフェイスの MD5 メッセージ ダイジェスト認証モードを設定します。この設定は、ルータの VRF モードで設定された認証設定よりも優先します。 インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、EIGRP の MD5 メッセージ ダイジェスト認証をイーサネット インターフェイス 1/2 上で設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# ip authentication key-chain eigrp Test1 routeKeys
switch(config-if)# ip authentication mode eigrp Test1 md5
switch(config-if)# copy running-config startup-config
```

EIGRP スタブ ルーティングの設定

ルータで EIGRP スタブ ルーティングを設定するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config-router-af)# **stub** [**direct** | **receive-only** | **redistributed** [**direct**] **leak-map** *map-name*] **Example:** switch(config-router-af)# eigrp stub redistributed	リモート ルータを EIGRP スタブ ルータとして設定します。マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。

次に、直接接続され、再配布されるルートをアドバタイズするスタブ ルータを設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# stub direct redistributed
switch(config-router-af)# copy running-config startup-config
```

ルータがスタブ ルータとして設定されていることを確認するには、**show ip eigrp neighbor detail** コマンドを使用します。出力の最後の行は、リモート ルータまたはスポーク ルータのスタブ ステータスを示します。次に、**show ip eigrp neighbor detail** コマンドの出力例を示します。

```
Router# show ip eigrp neighbor detail
IP-EIGRP neighbors for process 201
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   10.1.1.2                Se3/1         11 00:00:59    1  4500  0  7
   Version 12.1/1.2, Retrans: 2, Retries: 0
   Stub Peer Advertising ( CONNECTED SUMMARY ) Routes
```

EIGRP のサマリー集約アドレスの設定

指定したインターフェイスにサマリー集約アドレスを設定できます。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、それらすべての個別ルートのメトリックのうち最小のメトリックを使用して、集約アドレスをインターフェイスからアドバタイズします。「ルート集約」（P.4-6）を参照してください。

サマリー集約アドレスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的

`switch(config-if)# ip summary-address eigrp` *instance-tag ip-prefix/length* `[`*distance* `|` **leak-map** *map-name*`]`
 	
Example:
`switch(config-if)# ip summary-address eigrp Test1 192.0.2.0/8`
	サマリー集約アドレスを、IP アドレスとネットワーク マスク、または IP プレフィクス/長さとして設定します。インスタンス タグおよびマップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
	
	また、この集約アドレスのアドミニストレーティブ ディスタンスを設定することもできます。集約アドレスのデフォルト アドミニストレーティブ ディスタンスは 5 です。

次に、EIGRP によりネットワーク 192.0.2.0 がイーサネット 1/2 のみに集約されるようにする例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip summary-address eigrp Test1 192.0.2.0 255.255.255.0
```

EIGRP へのルートの再配布

他のルーティング プロトコルから EIGRP にルートを再配布できます。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

他のプロトコルから再配布されるルートには、メトリック（デフォルト メトリック設定オプションまたはルート マップによる）を設定する必要があります。

ルートマップを作成して、EIGRP に再配布されるルートのタイプを管理する必要があります。第 11 章「Route Policy Manager の設定」を参照してください。

手順の概要

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **address-family ipv4 unicast**
4. **redistribute** {**bgp** *as* | {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **direct** | **static**} **route-map** *name*
5. **default-metric** *bandwidth delay reliability loading mtu*
6. **show ip eigrp route-map statistics redistribute**
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp Test1 switch(config-router)#	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	**address-family ipv4 unicast** **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。IPv4 の場合、このコマンドはオプションです。
ステップ 4	**redistribute** {**bgp** *as*| {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **direct** | **static**} **route-map** *name* **Example:** switch(config-router-af)# redistribute bgp 100 route-map BGPFilter	1 つのルーティング ドメインから EIGRP にルートを注入します。インスタンス タグおよびマップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 5	**default-metric** *bandwidth delay reliability loading mtu* **Example:** switch(config-router-af)# default-metric 500000 30 200 1 1500	ルート再配布で学習したルートに割り当てられるメトリックを設定します。デフォルト値は次のとおりです。 • bandwidth：100000 kbps • delay：100（10 マイクロ秒単位） • reliability：255 • loading：1 • MTU：1492
ステップ 6	**show ip eigrp route-map statistics redistribute** **Example:** switch(config-router-af)# show ip eigrp route-map statistics redistribute bgp	EIGRP ルート マップ統計に関する情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、BGP を IPv4 向けの EIGRP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# redistribute bgp 100 route-map BGPFilter
switch(config-router)# default-metric 500000 30 200 1 1500
switch(config-router)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布では、多くのルートを EIGRP ルート テーブルに追加できます。外部プロトコルから受け取るルートの数に最大制限を設定できます。EIGRP では、再配布されるルートの上限を設定するために次のオプションが用意されています。

- 上限固定：EIGRP が設定された最大値に達すると、メッセージをログに記録します。EIGRP は、それ以上の再配布されたルートを受け入れません。しきい値を超えたときに EIGRP が警告をログに記録する、最大値のしきい値に対する割合を設定することもできます。
- 警告のみ：EIGRP が最大値に達したときのみ、警告のログを記録します。EIGRP は、再配布されたルートを受け入れ続けます。
- 取り消し：EIGRP が最大値に達すると、タイムアウト期間が開始します。タイムアウト期間の経過後、再配布されたルートの現在数が最大数よりも少ない場合、EIGRP はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、EIGRP はすべての再配布されたルートを取り消します。EIGRP が再配布されたルートをさらに受け入れられるように、この条件をクリアする必要があります。
  任意で、タイムアウト期間を設定できます。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

手順の概要

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name*
4. **redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]]
5. （任意）**show running-config eigrp**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp Test1 switch(config-router)#	インスタンス タグを設定して、新しい EIGRP インスタンスを作成します。
ステップ 3	**redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name* **Example:** switch(config-router)# redistribute bgp route-map FilterExternalBGP	設定したルートマップ経由で、選択したプロトコルを EIGRP に再配布します。
ステップ 4	**redistribute maximum-prefix** *max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timeout*]] **Example:** switch(config-router)# redistribute maximum-prefix 1000 75 warning-only	EIGRP が再配布するプレフィクスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • *threshold*：警告メッセージをトリガーする最大プレフィクスの割合。 • **warning-only**：プレフィクスの最大数を超えたときに警告メッセージを記録します。 • **withdraw**：再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。*num-retries* の範囲は 1 ～ 12 です。*timeout* は 60 ～ 600 秒です。デフォルト値は 300 秒です。すべてのルートが取り消されるときは、**clear ip eigrp redistribution** を使用します。
ステップ 5	**show running-config eigrp** **Example:** switch(config-router)# show running-config eigrp	（任意）EIGRP の設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、EIGRP に再配布されるルートの数を制限する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

EIGRP でのロード バランシングの設定

EIGRP でのロード バランシングを設定できます。最大パス オプションを使用して、ECMP ルートの数を設定できます。「EIGRP でのロード バランシングの設定」（P.4-22）を参照してください。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

手順の概要

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **address-family ipv4 unicast**
4. **maximum-paths** *num-paths*
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router eigrp** *instance-tag*
	
	Example:
	`switch(config)# router eigrp Test1`
	`switch(config-router)#`
		インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
		
		AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。

ステップ 3	**address-family ipv4 unicast**
	
	Example:
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		アドレス ファミリ コンフィギュレーション モードを開始します。IPv4 の場合、このコマンドはオプションです。

ステップ 4	**maximum-paths** *num-paths* **Example:** `switch(config-router-af)# maximum-paths 5`	EIGRP がルート テーブルに受け入れる等コスト パスの数を設定します。指定できる範囲は 1 ～ 16 です。デフォルトは 8 です。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config-router-af)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、6 つまでの等コストパスによる、EIGRP の等コスト ロード バランシングを IPv4 上で設定する例を示します。

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# maximum-paths 6
switch(config-router)# copy running-config startup-config
```

hello パケット間のインターバルとホールド タイムの調整

各 Hello メッセージの間隔とホールド タイムを調整できます。

デフォルトでは、5 秒ごとに Hello メッセージが送信されます。ホールド タイムは Hello メッセージでアドバタイズされ、送信者が有効であると見なすまでの時間をネイバーに示します。デフォルトのホールド タイムは、hello 間隔の 3 倍または 15 秒です。

hello パケットの間隔を変更するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config-if)# **ip hello-interval eigrp** *instance-tag seconds* **Example:** switch(config-if)# ip hello-interval eigrp Test1 30	EIGRP ルーティング処理の hello 間隔を設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。指定できる範囲は 1 ～ 65535 秒です。デフォルトは 5 です。

非常に輻輳した大規模ネットワークでは、一部のルータが、デフォルト ホールド タイム内にネイバーから hello パケットを受信できない可能性があります。この場合は、ホールド タイムを増やすことを推奨します。

ホールド タイムを変更するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config-if)# **ip hold-time eigrp** *instance-tag seconds* **Example:** switch(config-if)# ip hold-time eigrp Test1 30	EIGRP ルーティング処理のホールド タイムを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。有効な範囲は 1 ～ 65535 です。

タイマー設定を確認するには、**show ip eigrp interface detail** コマンドを使用します。

スプリット ホライズンのディセーブル化

スプリット ホライズンを使用して、ルート情報がルータにより、その情報の送信元インターフェイスの外部にアドバタイズされないようにすることができます。通常はスプリット ホライズンにより、特にリンクに障害がある場合に、複数のルーティング スイッチ間での通信が最適化されます。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンをディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config-if)# **no ip split-horizon eigrp** *instance-tag* **Example:** switch(config-if)# no ip split-horizon eigrp Test1	スプリット ホライズンをディセーブルにします。

EIGRP の調整

省略可能なパラメータを設定して、EIGRP をネットワークに合わせて調整できます。

アドレス ファミリ コンフィギュレーション モードでは、次のオプション パラメータを設定できます。

コマンド	目的
default-information originate [**always** | **route-map** *map-name*] **Example:** switch(config-router-af)# default-information originate always	プレフィクス 0.0.0.0/0 を持つデフォルト ルートを発信するか、受け入れます。ルート マップが提供されると、ルート マップが true 状態となっている場合にのみデフォルト ルートが発信されます。マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
distance *internal external* **Example:** switch(config-router-af)# distance 25 100	この EIGRP プロセスのアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。内部の値で、同じ AS 内で学習したルートのディスタンスが設定されます（デフォルト値は 90 です）。外部の値で、外部 AS から学習したルートのディスタンスが設定されます（デフォルト値は 170 です）。
metric maximum-hops *hop-count* **Example:** switch(config-router-af)# metric maximum-hops 70	アドバタイズされるルートに許容される最大ホップ カウントを設定します。ホップ カウントがこの最大値を超えるルートは、到達不能としてアドバタイズされます。指定できる範囲は 1 ～ 255 です。デフォルトは 100 です。

コマンド	目的
metric weights *tos k1 k2 k3 k4 k5* **Example:** switch(config-router-af)# metric weights 0 1 3 2 1 0	EIGRP メトリックまたは K 値を調整します。EIGRP は次の式を使用して、ネットワークへの合計メトリックを決定します。 metric = [k1*bandwidth + (k2*bandwidth)/(256 – load) + k3*delay] * [k5/(reliability + k4)] デフォルト値と指定できる範囲は、次のとおりです。 • TOS：0。指定できる範囲は 0 ～ 8 です。 • k1：1。有効な範囲は 0 ～ 255 です。 • k2：0。有効な範囲は 0 ～ 255 です。 • k3：1。有効な範囲は 0 ～ 255 です。 • k4：0。有効な範囲は 0 ～ 255 です。 • k5：0。有効な範囲は 0 ～ 255 です。
timers active-time {*time-limit* | **disabled**} **Example:** switch(config-router-af)# timers active-time 200.	（照会の送信後に）ルートがアクティブ（SIA）状態のままとなっていることを宣言するまでに、ルータが待機する時間を分単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 3 です。

インターフェイス コンフィギュレーション モードで、省略可能な次のパラメータを設定できます。

コマンド	目的
ip bandwidth eigrp *instance-tag bandwidth* **Example:** switch(config-if)# ip bandwidth eigrp Test1 30000	インターフェイス上の EIGRP の帯域幅メトリックを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。帯域幅の範囲は、1 ～ 2,560,000,000 kbps です。
ip bandwidth-percent eigrp *instance-tag percent* **Example:** switch(config-if)# ip bandwidth-percent eigrp Test1 30	EIGRP がインターフェイス上で使用する可能性のある帯域幅の割合を設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 割合の範囲は 0 ～ 100 です。デフォルトは 50 です。
no ip delay eigrp *instance-tag delay* **Example:** switch(config-if)# ip delay eigrp Test1 100	インターフェイス上の EIGRP の遅延メトリックを設定します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。遅延の範囲は、1 ～ 16777215（10 マイクロ秒単位）です。
ip distribute-list eigrp *instance-tag* {**prefix-list** *name*| **route-map** name} {**in** | **out**} **Example:** switch(config-if)# ip distribute-list eigrp Test1 route-map EigrpTest in	このインターフェイス上の EIGRP のルータ フィルタリング ポリシーを設定します。インスタンス タグ、プレフィクス リスト名、およびルート マップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。

コマンド	目的
no ip next-hop-self eigrp *instance-tag* **Example:** switch(config-if)# ip next-hop-self eigrp Test1	このインターフェイスのアドレスではなく、受信したネクストホップ アドレスを使用するよう、EIGRP を設定します。デフォルトでは、このインターフェイスの IP アドレスをネクストホップ アドレスに使用します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ip offset-list eigrp *instance-tag* {**prefix-list** *name*| **route-map** name} {**in** | **out**} *offset* **Example:** switch(config-if)# ip offfset-list eigrp Test1 prefix-list EigrpList in	EIGRP が学習したルートに、着信および発信メトリックへのオフセットを追加します。インスタンス タグ、プレフィクス リスト名、およびルートマップ名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ip passive-interface eigrp *instance-tag* **Example:** switch(config-if)# ip passive-interface eigrp Test1	EIGRP hello を抑制します。これにより、EIGRP インターフェイス上でネイバーがルーティング アップデートを形成および送信することを防ぎます。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。

EIGRP の仮想化の設定

複数の VRF を作成して、各 VRF で同じまたは複数の EIGRP プロセスを使用することもできます。VRF にはインターフェイスを割り当てます。

（注）　インターフェイスの VRF を設定したあとに、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスの他の設定がすべて削除されます。

はじめる前に

EIGRP 機能がイネーブルにされていることを確認します（「EIGRP 機能のイネーブル化」（P.4-9）を参照）。

VRF を作成します。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **router eigrp** *instance-tag*
4. **interface ethernet** *slot/port*
5. **no switchport**
6. **vrf member** *vrf-name*
7. **ip router eigrp** *instance-tag*
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF コンフィギュレーション モードを開始します。VRN 名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 3	**router eigrp** *instance-tag* **Example:** switch(config)# router eigrp Test1 switch(config-router)#	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていない *instance-tag* を設定する場合は、**autonomous-system** コマンドを使用して AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 4	**interface ethernet** *slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	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。**?** を使用すると、スロットおよびポートの範囲を調査できます。
ステップ 5	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 6	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。VRF 名には最大 20 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 7	**ip router eigrp** *instance-tag* **Example:** switch(config-if)# ip router eigrp Test1	このインターフェイスを EIGRP プロセスに追加します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 8	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# router eigrp Test1
switch(config-router)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router eigrp Test1
switch(config-if)# vrf member NewVRF
switch(config-if)# copy running-config startup-config
```

EIGRP 設定の確認

EIGRP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip eigrp [*instance-tag*]	設定した EIGRP プロセスの要約を表示します。
show ip eigrp [*instance-tag*] **interfaces** [*type number*] [**brief**] [**detail**]	設定されているすべての EIGRP インターフェイスに関する情報を表示します。
show ip eigrp *instance-tag* **neighbors** [*type number*]	すべての EIGRP ネイバーに関する情報を表示します。EIGRP ネイバー設定を確認するには、次のコマンドを使用します。
show ip eigrp [*instance-tag*] **route** [*ip-prefix/length*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**vrf** *vrf-name*]	すべての EIGRP ルートに関する情報を表示します。
show ip eigrp [*instance-tag*] **topology** [*ip-prefix/length*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**vrf** *vrf-name*]	EIGRP トポロジ テーブルに関する情報を表示します。
show running-configuration eigrp	現在実行中の EIGRP コンフィギュレーションを表示します。

EIGRP 統計情報の表示

EIGRP 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip eigrp [*instance-tag*] **accounting** [**vrf** *vrf-name*]	EIGRP の課金統計情報を表示します。
show ip eigrp [*instance-tag*] **route-map statistics redistribute**	EIGRP の再配布統計情報を表示します。
show ip eigrp [*instance-tag*] **traffic** [**vrf** *vrf-name*]	EIGRP のトラフィック統計情報を表示します。

設定：EIGRP の例

次に、EIGRP を設定する例を示します。

```
feature eigrp
interface ethernet 1/2
 no switchport
 ip address 192.0.2.55/24
 ip router eigrp Test1
  no shutdown
router eigrp Test1
  router-id 192.0.2.1
```

関連資料

ルート マップの詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

その他の関連資料

EIGRP の実装に関する詳細情報については、次のページを参照してください。

- 「関連資料」（P.4-30）
- 「MIB」（P.4-30）

関連資料

関連項目	マニュアル名
EIGRP CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*
http://www.cisco.com/warp/public/103/1.html	*『Introduction to EIGRP Tech Note』*
http://www.cisco.com/en/US/tech/tk365/technologies_q_and_a_item09186a008012dac4.shtml	EIGRP Frequently Asked Questions

MIB

管理情報ベース（MIB）	MIB のリンク
CISCO-EIGRP-MIB	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

EIGRP 機能の履歴

表 4-2 は、この機能のリリースの履歴です。

表 4-2　EIGRP 機能の履歴

機能名	リリース	機能情報
EIGRP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 5

ベーシック BGP の設定

この章では、Cisco NX-OS スイッチ上でボーダー ゲートウェイ プロトコル（BGP）を設定する方法について説明します。

この章では、次の内容について説明します。

ベーシック BGP の概要

Cisco NX-OS は BGP バージョン 4 をサポートします。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応スイッチとの間で TCP セッションを確立するための、信頼できるトランスポート プロトコルとして TCP を使用します。

BGP ではパスベクトル ルーティング アルゴリズムを使用して、BGP 対応ネットワーク スイッチまたは *BGP スピーカ*間でルーティング情報を交換します。各 BGP スピーカはこの情報を使用して、特定の宛先までのパスを判別し、なおかつルーティング ループを伴うパスを検出して回避します。ルーティング情報には、宛先の実際のルート プレフィクス、宛先に対する自律システム（AS）のパス、およびその他のパス属性が含まれます。

BGP はデフォルトで、宛先ホストまたはネットワークへのベスト パスとして、1 つだけパスを選択します。各パスは、BGP ベストパス分析で使用される well-known mandatory、well-known discretionary、optional transitive の各属性を伝送します。BGP ポリシーを設定し、これらの属性の一部を変更することによって、BGP パス選択を制御できます。詳細については、「ルート ポリシーおよび BGP セッションのリセット」（P.6-3）を参照してください。

BGP は、ロード バランシングまたは Equal-Cost Multipath（ECMP; 等コスト マルチパス）もサポートします。詳細については、「ロード シェアリングおよびマルチパス」（P.6-6）を参照してください。

ここでは、次の内容について説明します。

BGP AS

自律システム（AS）とは、単一の管理エンティティにより制御されるネットワークです。AS は 1 つまたは複数の IGP および整合性のある一連のルーティング ポリシーを使用して、ルーティング ドメインを形成します。BGP は 16 ビットおよび 32 ビットの AS 番号をサポートします。詳細については、「自律システム」（P.1-5）を参照してください。

個々の BGP AS は external BGP（eBGP; 外部 BGP）ピアリング セッションを通じて、ルーティング情報をダイナミックに交換します。同じ AS 内の BGP スピーカは、internal BGP（iBGP; 内部 BGP）を通じて、ルーティング情報を交換できます。

4 バイトの AS 番号のサポート

BGP では、2 バイトまたは 4 バイトの AS 番号をサポートしています。Cisco NX-OS は、プレーンテキスト表記で 4 バイト（つまり 32 ビットの整数）の AS 番号を表示します。4 バイトの AS 番号は、プレーンテキスト表記（たとえば 1 ～ 4294967295）または AS ドット表記（たとえば 1.0）で設定できます。詳細については、「自律システム」（P.1-5）を参照してください。

アドミニストレーティブ ディスタンス

*アドミニストレーティブ ディスタンス*は、ルーティング情報の送信元の信頼性のランクです。BGP はデフォルトで、表 5-1 のアドミニストレーティブ ディスタンスを使用します。

表 5-1　デフォルトの BGP アドミニストレーティブ ディスタンス

ディスタンス	デフォルト値	機能
外部	20	eBGP から学習したルートに適用。
内部	200	iBGP から学習したルートに適用。
ローカル	200	ルータを起点とするルートに適用。

（注）　アドミニストレーティブ ディスタンスが BGP パス選択アルゴリズムに影響を与えることはありませんが、BGP で学習されたルートが IP ルーティング テーブルに組み込まれるかどうかを左右します。

詳細については、「アドミニストレーティブ ディスタンス」（P.1-7）を参照してください。

BGP ピア

BGP スピーカが別の BGP スピーカを自動的に検出することはありません。ユーザ側で BGP スピーカ間の関係を設定する必要があります。*BGP ピア*は、もう 1 つの BGP スピーカとの間にアクティブな TCP 接続が存在する BGP スピーカです。

BGP セッション

BGP は TCP ポート 179 を使用して、ピアとの TCP セッションを作成します。ピア間で TCP 接続が確立されると、各 BGP ピアは最初に相手と、それぞれのすべてのルートを交換し、BGP ルーティング テーブルを完成させます。初期交換以後、BGP ピアはネットワーク トポロジが変化したとき、またはルーティング ポリシーが変更されたときに、差分アップデートだけを送信します。このようなアップデートからアップデートまでの非アクティブ期間中に、ピアは*キープアライブ*という特殊なメッセージを交換します。*ホールド タイム*は、次の BGP アップデートまたはキープアライブ メッセージを受信するまでに経過することが許容される、最大時間限度です。

Cisco NX-OS は、次のピア設定オプションをサポートします。

- 個別の IPv4 または IPv4 アドレス：BGP は、リモート アドレスと AS 番号が一致する BGP スピーカとのセッションを確立します。
- 単一 AS 番号の IPv4 プレフィクス ピア：BGP は、プレフィクスおよび AS 番号が一致する BGP スピーカとのセッションを確立します。
- ダイナミック AS 番号プレフィクス ピア：BGP は、プレフィクスと、設定済み AS 番号のリストに載っている AS 番号と一致する BGP スピーカとのセッションを確立します。

プレフィクス ピアのダイナミック AS 番号

Cisco NX-OS では、BGP セッションを確立する AS 番号の範囲またはリストを受け入れます。たとえば IPv4 プレフィクス 192.0.2.0/8 および AS 番号 33、66、99 を使用するように BGP を設定する場合、BGP は 192.0.2.1 および AS 番号 66 を使用してセッションを確立しますが、192.0.2.2 および AS 番号 50 からのセッションは拒否します。

Cisco NX-OS では、セッションが確立されるまで internal BGP（iBGP; 内部 BGP）または external BGP（eBGP; 外部 BGP）セッションとして、プレフィクス ピアをダイナミック AS 番号と関連付けません。iBGP および eBGP の詳細については、第 6 章「拡張 BGP の設定」を参照してください。

（注）　ダイナミック AS 番号プレフィクス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。テンプレートの詳細については、第 6 章「拡張 BGP の設定」を参照してください。

BGP ルータ ID

ピア間で BGP セッションを確立するには、BGP に *ルータ ID* を設定する必要があります。ルータ ID は BGP セッションの確立時に、OPEN メッセージで BGP ピアに送信されます。BGP ルータ ID は 32 ビット値であり、IPv4 アドレスで表すことがよくあります。ルータ ID はユーザ側で設定できます。ルータ ID はデフォルトで、Cisco NX-OS によってルータのループバック インターフェイスの IPv4 アドレスに設定されます。ルータ上でループバック インターフェイスが設定されていない場合は、ルータ上の物理インターフェイスに設定されている最大の IPv4 アドレスが BGP ルータ ID を表すものとして、ソフトウェアによって選択されます。BGP ルータ ID は、ネットワーク内の BGP ピアごとに一意である必要があります。

BGP にルータ ID が設定されていない場合、BGP ピアとのピアリング セッションを確立できません。

BGP パスの選択

BGP は複数の送信元から、同じルートのアドバタイズメントを受信する可能性がありますが、BGP はベスト パスとして、パスを 1 つだけ選択します。BGP は、そのパスを IP ルーティング テーブルに格納し、ピアにパスを伝達します。

所定のネットワークでパスが追加または削除されるたびに、ベストパス アルゴリズムが実行されます。ベストパス アルゴリズムは、ユーザが BGP 設定を変更した場合にも実行されます。BGP は所定のネットワークで使用できる一連の有効パスの中から、最適なパスを選択します。

Cisco NX-OS は次の手順で、BGP ベストパス アルゴリズムを実行します。

ステップ 1　2 つのパスを比較し、どちらが適切かを判別します（「ステップ 1：パス ペアの比較」（P.5-4）を参照）。

ステップ 2　すべてのパスを繰り返し、全体として最適なパスを選択するためにパスを比較する順序を決定します（「ステップ 2：比較順序の決定」（P.5-6）を参照）。

ステップ 3　新しいベスト パスを使用するに足るだけの差が新旧のベスト パスにあるかどうかを判別します（「ステップ 3：ベスト パス変更の抑制の決定」（P.5-6）を参照）。

（注）　重要なのは、パート 2 で決定される比較順序です。A、B、C という 3 つのパスがあるとします。A と B を比較して Cisco NX-OS は A を選択します。B と C を比較して Cisco NX-OS は B を選択します。しかし、A と C を比較した場合、Cisco NX-OS は A を選択しません。これは一部の BGP メトリックが同じネイバー AS からのパスだけに適用され、すべてのパスにわたっては適用されないからです。

パス選択には、BGP AS パス属性が使用されます。AS パス属性には、アドバタイズされたパスでたどる自律システム番号（AS 番号）のリストが含まれます。BGP AS を AS の集合または連合に細分化する場合は、AS パスにローカル定義の AS を指定した連合セグメントが含まれます。

ステップ 1：パス ペアの比較

BGP ベストパス アルゴリズムの最初のステップでは、より適切なパスを判別するために 2 つのパスを比較します。次に、Cisco NX-OS が 2 つのパスを比較して、より適切なパスを判別する基本的なステップについて説明します。

1. Cisco NX-OS は、比較のために有効なパスを選択します。（たとえば、到達不能なネクスト ホップがあるパスは無効です）。

2. Cisco NX-OS は、重みが最大のパスを選択します。
3. Cisco NX-OS は、ローカル プリファレンスが最大のパスを選択します。
4. パスの一方がローカル起点の場合、Cisco NX-OS はそのパスを選択します。
5. Cisco NX-OS は、AS パスが短い方のパスを選択します。

（注）　AS パス長を計算するときに、Cisco NX-OS は連合セグメントを無視し、AS セットを 1 として数えます。詳細については、「AS 連合」（P.6-4）を参照してください。

6. Cisco NX-OS は、起点が低い方のパスを選択します。IGP は EGP よりも低いと見なされます。
7. Cisco NX-OS は、Multi Exit Discriminator（MED）が小さい方のパスを選択します。

   このステップが実行されるされないを左右する、一連のオプションを選択できます。Cisco NX-OS が両方のパスの MED を比較するのは、通常、同じ AS のピアからそれらのパスを受け取った場合です。それ以外の場合、Cisco NX-OS は MED の比較を省略します。

   パスのピア AS に関係なく、ベストパス アルゴリズムの MED 比較が必ず実行されるように、Cisco NX-OS を設定することもできます。詳細については、「ベストパス アルゴリズムの調整」（P.6-9）を参照してください。この設定を行わなかった場合、Cisco NX-OS によって MED 比較が実行されるかどうかは、次のように比較する 2 つのパスの AS パス属性によって決まります。

   a. パスに AS パスがない場合、または AS パスが AS_SET で始まる場合、パスは内部であり、Cisco NX-OS は他の内部パスに対して MED を比較します。
   b. AS パスが AS_SEQUENCE から始まる場合、ピア AS がシーケンスで最初の AS 番号になり、Cisco NX-OS は同じピア AS を持つ他のパスに対して MED を比較します。
   c. AS-path パスに連合セグメントだけが含まれている場合、または連合セグメントで始まり、AS_SET が続いている場合、パスは内部であり、Cisco NX-OS は他の内部パスに対して MED を比較します。
   d. AS パスが連合セグメントで始まり、AS_SEQUENCE が続いている場合、ピア AS が AS_SEQUENCE で最初の AS 番号になり、Cisco NX-OS は同じピア AS を持つ他のパスに対して MED を比較します。

   （注）　Cisco NX-OS がパスの指定された MED 属性を受信しなかった場合、欠落 MED が使用可能な最大値になるように、ユーザがベストパス アルゴリズムを設定していない限り、Cisco NX-OS は MED を 0 と見なします。詳細については、「ベストパス アルゴリズムの調整」（P.6-9）を参照してください。

   e. 非決定性の MED 比較機能がイネーブルの場合、ベスト パス アルゴリズムでは Cisco IOS スタイルの MED 比較が使用されます。詳細については、「ベストパス アルゴリズムの調整」（P.6-9）を参照してください。
8. 一方のパスが内部ピアから、他方のパスが外部ピアからの場合、Cisco NX-OS は外部ピアからのパスを選択します。
9. ネクストホップ アドレスへの IGP メトリックが異なるパスの場合、Cisco NX-OS は IGP メトリックが小さい方のパスを選択します。
10. Cisco NX-OS は、最後に実行したベストパス アルゴリズムによって選択されたパスを使用します。

ステップ 1 ～ 9 のすべてのパス パラメータが同じ場合、ルータ ID を比較するようにベストパス アルゴリズムを設定できます。詳細については、「ベストパス アルゴリズムの調整」（P.6-9）を参照してください。パスに発信元属性が含まれている場合、Cisco NX-OS はその属性をルータ ID として使用して

比較します。発信元属性が含まれていない場合、Cisco NX-OS はパスを送信したピアのルータ ID を使用します。パス間でルータ ID が異なる場合、Cisco NX-OS はルータ ID が小さい方のパスを選択します。

（注）　属性の送信元をルータ ID として使用する場合は、2 つのパスに同じルータ ID を設定することができます。また、同じピア ルータとの 2 つの BGP セッションが可能です。したがって、同じルータ ID で 2 つのパスを受信できます。

11. Cisco NX-OS は、クラスタ長が短いほうのパスを選択します。クラスタ リスト属性の指定されたパスを受け取らなかった場合、クラスタ長は 0 です。
12. Cisco NX-OS は、IP アドレスが小さいほうのピアから受信したパスを選択します。ローカル発生のパス（再配布のパスなど）は、ピア IP アドレスが 0 になります。

（注）　ステップ 9 以降が同じパスは、マルチパスを設定している場合、マルチパスに使用できます。詳細については、「ロード シェアリングおよびマルチパス」（P.6-6）を参照してください。

ステップ 2：比較順序の決定

BGP ベストパス アルゴリズム実装の 2 番めのステップでは、Cisco NX-OS がパスを比較する順序を決定します。

1. Cisco NX-OS は、パスをグループに分けます。各グループ内で、Cisco NX-OS はすべてのパスにわたって MED を比較します。Cisco NX-OS は、「ステップ 1：パス ペアの比較」（P.5-4）と同じルールを使用して、2 つのパス間で MED を比較できるかどうかを決定します。この比較では通常、ネイバー AS ごとに 1 つずつグループが選択されます。**bgp bestpath med always** コマンドを設定すると、Cisco NX-OS はすべてのパスが含まれた 1 グループだけを選択します。
2. Cisco NX-OS は、常に最適な方を維持しながら、グループのすべてのパスを反復することによって、各グループのベスト パスを決定します。Cisco NX-OS は、各パスをそれまでの一時的なベスト パスと比較します。それまでのベスト パスよりも適切な場合は、そのパスが新しく一時的なベスト パスになり、Cisco NX-OS はグループの次のパスと比較します。
3. Cisco NX-OS は、ステップ 2 の各グループで選択されたベスト パスからなる、パス セットを形成します。Cisco NX-OS は、このパス セットでもステップ 2 と同様にそれぞれの比較を繰り返すことによって、全体としてのベスト パスを選択します。

ステップ 3：ベスト パス変更の抑制の決定

実装の次のパートでは、Cisco NX-OS が新しいベスト パスを使用するのか抑制するのかを決定します。新しいベスト パスが古いパスとまったく同じ場合、ルータは引き続き既存のベスト パスを使用できます（ルータ ID が同じ場合）。Cisco NX-OS では引き続き既存のベスト パスを使用することによって、ネットワークにおけるルート変更を回避できます。

抑制機能をオフにするには、ルータ ID を比較するようにベスト パス アルゴリズムを設定します。詳細については、「ベストパス アルゴリズムの調整」（P.6-9）を参照してください。この機能を設定すると、新しいベスト パスが常に既存のベスト パスよりも優先されます。

次の条件が発生した場合に、ベスト パス変更を抑制できません。

- 既存のベスト パスが無効になった。
- 既存または新しいベスト パスを内部（または連合）ピアから受信したか、またはローカルに発生した（再配布などによって）。

- 同じピアからパスを受信した（パスのルータ ID が同じ）。
- パス間で重み値、ローカル プリファレンス、オリジン、またはネクストホップ アドレスに対する IGP メトリックが異なっている。
- パス間で MED が異なっている。

BGP およびユニキャスト RIB

BGP はユニキャスト RIB（ルーティング情報ベース）と通信して、ユニキャスト ルーティング テーブルに IPv4 ルートを格納します。ベスト パスの選択後、ベスト パスの変更をルーティング テーブルに反映させる必要があると BGP が判別した場合、BGP はユニキャスト RIB にルート アップデートを送信します。

BGP はユニキャスト RIB における BGP ルートの変更に関して、ルート通知を受け取ります。さらに、再配布をサポートする他のプロトコル ルートに関するルート通知を受け取ります。

BGP はネクストホップの変更に関する通知も、ユニキャスト RIB から受け取ります。BGP はこれらの通知を使用して、ネクストホップ アドレスへの到達可能性および IGP メトリックを追跡します。

ユニキャスト RIB でネクストホップ到達可能性または IGP メトリックが変更されるたびに、BGP は影響を受けるルートについて、ベスト パス再計算を開始させます。

BGP の仮想化

BGP は Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

ベーシック BGP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BGP には、LAN Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。 **（注）** レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP 機能をイネーブルにする必要があります（「BGP 機能のイネーブル化」（P.5-11）を参照）。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。

- 再帰ネクストホップ解決に対応できる IGP を 1 つ以上設定する必要があります。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを設定する必要があります。

BGP に関する注意事項および制限事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- ダイナミック AS 番号プレフィクス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。
- AS 連合でプレフィクス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィクス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ Time-to-Live（TTL; 存続可能時間）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィクス設定オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。
- update-source を設定し、BGP/eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ポリシーを指定します。
- VRF 内で BGP ルータ ID を定義します。
- キープアライブおよびホールド タイマーの値を小さくすると、BGP セッション フラップが発生する可能性があります。
- VRF を設定する場合、該当する VRF を入力します（第 9 章「レイヤ 3 仮想化の設定」を参照）。

CLI コンフィギュレーション モード

ここでは BGP に対応する各 CLI コンフィギュレーション モードの開始方法について説明します。各モードから、**?** コマンドを入力すると、そのモードで使用できるコマンドが表示されます。

ここでは、次の内容について説明します。

グローバル コンフィギュレーション モード

グローバル コンフィギュレーション モードは、BGP プロセスを作成したり、AS 連合、ルート ダンプニングなどの拡張機能を設定したりする場合に使用します。詳細については、第 6 章「拡張 BGP の設定」を参照してください。

次に、ルータ コンフィギュレーション モードを開始する例を示します。

```
switch# configuration
```

```
switch(config)# router bgp 64496
switch(config-router)#
```

BGP は VRF（仮想ルーティングおよびフォワーディング）をサポートします。ネットワークで VRF を使用する場合は、適切な VRF 内で BGP を設定できます。詳細については、「仮想化の設定」（P.6-37）を参照してください。

次に、VRF コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)#
```

アドレス ファミリ コンフィギュレーション モード

任意で、BGP がサポートするアドレス ファミリを設定できます。アドレス ファミリ用の機能を設定する場合は、ルータ コンフィギュレーション モードで **address-family** コマンドを使用します。ネイバーに対応する特定のアドレス ファミリを設定する場合は、ネイバー コンフィギュレーション モードで **address-family** コマンドを使用します。

ルート再配布、アドレス集約、ロード バランシングなどの拡張機能を使用する場合は、アドレス ファミリを設定する必要があります。

次に、ルータ コンフィギュレーション モードからアドレス ファミリ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)#
```

次に、VRF を使用している場合に、VRF アドレス ファミリ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# address-family ipv4 unicast
switch(config-router-vrf-af)#
```

ネイバー コンフィギュレーション モード

Cisco NX-OS には、BGP ピアを設定するためのネイバー コンフィギュレーション モードがあります。ネイバー コンフィギュレーション モードを使用して、ピアのあらゆるパラメータを設定できます。

次に、ネイバー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1
switch(config-router-neighbor)#
```

次に、VRF ネイバー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# neighbor 192.0.2.1
switch(config-router-vrf-neighbor)#
```

ネイバー アドレス ファミリ コンフィギュレーション モード

アドレス ファミリ固有のネイバー設定を入力し、ネイバーのアドレス ファミリをイネーブルにするには、ネイバー コンフィギュレーション サブモード内のアドレス ファミリ コンフィギュレーション サブモードを使用できます。このモードは、所定のネイバーに認められるプレフィクス数の制限、eBGP のプライベート AS 番号の削除といった拡張機能に使用します。

次に、ネイバー アドレス ファミリ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router# neighbor 192.0.2.1
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

次に、VRF ネイバー アドレス ファミリ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64497
switch(config-router)# vrf vrf_A
switch(config-router-vrf)# neighbor 209.165.201.1
switch(config-router-vrf-neighbor)# address-family ipv4 unicast
switch(config-router-vrf-neighbor-af)#
```

デフォルト設定

表 5-2 に、BGP パラメータのデフォルト設定を示します。

表 5-2　デフォルトの BGP パラメータ

パラメータ	デフォルト
BGP 機能	ディセーブル
キープアライブ インターバル	60 秒
ホールド タイマー	180 秒

ベーシック BGP の設定

ベーシック BGP を設定するには、BGP をイネーブルにして、BGP ピアを設定する必要があります。ベーシック BGP ネットワークの設定は、いくつかの必須作業と多数の任意の作業からなります。BGP ルーティング プロセスおよび BGP ピアの設定は必須です。

ここでは、次の内容について説明します。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

BGP 機能のイネーブル化

BGP を設定するには、BGP 機能をイネーブルにしておく必要があります。

手順の概要

1. **configure terminal**
2. **feature bgp**
3. （任意）**show feature**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**feature bgp** **Example:** switch(config)# feature bgp	BGP 機能をイネーブルにします。
ステップ 3	**show feature** **Example:** switch(config)# show feature	（任意）イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

BGP 機能をディセーブルにして、関連するすべての設定を削除する場合は、**no feature bgp** コマンドを使用します。

コマンド	目的
no feature bgp **Example:** switch(config)# no feature bgp	BGP 機能をディセーブルにして、関連するすべての設定を削除します。

BGP インスタンスの作成

BGP インスタンスを作成し、BGP インスタンスにルータ ID を割り当てることができます。「BGP ルータ ID」（P.5-4）を参照してください。Cisco NX-OS は、2 バイトまたは 4 バイトのプレーンテキスト表記または AS ドット表記による AS 番号をサポートします。詳細については、「4 バイトの AS 番号のサポート」（P.5-2）を参照してください。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

BGP はルータ ID（設定済みループバック アドレスなど）を取得できなければなりません。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. （任意）**router-id** *ip-address*
4. （任意）**address-family ipv4** {**unicast** | **multicast**}
5. （任意）**network** *ip-prefix* [**route-map** *map-name*]
6. （任意）**show bgp all**
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 64496 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	**router-id** *ip-address* **Example:** switch(config-router)# router-id 192.0.2.255	（任意）BGP ルータ ID を設定します。この IP アドレスによって、この BGP スピーカを特定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 4	**address-family ipv4**{**unicast**	**multicast**} Example: switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	（任意）IPv4 アドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。このコマンドによって、すべての BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

	コマンド	目的
ステップ 5	**network** *ip-prefix* [**route-map** *map-name*] **Example:** switch(config-router-af)# network 192.0.2.0	（任意）この AS にローカルとしてネットワークを指定し、BGP ルーティング テーブルに追加します。 エクステリア プロトコルの場合、network コマンドでアドバタイズするネットワークを制御します。インテリア プロトコルでは、network コマンドを使用して、アップデートの送信先を決定します。
ステップ 6	**show bgp all** **Example:** switch(config-router-af)# show bgp all	（任意）すべての BGP アドレス ファミリに関する情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** switch(config-router-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

BGP プロセスおよび関連するすべての設定を削除するには、**no router bgp** コマンドを使用します。

コマンド	目的
no router bgp *autonomous-system-number* **Example:** switch(config)# no router bgp 201	BGP プロセスおよび関連する設定を削除します。

次に、IPv4 ユニキャスト アドレス ファミリを指定して BGP をイネーブルに設定し、アドバタイズするネットワークを 1 つ追加する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# network 192.0.2.0
switch(config-router-af)# copy running-config startup-config
```

BGP インスタンスの再起動

BGP インスタンスを再起動し、そのインスタンスのすべてのピア セッションをクリアできます。

BGP インスタンスを再起動し、関連付けられたすべてのピアを削除するには、次のコマンドを使用します。

コマンド	目的
restart bgp instance-tag **Example:** switch(config)# restart bgp 201	BGP インスタンスを再起動し、すべてのピアリング セッションをリセットまたは再確立します。

BGP のシャットダウン

BGP プロトコルをシャットダウンして BGP を正常にディセーブルし、設定を保持できます。

BGP をシャットダウンするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
shutdown **Example:** `switch(config-router)# shutdown`	BGP を正常にシャットダウンします。

BGP ピアの設定

BGP プロセス内で BGP ピアを設定できます。BGP ピアごとに、関連付けられたキープアライブ タイマーとホールド タイマーがあります。これらのタイマーは、グローバルに設定することも、BGP ピアごとに設定することもできます。ピア設定はグローバル設定を上書きします。

（注） ピアごとに、ネイバー コンフィギュレーション モードでアドレス ファミリを設定する必要があります。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *ip-address* **remote-as** *as-number*
4. （任意）**description** *text*
5. （任意）**timers** *keepalive-time hold-time*
6. （任意）**shutdown**
7. **address-family ipv4** {**unicast** | **multicast**}
8. （任意）**show bgp ipv4** {**unicast** | **multicast**} **neighbors**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 64496 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#	リモート BGP ピアの IPv4 アドレスおよび AS 番号を設定します。*ip-address* の形式は x.x.x.x です。
ステップ 4	**description** *text* Example: switch(config-router-neighbor)# description Peer Router B switch(config-router-neighbor)#	（任意）ネイバーの説明を追加します。最大 80 文字の英数字ストリングを使用できます。
ステップ 5	**timers** *keepalive-time hold-time* Example: switch(config-router-neighbor)# timers 30 90	（任意）ネイバーのキープアライブおよびホールド タイムを表す BGP タイマー値を追加します。指定できる範囲は 0 ～ 3600 秒です。デフォルトは、キープアライブ タイムで 60 秒、ホールド タイムで 180 秒です。
ステップ 6	**shutdown** **Example:** switch(config-router-neighbor)# shutdown	（任意）この BGP ネイバーを管理目的でシャットダウンします。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 7	**address-family ipv4** {**unicast** | **multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	ユニキャスト IPv4 アドレス ファミリに対応するネイバー アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 8	**show bgp ipv4** {**unicast** | **multicast**} **neighbors** **Example:** switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors	（任意）GBP ピアの情報を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af) copy running-config startup-config	（任意）この設定の変更を保存します。

次に、BGP ピアを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1 remote-as 64497
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

プレフィクス ピアのダイナミック AS 番号の設定

BGP プロセス内で複数の BGP ピアを設定できます。BGP セッションの確立をルート マップの単一の AS 番号または複数の AS 番号に制限できます。

プレフィクス ピアのダイナミック AS 番号を使用して設定された BGP セッションでは、**ebgp-multihop** コマンドおよび **disable-connected-check** コマンドを無視します。

ルート マップの AS 番号のリストを変更できますが、ルート マップ名を変更するには **no neighbor** コマンドを使用する必要があります。設定されたルート マップの AS 番号に変更を加えた場合、新しいセッションのみに影響します。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *prefix* **remote-as route-map** *map-name*
4. （任意）**show bgp ipv4** {**unicast** | **multicast**} **neighbors**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 64496 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

	コマンド	目的

ステップ 3	**neighbor** *prefix* **remote-as route-map** *map-name*
	
	Example:
	`switch(config-router)# neighbor 192.0.2.0/8 remote-as routemap BGPPeers`
	`switch(config-router-neighbor)#`
		IPv4 プレフィクス、およびリモート BGP ピアの受け付けられた AS 番号のリストのルート マップを設定します。IPv4 の場合の *prefix* の形式は「x.x.x.x/ 長さ」です。長さの範囲は 1 ～ 32 です。
		
		map-name には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。

ステップ 4	**show bgp ipv4** {**unicast** | **multicast**} **neighbors** **Example:** `switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors`	（任意）GBP ピアの情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config-router-neighbor-af) copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、プレフィクス ピアのダイナミック AS 番号を設定する例を示します。

```
switch# configure terminal
switch(config)# route-map BGPPeers
switch(config-route-map)# match as-number 64496, 64501-64510
switch(config-route-map)# match as-number as-path-list List1, List2
switch(config-route-map)# exit
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.0/8 remote-as route-map BGPPeers
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

ルート マップについては、第 11 章「Route Policy Manager の設定」を参照してください。

BGP 情報のクリア

BGP 情報をクリアするには、次のコマンドを使用します。

コマンド	目的
clear bgp all {*neighbor* | ***** | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name*]	すべてのアドレス ファミリから 1 つ以上のネイバーをクリアします。***** は、すべてのアドレス ファミリのすべてのネイバーをクリアします。引数は次のとおりです。 • *neighbor*：ネイバーの IPv4 アドレス。 • *as-number*：AS 番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • *prefix*：IPv4 プレフィクス。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear bgp all dampening [**vrf** *vrf-name*]	すべてのアドレス ファミリのルート フラップ ダンプニング ネットワークをクリアします。*vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp all flap-statistics [**vrf** *vrf-name*]	すべてのアドレス ファミリのルート フラップ統計情報をクリアします。*vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp ip {**unicast** | **multicast**} **dampening** [**vrf** *vrf-name*]	選択したアドレス ファミリのルート フラップ ダンプニング ネットワークをクリアします。*vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear bgp ip {**unicast** | **multicast**} **flap-statistics** [**vrf** *vrf-name*]	選択したアドレス ファミリのルート フラップ統計情報をクリアします。*vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。

コマンド	目的
clear bgp ip {**unicast** | **multicast**} {*neighbor* | ***** | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name*]	選択したアドレス ファミリから 1 つ以上のネイバーをクリアします。***** は、アドレス ファミリのすべてのネイバーをクリアします。引数は次のとおりです。 • *neighbor*：ネイバーの IPv4 アドレス。 • *as-number*：AS 番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • *prefix*：IPv4 プレフィクス。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear ip bgp {**ip** {**unicast** | **multicast**}} {*neighbor* | ***** | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name*]	1 つ以上のネイバーをクリアします。***** は、アドレス ファミリのすべてのネイバーをクリアします。引数は次のとおりです。 • *neighbor*：ネイバーの IPv4 アドレス。 • *as-number*：AS 番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • *prefix*：IPv4 プレフィクス。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear ip bgp dampening [*ip-neighbor* | *ip-prefix*] [**vrf** *vrf-name*]	1 つ以上のネットワークのルート フラップ ダンプニングをクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*：IPv4。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

コマンド	目的
clear ip bgp flap-statistics [*ip-neighbor* | *ip-prefix*] [**vrf** *vrf-name*]	1 つ以上のネットワークのルート フラップ統計情報をクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*：IPv4。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear ip mbgp {**ip** {**unicast** | **multicast**}} {*neighbor* | ***** | *as-number* | **peer-template** *name* | *prefix*} [**vrf** *vrf-name*]	1 つ以上のネイバーをクリアします。***** は、アドレス ファミリのすべてのネイバーをクリアします。引数は次のとおりです。 • *neighbor*：ネイバーの IPv4 アドレス。 • *as-number*：AS 番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • *prefix*：IPv4 プレフィクス。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

コマンド	目的
clear ip mbgp dampening [*ip-neighbor* | *ip-prefix*] [**vrf** *vrf-name*]	1 つ以上のネットワークのルート フラップ ダンプニングをクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*：IPv4。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
clear ip mbgp flap-statistics [*ip-neighbor* | *ip-prefix*] [**vrf** *vrf-name*]	1 つ以上のネットワークのルート フラップ統計情報をクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*：IPv4。そのプレフィクス内のすべてのネイバーがクリアされます。 • *vrf-name*：VRF 名。その VRF 内のすべてのネイバーがクリアされます。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ベーシック BGP の設定確認

BGP の設定情報を表示するには、次の作業を行います。

コマンド	目的
show bgp all [**summary**] [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp convergence [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **community** {**regexp** ***expression*** | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]} [**vrf** *vrf-name*]	BGP コミュニティと一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] **ip** {**unicast** | **multicast**} [*ip-address*] **community-list** ***list-nam*e** [**vrf** *vrf-name*]	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **extcommunity** {**regexp** ***expression*** | **generic** [**non-transitive** | **transitive**] *aa4:nn* [**exact-match**]} [**vrf** *vrf-name*]	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **extcommunity-list** ***list-nam*e** [**exact-match**] [**vrf** *vrf-name*]	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。

コマンド	目的
show bgp ip {**unicast** | **multicast**} [*ip-address*] {**dampening dampened-paths** [**regexp** ***expression***]} [**vrf** *vrf-name*]	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、**clear bgp dampening** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **history-paths** [**regexp** ***expression***] [**vrf** *vrf-name*]	BGP ルート ヒストリ パスを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **filter-list** *list-name* [**vrf** *vrf-name*]	BGP フィルタ リストの情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **neighbors** [*ip-address*] [**vrf** *vrf-name*]	BGP ピアの情報を表示します。これらのネイバーを消去するには、**clear bgp neighbors** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] {**nexthop** | **nexthop-database**} [**vrf** *vrf-name*]	BGP ルート ネクストホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **policy** ***name*** [**vrf** *vrf-name*]	BGP ポリシー情報を表示します。ポリシー情報を消去するには、**clear bgp policy** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **prefix-list** *list-name* [**vrf** *vrf-name*]	プレフィクス リストと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **received-paths** [**vrf** *vrf-name*]	ソフト再構成用に保管されている BGP パスを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **regexp** *expression* [**vrf** *vrf-name*]	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **route-map** *map-name* [**vrf** *vrf-name*]	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy *name* [**vrf** *vrf-name*]	BGP ピア ポリシー情報を表示します。
show bgp peer-session ***name*** [**vrf** *vrf-name*]	BGP ピア セッション情報を表示します。
show bgp peer-template *name* [**vrf** *vrf-name*]	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、**clear bgp peer-template** コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。
show ip bgp *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。
show ip mbgp *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報の表示

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp ip {**unicast** | **multicast**} [*ip-address*] **flap-statistics** [**vrf** *vrf-name*]	BGP ルート フラップの統計情報を表示します。これらの統計情報を消去するには、**clear bgp flap-statistics** コマンドを使用します。
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

ベーシック BGP の設定例

次に、ベーシック BGP 設定の例を示します。

```
feature bgp
router bgp 64496
 neighbor 2001:ODB8:0:1::55 remote-as 64496
  address-family ipv4 unicast
    next-hop-self
```

関連資料

BGP の関連項目は、次のとおりです。

- 第 11 章「Route Policy Manager の設定」

次の作業

次の機能の詳細について、第 6 章「拡張 BGP の設定」を参照してください。

- ピア テンプレート
- ルートの再配布
- ルート マップ

その他の関連資料

BGP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.5-24）
- 「MIB」（P.5-24）

関連資料

関連項目	マニュアル名
BGP CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

MIB

管理情報ベース（MIB）	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

BGP 機能の履歴

表 5-3 は、この機能のリリースの履歴です。

表 5-3　BGP 機能の履歴

機能名	リリース	機能情報
BGP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 6

拡張 BGP の設定

この章では、Cisco NX-OS スイッチでボーダー ゲートウェイ プロトコル（BGP）の拡張機能を設定する方法について説明します。

この章では、次の内容について説明します。

拡張 BGP の概要

BGP は、組織または自律システム間のループフリー ルーティングを実現する、ドメイン間ルーティング プロトコルです。Cisco NX-OS は BGP バージョン 4 をサポートしています。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応スイッチ（BGP ピア）との間で TCP セッションを確立するために、信頼できるトランスポート プロトコルとして TCP を使用します。外部組織に接続するときには、ルータが外部 BGP（eBGP）ピアリング セッションを作成します。同じ組織内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

ここでは、次の内容について説明します。

ピア テンプレート

BGP ピア テンプレートを使用すると、共通のコンフィギュレーション ブロックを作成し、類似している BGP ピア間で再利用できます。各ブロックでは、ピアに継承させる一連の属性を定義できます。継承した属性の一部を上書きすることもできるので、非常に柔軟性のある方法で、繰り返しの多い BGP の設定を簡素化できます。

Cisco NX-OS は、3 種類のピア テンプレートを実装します。

- *peer-session* テンプレートでは、トランスポートの詳細、ピアのリモート AS 番号、セッション タイマーといった BGP セッション属性を定義します。peer-session テンプレートは、別の peer-session テンプレートから属性を継承することもできます（ローカル定義の属性によって、継承した peer-session 属性は上書きされます）。
- *peer-policy* テンプレートでは、着信ポリシー、発信ポリシー、フィルタ リスト、プレフィクス リストを含め、アドレス ファミリに依存する、ピアのポリシー要素を定義します。peer-policy テンプレートは、一連の peer-policy テンプレートからの継承が可能です。Cisco NX-OS は、継承設定のプリファレンス値で指定された順序で、これらの peer-policy テンプレートを評価します。最小値が大きい値よりも優先されます。
- *peer* テンプレートは、peer-session および peer-policy テンプレートからの継承が可能であり、ピアの定義を簡素化できます。peer テンプレートの使用は必須ではありませんが、peer テンプレートによって再利用可能なコンフィギュレーション ブロックが得られるので、BGP の設定を簡素化できます。

認証

BGP ネイバー セッションに認証を設定できます。この認証方式によって、ネイバーに送られる各 TCP セグメントに MD5 認証ダイジェストが追加され、不正なメッセージや TCP セキュリティ アタックから BGP が保護されます。

（注）　BGP ピア間で MD5 パスワードを一致させる必要があります。

ルート ポリシーおよび BGP セッションのリセット

BGP ピアにルート ポリシーを関連付けることができます。ルート ポリシーではルート マップを使用して、BGP が認識するルートを制御または変更します。着信または発信ルート アップデートに関するルート ポリシーを設定できます。ルート ポリシーはプレフィクス、AS_path 属性など、さまざまな条件で一致が必要であり、ルートを選択して受け付けるかまたは拒否します。ルート ポリシーでパス属性を変更することもできます。

BGP ピアに適用するルート ポリシーを変更する場合は、そのピアの BGP セッションをリセットする必要があります。Cisco NX-OS は、BGP ピアリング セッションのリセット方法として、次の 3 種類をサポートします。

- ハード リセット：ハード リセットでは、指定されたピアリング セッションが TCP 接続を含めて切断され、指定のピアからのルートが削除されます。このオプションを使用すると、BGP ネットワーク上のパケット フローが中断します。ハード リセットは、デフォルトでディセーブルです。
- ソフト再構成着信：ソフト再構成着信によって、セッションをリセットすることなく、指定されたピアのルーティング アップデートが開始されます。このオプションを使用できるのは、着信ルート ポリシーを変更する場合です。ソフト再構成着信の場合、ピアから受け取ったすべてのルートのコピーを保存したあとで、着信ルート ポリシーを介してルートが処理されます。着信ルート ポリシーをする場合、Cisco NX-OS は変更された着信ルート ポリシーを介して保存ルートを渡し、既存のピアリング セッションを切断することなく、ルート テーブルをアップデートします。ソフト再構成着信の場合、まだフィルタリングされていない BGP ルートの保存に、大量のメモリ リソースを使用する可能性があります。ソフト再構成着信は、デフォルトでディセーブルです。
- ルート リフレッシュ：ルート リフレッシュでは、着信ルート ポリシーの変更時に、サポートするピアにルート リフレッシュ要求を送信することによって、着信ルーティング テーブルがダイナミックにアップデートされます。リモート BGP ピアは新しいルート コピーで応答し、ローカル BGP スピーカが変更されたルート ポリシーでそれを処理します。Cisco NX-OS はピアに、プレフィクスの発信ルート リフレッシュを自動的に送信します。
- BGP ピアは、BGP ピア セッションの確立時に、BGP 機能ネゴシエーションの一部として、ルート リフレッシュ機能をアドバタイズします。ルート リフレッシュは優先オプションであり、デフォルトでイネーブルです。

（注）　BGP はさらに、ルート再配布、ルート集約、ルート ダンプニングなどの機能にルート マップを使用します。ルート マップの詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

eBGP

eBGP を使用すると、異なる AS からの BGP ピアを接続し、ルーティング アップデートを交換できます。外部ネットワークへの接続によって、自分のネットワークから他のネットワークへ、またインターネットを介して、トラフィックを転送できます。

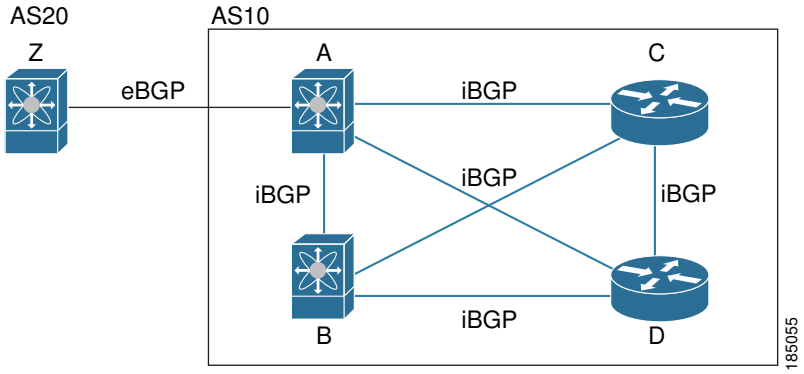
eBGP ピアリング セッションの確立には、ループバック インターフェイスを使用します。ループバック インターフェイスは、インターフェイス フラップが発生する可能性が小さいからです。インターフェイス *フラップ*が発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フェールオーバー、AS パス属性のサイズ制限については、「eBGP の設定」（P.6-23）を参照してください。

iBGP

iBGP を使用すると、同じ AS 内の BGP ピアを接続できます。iBGP はマルチホーム BGP ネットワーク（同じ外部 AS に対して複数の接続があるネットワーク）に使用できます。

図 6-1 に、大きい BGP ネットワークの中の iBGP ネットワークを示します。

図 6-1　iBGP ネットワーク



iBGP ネットワークはフルメッシュです。各 iBGP ピアは、ネットワーク ループを防止するために、他のすべての iBGP ピアに対して直接接続されています。

（注） iBGP ネットワークでは別個のインテリア ゲートウェイ プロトコルを設定する必要があります。

ここでは、次の内容について説明します。

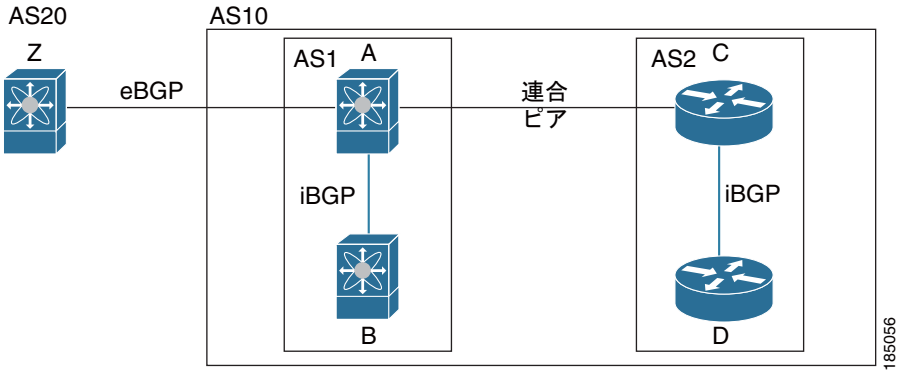
- 「AS 連合」（P.6-4）
- 「ルート リフレクタ」（P.6-5）

AS 連合

フルメッシュの iBGP ネットワークは、iBGP ピア数が増えるにしたがって複雑になります。AS を複数のサブ AS に分割し、それを 1 つの連合としてまとめることによって、iBGP メッシュを緩和できます。連合は、同じ AS 番号を使用して外部ネットワークと通信する、iBGP ピアからなるグループです。各サブ AS はその中ではフルメッシュであり、同じ連合内の他のサブ AS に対する少数の接続があります。

図 6-2 に、図 6-1 の BGP ネットワークを 2 つのサブ AS に分割し、1 つの連合にしたものを示します。

図 6-2　AS 連合



この例では、AS10 が 2 つの AS（AS1 および AS2）に分割されています。各サブ AS はフルメッシュですが、サブ AS 間のリンクは 1 つだけです。AS 連合を使用することによって、図 6-1 のフルメッシュ AS に比べて、リンク数を少なくできます。

ルート リフレクタ

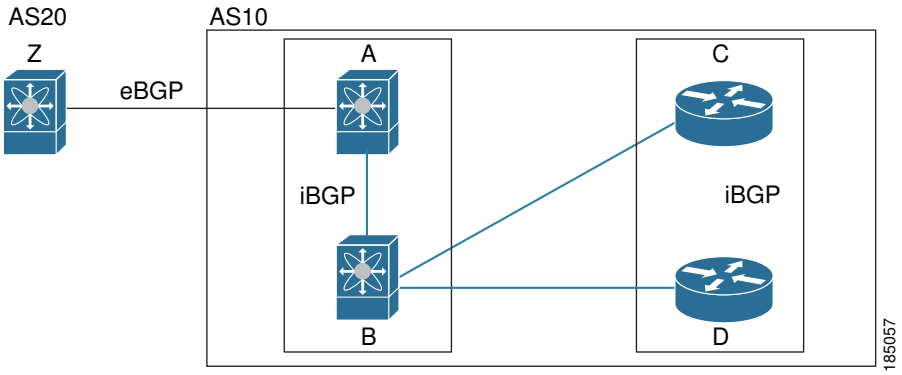
ルート リフレクタ構成を使用することによって、iBGP メッシュを緩和することもできます。ルート リフレクタは学習したルートをネイバーに渡すことで、すべての iBGP ピアをフルメッシュにしなくてもすむようにします。

図 6-1 に、メッシュの iBGP スピーカを 4 つ使用する（ルータ A、B、C、D）、単純な iBGP 構成を示します。ルート リフレクタを使用しなかった場合、外部ネイバーからルートを受け取ったルータ A は、3 つの iBGP ネイバーのすべてにルートをアドバタイズします。

ある iBGP ピアをルート リフレクタとして設定すると、そのピアが iBGP で学習したルートを一連の iBGP ネイバーに渡す役割を担います。

図 6-3 では、ルータ B がルート リフレクタです。ルータ A からアドバタイズされたルートを受信したルート リフレクタは、そのルートをルータ C および D にアドバタイズ（リフレクション）します。ルータ A からルータ C および D の両方にアドバタイズする必要がなくなります。

図 6-3　ルート リフレクタ



ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。ルート リフレクタのクライアント ピアとして動作するように、すべての iBGP ピアを設定する必要はありません。ただし、完全な BGP アップデートがすべてのピアに届くように、非クライアント ピアはフルメッシュとして設定する必要があります。

機能ネゴシエーション

BGP スピーカは機能ネゴシエーション機能を使用することによって、ピアがサポートする BGP 拡張機能について学習できます。機能ネゴシエーションによって、リンクの両側の BGP ピアがサポートする機能セットだけを BGP に使用させることができます。

BGP ピアが機能ネゴシエーションをサポートしない場合で、なおかつアドレス ファミリが IPv4 として設定されている場合、Cisco NX-OS は機能ネゴシエーションを行わずに、ピアとの新規セッションを試みます。

ルート ダンプニング

ルート ダンプニングは、インターネットワーク上でのフラッピング ルートの伝播を最小限に抑える BGP 機能です。ルート フラップが発生するのは、使用可能ステートと使用不能ステートが短時間で次々切り替わる場合です。

AS1、AS2、および AS3 という 3 つの BGP AS からなるネットワークの場合について考えてみます。AS1 のルートがフラップした（使用不能になった）とします。ルート ダンプニングを使用しない場合、AS1 は AS2 に回収メッセージを送信します。AS2 は AS3 にその回収メッセージを伝達します。フラッピング ルートが再び発生すると、AS1 から AS2 にアドバタイズメント メッセージを送信し、AS2 は AS3 にそのアドバタイズメントを送信します。ルートの使用不能と使用可能が繰り返されると、AS1 は多数の回収メッセージおよびアドバタイズメント メッセージを送信することになり、それが他の AS に伝播します。

ルート ダンプニングによって、フラッピングを最小限に抑えることができます。ルート フラップが発生したとします。（ルート ダンプニングがイネーブルの）AS2 がルートにペナルティとして 1000 を割り当てます。AS2 は引き続き、ネイバーにルートの状態をアドバタイズします。ルート フラップが発生するたびに、AS2 がペナルティ値を追加します。ルート フラップが頻繁に発生して、ペナルティが設定可能な抑制限度を超えると、AS2 はフラップ回数に関係なく、ルートのアドバタイズを中止します。その結果、ルートが減衰（ダンプニング）します。

ルートに与えられたペナルティは、再使用限度に達するまで減衰します。その時点で、AS2 は再びルートをアドバタイズします。再使用限度が 50% になると、AS2 はそのルートのダンプニング情報を削除します。

（注） ルート ダンプニングがイネーブルの場合は、ピアのリセットによってルートが回収されても、リセット中の BGP にはペナルティは適用されません。

ロード シェアリングおよびマルチパス

BGP はルーティング テーブルに、同じ宛先プレフィクスに到達する複数の等コスト eBGP または iBGP パスを組み込むことができます。その場合、宛先プレフィクスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

BGP ベストパス アルゴリズムでは、次の属性が同じ場合に、等コスト パスと見なされます。

- 重量

- ローカル プリファレンス
- AS_path
- オリジン コード
- multi-exit discriminator（MED）
- BGP ネクストホップまでの IGP コスト

BGP はこれら複数のパスの中から、ベスト パスとして 1 つだけ選択し、そのパスを BGP ピアにアドバタイズします。

（注）　異なる AS 連合から受け取ったパスは、外部 AS_path 値およびその他の属性が同じ場合に、等コストパスと見なされます。

（注）　iBGP マルチパスに関してルート リフレクタを設定すると、ルート リフレクタが、選択されたベストパスをピアにアドバタイズします。そのパスのネクストホップは変更されません。

ルート集約

集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 という固有性の強い 3 つのアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

アドバタイズするルートが少なくなるように、BGP ルート テーブルでは集約プレフィクスを使用します。

（注）　Cisco NX-OS は、自動ルート集約をサポートしません。

ルート集約はフォワーディング ループにつながる可能性があります。この問題を回避するために、集約アドレスのアドバタイズメントを生成するときに、BGP はローカル ルーティング テーブルに、その集約アドレスに対応するサマリー廃棄ルートを自動的に組み込みます。BGP はサマリー廃棄のアドミニストレーティブ ディスタンスを 220 に設定し、ルート タイプを廃棄に設定します。BGP はネクストホップ解決に廃棄ルートを使用しません。

BGP 条件付きアドバタイズメント

BGP 条件付きアドバタイズメントを使用すると、プレフィクスが BGP テーブルに存在するかどうかに基づいてルートをアドバタイズまたは撤回するように BGP を設定できます。この機能は、たとえば、BGP でいずれかのプロバイダーにプレフィクスをアドバタイズするようなマルチホーム ネットワーク（他のプロバイダーからの情報が存在しない場合のみ）で便利です。

AS1、AS2、および AS3 という 3 つの BGP AS からなるネットワークの例について考えてみます。この例で、AS1 と AS3 はインターネットと AS2 に接続しています。条件付きアドバタイズメントを使用しない場合、AS2 はすべてのルートを AS1 と AS3 の両方にプロパゲートします。条件付きアドバタイズメントを使用すれば、AS1 からのルートが存在しない場合のみ（たとえば AS1 へのリンクがダウンした場合）、特定のルートを AS3 にアドバタイズするように AS2 を設定できます。

BGP 条件付きアドバタイズメントでは、設定されたルート マップに一致する各ルートに、存在テストまたは非存在テストが追加されます。詳細については、「BGP 条件付きアドバタイズメントの設定」（P.6-29）を参照してください。

BGP ネクストホップ アドレス トラッキング

BGP は、インストールされているルートのネクストホップ アドレスをモニタして、ネクストホップの到達可能性の確認、および BGP ベスト パスの選択、インストール、検証を行います。BGP ネクストホップ アドレスのトラッキングを行うと、ネクストホップの到達可能性に影響を及ぼす可能性のあるルート変更が RIB で行われたときに確認プロセスをトリガーすることで、このようなネクストホップ到達可能性テストの速度が向上します。

ネクストホップ情報が変更されると、BGP は RIB から通知を受信します（イベント駆動型の通知）。BGP は、次のいずれかのイベントが発生したときに通知を受けます。

- ネクストホップが到達不能になった。
- ネクストホップが到達可能になった。
- ネクストホップへの完全な繰り返し IGP メトリックが変更される。
- ファースト ホップの IP アドレスまたはファースト ホップのインターフェイスが変更される。
- ネクストホップが接続された。
- ネクストホップが接続解除された。
- ネクストホップがローカル アドレスになった。
- ネクストホップが非ローカル アドレスになった。

（注）　到達可能性および繰り返しメトリック イベントは、ベスト パスの再計算をトリガーします。

RIB からのイベント通知は、クリティカルおよび非クリティカルとして分類されます。クリティカルおよび非クリティカル イベントの通知は、別々のバッチで送信されます。ただし、非クリティカル イベントが保留中であり、クリティカル イベントを読み込む要求がある場合は、非クリティカル イベントがクリティカル イベントとともに送信されます。

- クリティカル イベントは、ネクストホップの到達可能性（到達可能と到達不能）、接続性（接続と非接続）、および局在性（ローカルと非ローカル）に関係があります。これらのイベントの通知は遅延しません。
- 非クリティカル イベントには、IGP メトリックの変更のみが含まれます。

詳細については、「BGP ネクストホップ アドレス トラッキングの設定」（P.6-21）を参照してください。

ルートの再配布

スタティック ルートまたは他のプロトコルからのルートを再配布するように、BGP を設定できます。再配布を指定してルート ポリシーを設定し、BGP に渡されるルートを制御します。ルート ポリシーを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

BGP の調整

BGP タイマーによって、さらにベストパス アルゴリズムの調整によって、BGP のデフォルト動作を変更できます。

ここでは、次の内容について説明します。

BGP タイマー

BGP では、ネイバー セッションおよびグローバル プロトコル イベントにさまざまなタイプのタイマーを使用します。確立されたセッションごとに、最低限 2 つのタイマーがあります。定期的にキープアライブ メッセージを送信するためのタイマー、さらに想定時間内にピアのキープアライブが届かなかった場合に、セッションをタイムアウトさせるためのタイマーです。また、個々の機能を処理するための、その他のタイマーがあります。これらのタイマーは通常、秒単位で設定します。タイマーには、異なる BGP ピアで同じタイマーが異なるタイミングでスタートするように、ランダム アジャストメントが組み込まれています。

ベストパス アルゴリズムの調整

オプションの設定パラメータによって、ベストパス アルゴリズムのデフォルト動作を変更できます。たとえば、アルゴリズムでの MED 属性およびルータ ID の扱い方を変更できます。

マルチプロトコル BGP

Cisco NX-OS の BGP は、複数のアドレス ファミリをサポートします。マルチプロトコル BGP（MP-BGP）は、アドレス ファミリに応じて異なるルート セットを伝送します。たとえば、BGP は IPv4 ユニキャスト ルーティングのルート 1 セットと IPv4 マルチキャスト ルーティングのルート 1 セットを伝送します。IP マルチキャスト ネットワークでは Reverse Path Forwarding（RPF; リバースパス フォワーディング）のチェックに MP-BGP を使用できます。

（注）　マルチキャスト BGP ではマルチキャスト状態情報をプロパゲートしないため、Protocol Independent Multicast（PIM; プロトコル独立マルチキャスト）などのマルチキャスト プロトコルが必要です。

マルチプロトコル BGP 設定をサポートするには、ルータ アドレスファミリおよびネイバー アドレス ファミリの各コンフィギュレーション モードを使用します。MP-BGP では、設定されたアドレス ファミリごとに別々の RIB が維持されます（ユニキャスト RIB と、BGP のマルチキャスト RIB など）。

マルチプロトコル BGP ネットワークは下位互換性がありますが、マルチプロトコル拡張機能をサポートしない BGP ピアは、アドレス ファミリ ID 情報など、マルチプロトコル拡張機能が伝送するルーティング情報を転送できません。

仮想化のサポート

Cisco NX-OS は、同一システム上で動作する複数の BGP インスタンスをサポートします。BGP は Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスをサポートします。

デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。第 9 章「レイヤ 3 仮想化の設定」を参照してください。

拡張 BGP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	BGP には、LAN Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、*『Cisco NX-OS Licensing Guide』を参照してください。* **（注）** レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP 機能をイネーブルにする必要があります（「BGP 機能のイネーブル化」（P.5-11）を参照）。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。
- ネイバー関係を作成しようとするピアに到達可能でなければなりません（Interior Gateway Protocol（IGP）、スタティック ルート、直接接続など）。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを明示的に設定する必要があります。

BGP に関する注意事項および制限事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- ダイナミック AS 番号プレフィクス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。
- AS 連合でプレフィクス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィクス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ Time-to-Live（TTL; 存続可能時間）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィクス設定オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。
- update-source を設定し、eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ルート マップを指定します。

- VRF 内で BGP ルータ ID を設定します。
- キープアライブおよびホールド タイマーの値を小さくすると、ネットワークでセッション フラップが発生する可能性があります。

デフォルト設定

表 6-1 に、BGP パラメータのデフォルト設定を示します。

表 6-1　デフォルトの BGP パラメータ

パラメータ	デフォルト
BGP 機能	ディセーブル
キープアライブ インターバル	60 秒
ホールド タイマー	180 秒

拡張 BGP の設定

ここでは、拡張 BGP の設定方法について説明します。内容は次のとおりです。

- 「BGP の調整」（P.6-34）
- 「仮想化の設定」（P.6-37）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

BGP セッション テンプレートの設定

BGP セッション テンプレートを使用すると、類似した設定が必要な複数の BGP ピアで、BGP の設定を簡素化できます。BGP テンプレートによって、共通のコンフィギュレーション ブロックを再利用できます。先に BGP テンプレートを設定し、そのあとで BGP ピアにテンプレートを適用します。

BGP セッション テンプレートでは、継承、パスワード、タイマー、セキュリティなどのセッション属性を設定できます。

peer-session テンプレートは、別の peer-session テンプレートからの継承が可能です。第 3 のテンプレートから継承するように第 2 テンプレートを設定できます。さらに最初のテンプレートもこの第 3 のテンプレートから継承させることができます。この間接継承を続けることができる peer-session テンプレートの数は、最大 7 つです。

ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

（注）　テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、**default** 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer-session** *template-name*
4. **password** *number password*
5. **timers** *keepalive* ***hold***
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **inherit peer-session** *template-name*
9. （任意）**description** *text*
10. （任意）**show bgp peer-session** *template-name*
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**template peer-session** *template-name* **Example:** switch(config-router)# template peer-session BaseSession switch(config-router-stmp)#	peer-session テンプレート 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	**password** *number password* **Example:** switch(config-router-stmp)# password 0 test	（任意）ネイバーにクリアテキスト パスワード *test* を追加します。パスワードは 3DES（タイプ 3 暗号形式）で保存および表示されます。
ステップ 5	**timers** *keepalive hold* **Example:** switch(config-router-stmp)# timers 30 90	（任意）peer-session テンプレートに BGP キープアライブおよびホールド タイマー値を追加します。 デフォルトのキープアライブ インターバルは 60 です。デフォルトのホールド タイムは 180 です。
ステップ 6	**exit** **Example:** switch(config-router-stmp)# exit switch(config-router)#	peer-session テンプレート コンフィギュレーション モードを終了します。
ステップ 7	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

ステップ 8	**inherit peer-session** *template-name*
	
	Example:
	switch(config-router-neighbor)# inherit peer-session BaseSession
	switch(config-router-neighbor)
		ピアに peer-session テンプレートを適用します。

ステップ 9	**description** *text*
	
	Example:
	switch(config-router-neighbor)# description Peer Router A
	switch(config-router-neighbor)
		（任意）ネイバーの説明を追加します。

	コマンド	目的
ステップ 10	**show bgp peer-session** *template-name* **Example:** switch(config-router-neighbor)# show bgp peer-session BaseSession	（任意）peer-policy テンプレートを表示します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config-router-neighbor)# copy running-config startup-config	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BaseSession
switch(config-router-stmp)# timers 30 90
switch(config-router-stmp)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# description Peer Router A
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# copy running-config startup-config
```

BGP peer-policy テンプレートの設定

peer-policy テンプレートを設定すると、特定のアドレス ファミリに対応する属性を定義できます。各 peer-policy テンプレートにプリファレンスを割り当て、指定した順序でテンプレートが継承されるようにします。ネイバー アドレス ファミリでは最大 5 つの peer-policy テンプレートを使用できます。

Cisco NX-OS は、プリファレンス値を使用して、アドレス ファミリの複数のピア ポリシーを評価します。プリファレンス値が最小のものが最初に評価されます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

peer-policy テンプレートでは、AS-path フィルタ リスト、プレフィクス リスト、ルート リフレクション、ソフト再構成など、アドレス ファミリ固有の属性を設定できます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

（注） テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**

2. **router bgp** *autonomous-system-number*
3. **template peer-policy** *template-name*
4. **advertise-active-only**
5. **maximum-prefix** *number*
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **address-family ipv4 {multicast | unicast}**
9. **inherit peer-policy** *template-name preference*
10.（任意）**show bgp peer-policy** *template-name*
11.（任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP をイネーブルにして、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**template peer-policy** *template-name* **Example:** switch(config-router)# template peer-policy BasePolicy switch(config-router-ptmp)#	peer-policy テンプレートを作成します。
ステップ 4	**advertise-active-only** **Example:** switch(config-router-ptmp)# advertise-active-only	（任意）アクティブ ルートだけをピアにアドバタイズします。
ステップ 5	**maximum-prefix** *number* **Example:** switch(config-router-ptmp)# maximum-prefix 20	（任意）このピアに認めるプレフィクスの最大数を設定します。
ステップ 6	**exit** **Example:** switch(config-router-ptmp)# exit switch(config-router)#	peer-policy テンプレート コンフィギュレーション モードを終了します。
ステップ 7	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

	コマンド	目的
ステップ 8	**address-family ipv4** {**multicast** | **unicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	IPv4 アドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 9	**inherit peer-policy** *template-name preference* **Example:** switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1	ピア アドレス ファミリ設定に peer-policy テンプレートを適用し、このピア ポリシーのプリファレンス値を割り当てます。
ステップ 10	**show bgp peer-policy** *template-name* **Example:** switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy	（任意）peer-policy テンプレートを表示します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

BGP peer-policy テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BasePolicy
switch(config-router-ptmp)# maximum-prefix 20
switch(config-router-ptmp)# exit
switch(config-router)# neighbor 192.168.1.1 remote-as 65536
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP peer テンプレートの設定

BGP peer テンプレートを設定すると、1 つの再利用可能なコンフィギュレーション ブロックで、セッション属性とポリシー属性を結合することができます。peer テンプレートも、peer-session または peer-policy テンプレートを継承できます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。ネイバーに設定できる peer テンプレートは 1 つだけですが、peer テンプレートは peer-session および peer-policy テンプレートを継承できます。

peer テンプレートは、eBGP マルチホップ TTL、最大プレフィクス数、ネクストホップ セルフ、タイマーなど、セッション属性およびアドレス ファミリ属性をサポートします。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

（注）　テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer** *template-name*
4. （任意）**inherit peer-session** *template-name*
5. （任意）**address-family ipv4** {**multicast** | **unicast**}
6. （任意）**inherit peer** *template-name*
7. **exit**
8. （任意）**timers** *keepalive hold*
9. **exit**
10. **neighbor** *ip-address*
11. **inherit peer** *template-name*
12. （任意）**timers** *keepalive hold*
13. （任意）**show bgp peer-template** *template-name*
14. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **Example:** switch(config)# router bgp 65536	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**template peer** *template-name* **Example:** switch(config-router)# template peer BasePeer switch(config-router-neighbor)#	peer テンプレート コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**inherit peer-session***n template-name* **Example:** switch(config-router-neighbor)# inherit peer-session BaseSession	（任意）peer テンプレートで peer-session テンプレートを継承します。
ステップ 5	**address-family ipv4**{**multicast** | **unicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	（任意）IPv4 アドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを設定します。
ステップ 6	**inherit peer** *template-name* **Example:** switch(config-router-neighbor-af)# inherit peer BasePolicy	（任意）ネイバー アドレス ファミリ設定に peer テンプレートを適用します。
ステップ 7	**exit** **Example:** switch(config-router-neighbor-af)# exit switch(config-router-neighbor)#	BGP ネイバー アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 8	**timers** *keepalive hold* **Example:** switch(config-router-neighbor)# timers 45 100	（任意）ピアに BGP タイマー値を追加します。 これらの値によって、peer-session テンプレート、BaseSession のタイマー値が上書きされます。
ステップ 9	**exit** **Example:** switch(config-router-neighbor)# exit switch(config-router)#	BGP peer テンプレート コンフィギュレーション モードを終了します。
ステップ 10	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 11	**inherit peer** *template-name* **Example:** switch(config-router-neighbor)# inherit peer BasePeer	peer テンプレートを継承します。
ステップ 12	**timers** *keepalive hold* **Example:** switch(config-router-neighbor)# timers 60 120	（任意）このネイバーに BGP タイマー値を追加します。 これらの値によって、peer テンプレートおよび peer-session テンプレートのタイマー値が上書きされます。

	コマンド	目的
ステップ 13	**show bgp peer-template** *template-name* **Example:** switch(config-router-neighbor-af)# show bgp peer-template BasePeer	（任意）peer テンプレートを表示します。
ステップ 14	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

適用されたテンプレートを確認するには、**show bgp neighbor** コマンドを使用します。テンプレートで使用できるあらゆるコマンドの詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。

BGP peer テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer BasePeer
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

プレフィクス ピアリングの設定

BGP では IPv4 の両方のプレフィクスを使用して、ピア セットを定義できます。この機能を使用すると、各ネイバーを設定に追加する必要がありません。

プレフィクス ピアリングを定義する場合は、プレフィクスとともにリモート AS 番号を指定する必要があります。プレフィクス ピアリングが設定されている許容最大ピア数を超えない場合、BGP はプレフィクスおよび AS から接続するピアを受け付けます。

プレフィクス ピアリングに含まれている BGP ピアが切断されると、Cisco NX-OS は定義されているプレフィクス ピア タイムアウト値まで、ピア構造を維持します。この場合、そのプレフィクス ピアリングのすべてのスロットを他のピアが使い果たした結果、ブロックされるという危険性を伴わずに、確立されたピアのリセットまたは再接続が可能になります。

BGP プレフィクス ピアリング タイムアウト値を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
timers prefix-peer-timeout *value* **Example:** switch(config-router-neighbor)# timers prefix-peer-timeout 120	プレフィクス ピアリングのタイムアウト値を設定します。指定できる範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。

ピアの最大数を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-peers *value* **Example:** switch(config-router-neighbor)# maximum-peers 120	このプレフィクス ピアリングの最大ピア数を設定します。指定できる範囲は 1 ～ 1000 です。

最大 10 のピアを受け付けるプレフィクス ピアリングの設定例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 65536
switch(config-router-neighbor)# maximum-peers 10
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

所定のプレフィクス ピアリングの設定の詳細とともに、現在受け付けられているインスタンスのリスト、アクティブ ピア数、最大同時ピア数、および受け付けたピアの合計数を表示するには、**show ip bgp neighbor** コマンドを使用します。

BGP 認証の設定

MD5 ダイジェストを使用して、ピアからのルート アップデートを認証するように BGP を設定できます。

MD5 認証を使用するように BGP を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
password [**0** | **3** | **7**] *string* **Example:** switch(config-router-neighbor)# password BGPpassword	MGP ネイバー セッションの MD5 パスワードを設定します。

BGP セッションのリセット

BGP のルート ポリシーを変更した場合は、関連付けられた BGP ピア セッションをリセットする必要があります。BGP ピアがルート リフレッシュをサポートしない場合は、着信ポリシー変更に関するソフト再構成を設定できます。Cisco NX-OS は自動的に、セッションのソフト リセットを試みます。

ソフト再構成着信を設定するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
soft-reconfiguration inbound **Example:** switch(config-router-neighbor-af)# soft-reconfiguration inbound	着信 BGP ルート アップデートを格納するために、ソフト再構成をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

BGP ネイバー セッションをリセットするには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear bgp ip {**unicast** | **multicast**} *ip-address* **soft** {**in** | **out**} **Example:** switch# clear bgp ip unicast 192.0.2.1 soft in	TCP セッションを切断しないで、BGP セッションをリセットします。

ネクストホップ アドレスの変更

次の方法で、ルート アドバタイズメントで使用するネクストホップ アドレスを変更できます。

- ネクストホップ計算をディセーブルにして、ローカル BGP スピーカ アドレスをネクストホップ アドレスとして使用します。
- ネクストホップ アドレスをサードパーティ アドレスとして設定します。この機能は、元のネクストホップ アドレスがルートの送り先のピアと同じサブネット上にある場合に使用します。この機能を使用すると、フォワーディング時に余分なホップを節約できます。

ネクストホップ アドレスを変更するには、コマンド アドレス ファミリ コンフィギュレーション モードで次のパラメータを使用します。

コマンド	目的
next-hop-self **Example:** switch(config-router-neighbor-af)# next-hop-self	ルート アップデートのネクストホップ アドレスとして、ローカル BGP スピーカ アドレスを使用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
next-hop-third-party **Example:** switch(config-router-neighbor-af)# next-hop-third-party	ネクストホップ アドレスをサードパーティ アドレスとして設定します。このコマンドは、**next-hop-self** を設定されていないシングルホップ EBGP ピアに使用します。

BGP ネクストホップ アドレス トラッキングの設定

BGP ネクストホップ アドレス トラッキングはデフォルトでイネーブルであり、ディセーブルにすることができません。

BGP ネクストホップ トラッキングのパフォーマンスを向上するために、RIB チェック間の遅延インターバルを変更できます。BGP ネクストホップの到達可能性に影響を及ぼすルートのクリティカル タイマーを設定したり、BGP テーブルのその他のルートすべての非クリティカル タイマーを設定したりできます。

BGP ネクストホップ アドレス トラッキングを変更するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
nexthop trigger-delay {**critical** | **non-critical**} *milliseconds* **Example:** switch(config-router-af)# nexthop trigger-delay critical 5000	クリティカルなネクストホップの到達可能性ルートおよび非クリティカルなルートについて、ネクストホップ アドレス トラッキングの遅延タイマーを指定します。指定できる範囲は 1 ～ 4294967295 ミリ秒です。クリティカル タイマーのデフォルトは 3000 です。非クリティカル タイマーのデフォルトは 10000 です。
nexthop route-map *name* **Example:** switch(config-router-af)# nexthop route-map nextHopLimits	BGP ネクストホップ アドレスが一致するルートマップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ネクストホップ フィルタリングの設定

BGP ネクストホップ フィルタリングを使用すると、RIB でネクストホップ アドレスがチェックされるときにそのネクストホップ アドレスの基盤となるルートがルート マップを経由します。ルート マップでそのルートが拒否されると、ネクストホップ アドレスは到達不能として扱われます。

BGP は、ルート ポリシーによって拒否されたすべてのネクストホップを無効であるとマークし、無効なネクストホップ アドレスを使用するルートについてベスト パスを計算しません。

BGP ネクストホップ フィルタリングを設定するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
nexthop route-map *name* **Example:** switch(config-router-af)# nexthop route-map nextHopLimits	BGP ネクストホップ ルートが一致するルートマップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

機能ネゴシエーションのディセーブル化

機能ネゴシエーションをディセーブルにすると、機能ネゴシエーションをサポートしない古い BGP ピアとの相互運用が可能です。

機能ネゴシエーションをディセーブルにするには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dont-capability-negotiate **Example:** switch(config-router-neighbor)# dont-capability-negotiate	機能ネゴシエーションをディセーブルにします。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

eBGP の設定

ここでは、次の内容について説明します。

eBGP シングルホップ チェックのディセーブル化

シングルホップ eBGP ピアがローカル ルータに直接接続されているかどうかのチェック機能をディセーブルにするように、eBGP を設定できます。このオプションは、直接接続されたスイッチ間のシングルホップ ループバック eBGP セッションの設定に使用します。

シングルホップ eBGP ピアが直接接続されているかどうかのチェックをディセーブルにするには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
disable-connected-check **Example:** `switch(config-router-neighbor)# disable-connected-check`	シングルホップ eBGP ピアが直接接続されているかどうかのチェックをディセーブルにします。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

eBGP マルチホップの設定

eBGP マルチホップをサポートする eBGP TTL（存続可能時間）値を設定できます。eBGP ピアは状況によって、別の eBGP ピアに直接接続されず、リモート eBGP ピアに到達するために複数のホップを必要とします。ネイバー セッションに eBGP TTL 値を設定すると、このようなマルチホップ セッションが可能になります。

eBGP マルチホップを設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ebgp-multihop *ttl-value* **Example:** `switch(config-router-neighbor)# ebgp-multihop 5`	eBGP マルチホップの eBGP TTL を設定します。指定できる範囲は 2 ～ 255 です。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

高速外部フェールオーバーのディセーブル化

通常、BGP ルータと直接接続 eBGP ピア間の接続が失われると、ピアとの eBGP セッションをリセットすることによって、BGP が高速外部フェールオーバーを開始します。この高速外部フェールオーバーをディセーブルにすると、リンク フラップが原因の不安定さを制限できます。

高速外部フェールオーバーをディセーブルにするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no fast-external-failover **Example:** switch(config-router)# no fast-external-failover	eBGP ピアの高速外部フェールオーバーをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

AS パス属性の制限

AS パス属性で AS 番号が高いルートを廃棄するように eBGP を設定できます。

AS パス属性で AS 番号が高いルートを廃棄するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maxas-limit *number* **Example:** switch(config-router)# maxas-limit 50	AS パス セグメントの番号が指定された上限を超えている eBGP ルートを廃棄します。指定できる範囲は 1 ～ 2000 です。

AS 連合の設定

AS 連合を設定するには、連合識別情報を指定する必要があります。AS 連合内の AS グループは、AS 番号として連合 ID を持つ、1 つの AS として外部で認識されます。

BGP 連合 ID を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
confederation identifier *as-number* **Example:** switch(config-router)# confederation identifier 4000	AS 連合を表す連合 ID を設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

AS 連合に所属する AS を設定するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
bgp confederation peers *as-number* [*as-number2...*] **Example:** switch(config-router)# bgp confederation peers 5 33 44	連合に所属する AS のリストを指定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

ルート リフレクタの設定

ルート リフレクタとして動作するローカル BGP スピーカに対するルート リフレクタ クライアントとして、iBGP ピアを設定できます。ルート リフレクタとそのクライアントがともにクラスタを形成します。クライアントからなるクラスタには通常、ルート リフレクタが 1 つ存在します。このような状況では、ルート リフレクタのルータ ID でクラスタを識別します。ネットワークの冗長性を高め、シングル ポイント障害を回避するために、複数のルート リフレクタからなるクラスタを設定できます。クラスタ内のすべてのルート リフレクタは、同じ 4 バイト クラスタ ID で設定する必要があります。これは、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるようにするためです。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **cluster-id** *cluster-id*
4. **address-family ipv4** {**unicast** | **multicast**}
5. （任意）**client-to-client reflection**
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **address-family ipv4** {**unicast** | **multicast**}
9. **route-reflector-client**
10. **show bgp ip** {**unicast** | **multicast**} **neighbors**
11. （任意）**copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *as-number*
	
	Example:
	`switch(config)# router bgp 65536`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。

ステップ 3	**cluster-id** *cluster-id* **Example:** `switch(config-router)# cluster-id 192.0.2.1`	クラスタに対応するルート リフレクタの 1 つとして、ローカル ルータを設定します。クラスタを識別するクラスタ ID を指定します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv4** {**unicast** | **multicast**} **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	指定のアドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**client-to-client reflection** **Example:** switch(config-router-af)# client-to-client reflection	（任意）クライアント間のルート リフレクションを設定します。この機能は、デフォルトでイネーブルにされています。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 6	**exit** **Example:** switch(config-router-neighbor)# exit switch(config-router)#	ルータ アドレス コンフィギュレーション モードを終了します。
ステップ 7	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.0.2.10 remote-as 65536 switch(config-router-neighbor)#	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。
ステップ 8	**address-family ipv4** {**unicast** | **multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	ユニキャスト IPv4 アドレス ファミリに対応するネイバー アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 9	**route-reflector-client** **Example:** switch(config-router-neighbor-af)# route-reflector-client	BGP ルート リフレクタとしてスイッチを設定し、そのクライアントとしてネイバーを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 10	**show bgp ip** {**unicast** | **multicast**} **neighbors** **Example:** switch(config-router-neighbor-af)# show bgp ip unicast neighbors	（任意）BGP ピアを表示します。
ステップ 11	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ルート リフレクタとしてルータを設定し、クライアントとしてネイバーを 1 つ追加する例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.10 remote-as 65536
switch(config-router-neighbor)# address-family ip unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# copy running-config startup-config
```

ルート ダンプニングの設定

iBGP ネットワーク上でのルート フラップの伝播を最小限に抑えるために、ルート ダンプニングを設定できます。

ルート ダンプニングを設定するには、アドレス ファミリまたは VRF アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dampening [{*half-life reuse-limit suppress-limit max-suppress-time* | **route-map** *map-name*}] **Example:** `switch(config-router-af)# dampening route-map bgpDamp`	機能ネゴシエーションをディセーブルにします。パラメータ値は次のとおりです。 • half-life：指定できる範囲は 1 ～ 45 です。 • reuse-limit：指定できる範囲は 1 ～ 20000 です。 • suppress-limit：指定できる範囲は 1 ～ 20000 です。 • max-suppress-time：指定できる範囲は 1 ～ 255 です。

ロード シェアリングおよび ECMP の設定

等コスト マルチパス ロード バランシング用に BGP がルート テーブルに追加するパスの最大数を設定できます。

パスの最大数を設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-paths [**ibgp**] *maxpaths* **Example:** `switch(config-router-af)# maximum-paths 12`	ロード シェアリング用の等コスト パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルトは 8 です。

最大プレフィクス数の設定

BGP が BGP ピアから受け取ることのできるプレフィクスの最大数を設定できます。任意で、プレフィクス数がこの値を超えた場合に、BGP に警告メッセージを生成させる、またはピアとの BGP セッションを切断させることを設定できます。

BPG ピアに認めるプレフィクスの最大数を設定するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
maximum-prefix *maximum* [*threshold*] [**restart** *time* | **warming-only**] **Example:** `switch(config-router-neighbor-af)# maximum-prefix 12`	ピアからのプレフィクスの最大数を設定します。パラメータの範囲は次のとおりです。 • *maximum*：指定できる範囲は 1 ～ 300000 です。 • *threshold*：指定できる範囲は 1 ～ 100% です。デフォルトは 75% です。 • *time*：指定できる範囲は 1 ～ 65535 分です。 このコマンドによって、プレフィクス限度を超えた場合に、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

ダイナミック機能の設定

BGP ピアのダイナミック機能を設定できます。

ダイナミック機能を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
dynamic-capability **Example:** `switch(config-router-neighbor)# dynamic-capability`	ダイナミック機能をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。 このコマンドは、デフォルトではディセーブルです。

集約アドレスの設定

BGP ルート テーブルの集約アドレス エントリを設定できます。

集約アドレスを設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
aggregate-address *ip-prefix/length* [**as-set**] [**summary-only**] [**advertise-map** *map-name*] [**attribute-map** *map-name*] [*suppress*-**map** *map-name*] **Example:** `switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set`	集約アドレスを作成します。このルートに関してアドバタイズされるパスは、集約されているすべてのパスに含まれるすべての要素からなる、AS セットです。 • **as-set** キーワードで、AS セット パス情報および関係するパスに基づくコミュニティ情報が生成されます。 • **summary-only** キーワードによって、アップデートから固有性の強いルートがすべてフィルタリングされます。 • **advertise-map** キーワードおよび引数では、選択されたルートから属性情報を選択するためのルート マップを指定します。 • **attribute-map** キーワードおよび引数では、集約から属性情報を選択するためのルート マップを指定します。 • **suppress-map** キーワードおよび引数によって、固有性の強いルートを条件付きでフィルタリングします。

BGP 条件付きアドバタイズメントの設定

BGP がプロパゲートするルートを制限するように BGP 条件付きアドバタイズメントを設定できます。次の 2 つのルート マップを定義します。

- アドバタイズ マップ：BGP が条件付きアドバタイズメントを考慮する前にルートが一致する必要のある条件を指定します。このルート マップには、適切な match ステートメントを含めることができます。
- 存在マップまたは非存在マップ：BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在する必要のあるプレフィクスを定義します。非存在マップは、BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在してはならないプレフィクスを定義します。BGP は、これらのルート マップでプレフィクス リストの match ステートメント内にある permit ステートメントのみを処理します。

ルートが条件を渡さない場合、そのルートが BGP テーブルにあれば BGP によってルートが取り消されます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** *ipaddress* **remote-as** *as-number*
4. **address-family ipv4** {**unicast** | **multicast**}
5. **advertise-map** *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*}
6. （任意）**show ip bgp neighbor**
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	**address-family ipv4** {**unicast**	**multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	**advertise-map** *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*} **Example:** `switch(config-router-neighbor-af)# advertise-map advertise exist-map exist`	2 つの設定済みルート マップに従い、ルートを条件付きでアドバタイズするように BGP を設定します。 • *adv-map* : BGP がルートを次のルート マップに渡す前に、そのルートが渡す必要のある ***match*** ステートメントを使用してルート マップを指定します。*adv-map* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • *exist-rmap :* プレフィクス リストの match ステートメントを使用してルート マップを指定します。BGP テーブル内のプレフィクスは、BGP がルートをアドバタイズする前に、プレフィクス リスト内のプレフィクスと一致する必要があります。*exist-rmap* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。 • *nonexist-rmap :* プレフィクス リストの match ステートメントを使用してルート マップを指定します。BGP テーブル内のプレフィクスは、BGP がルートをアドバタイズする前に、プレフィクス リスト内のプレフィクスと一致してはいけません。*nonexist-rmap* は、大文字と小文字が区別される 63 文字以下の英数字文字列です。
ステップ 6	**show ip bgp neighbor** **Example:** `switch(config-router-neighbor-af)# show ip bgp neighbor`	（任意）BGP に関する情報、および設定した条件付きアドバタイズメントのルート マップに関する情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** `switch(config-router-neighbor-af)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、BGP 条件付きアドバタイズメントを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
```

ルートの再配布の設定

別のルーティング プロトコルからのルーティング情報を受け入れて、BGP ネットワークを通じてその情報を再配布するように、BGP を設定できます。任意で、再配布ルートのためのデフォルト ルートを割り当てることができます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **address-family ipv4** {**unicast** | **multicast**}
4. **redistribute** {**direct** | {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name*
5. （任意）**default-metric** *value*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* Example: switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。
ステップ 3	**address-family ipv4** {**unicast**	**multicast**} **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 4	**redistribute** {**direct**	{**eigrp**	**ospf**	**ospfv3**	**rip**} *instance-tag*	**static**} **route-map** *map-name* **Example:** switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap	他のプロトコルからのルートを BGP に再配布します。ルート マップの詳細については、「ルート マップの設定」（P.11-12）を参照してください。

	コマンド	目的
ステップ 5	**default-metric** *value* **Example:** switch(config-router-af)# default-metric 33	（任意）BGP へのデフォルト ルートを作成します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-router-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、EIGRP を BGP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap
switch(config-router-af)# copy running-config startup-config
```

マルチプロトコル BGP の設定

複数のアドレス ファミリ（IPv4 のユニキャストおよびマルチキャスト ルートを含む）をサポートするように MP-BGP を設定できます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** *ip-address* **remote-as** *as-number*
4. **address-family ipv4** {**unicast** | **multicast**}
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	BGP モードを開始し、ローカル BGP スピーカに AS 番号を割り当てます。

	コマンド	目的
ステップ 3	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。
ステップ 4	**address-family ipv4** {**unicast** | **multicast**} **Example:** switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-router-neighbor-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ネイバーのマルチキャスト RPF に対して IPv4 ルートのアドバタイズおよび受信をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv4 address 2001:0DB8::1
switch(config-if)# router bgp 65536
switch(config-router)# neighbor 192.168.1.2 remote-as 35537
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP の調整

一連のオプション パラメータを使用することによって、BGP 特性を調整できます。

BGP を調整するには、ルータ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
bestpath [**always-compare-med** | **compare-routerid** | **med** {**missing-as-worst** | **non-deterministic**}] **Example:** switch(config-router)# bestpath always-compare-med	ベストパス アルゴリズムを変更します。オプション パラメータは次のとおりです。 • **always-compare-med**：異なる AS からのパスの MED を比較します。 • **compare-routerid**：同一の eBGP パスのルータ ID を比較します。 • **med missing-as-worst**：脱落 MED を最上位 MED として扱います。 • **med non-deterministic**：同じ AS からのパス間で、必ずしも最適な MED パスを選択しません。
enforce-first-as **Example:** switch(config-router)# enforce-first-as	ネイバー AS を eBGP の AS_path 属性で指定する最初の AS 番号にします。
log-neighbor-changes **Example:** switch(config-router)# log-neighbor-changes	ネイバーでステートが変化したときに、システム メッセージを生成します。
router-id *id* **Example:** switch(config-router)# router-id 209.165.20.1	この BGP スピーカのルータ ID を手動で設定します。
timers [**bestpath-delay** *delay* | **bgp** *keepalive holdtime* | **prefix-peer-timeout** *timeout*] **Example:** switch(config-router)# timers bgp 90 270	BGP タイマー値を設定します。オプション パラメータは次のとおりです。 • *delay*：再起動後の初期ベスト パス タイムアウト値。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 300 です。 • keepalive：BGP セッション キープアライブ タイム。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 60 です。 • holdtime：BGP セッション ホールド タイム。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 180 です。 • timeout：プレフィクス ピア タイムアウト値。指定できる範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。 このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

BGP を調整するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
distance *ebgp-distance ibgp distance local-distance* **Example:** `switch(config-router-af)# distance 20 100 200`	BGP のアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトの設定は次のとおりです。 • eBGP ディスタンス：20 • iBGP ディスタンス：200 • ローカル ディスタンス：220。ローカル ディスタンスは、集約廃棄ルートが RIB に組み込まれている場合に、集約廃棄ルートに使用するアドミニストレーティブ ディスタンスです。

BGP を調整するには、ネイバー コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
description *string* **Example:** `switch(config-router-neighbor)# description main site`	この BGP ピアを説明するストリングを設定します。ストリングには最大 80 の英数字を使用できます。
low-memory exempt **Example:** `switch(config-router-neighbor)# low-memory exempt`	メモリ不足状態によるシャットダウンからこの BGP ネイバーを除外します。
transport connection-mode passive **Example:** `switch(config-router-neighbor)# transport connection-mode passive`	受動接続の確立だけが可能です。この BGP スピーカは BGP ピアへの TCP 接続を開始しません。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。
remove-private-as **Example:** `switch(config-router-neighbor)# remove-private-as`	eBGP ピアへの発信ルート アップデートからプライベート AS 番号を削除します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
update-source *interface-type number* **Example:** `switch(config-router-neighbor)# update-source ethernet 2/1`	ピアとの BGP セッション用に設定されたインターフェイスの送信元 IP アドレスを使用するように、BGP スピーカを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

BGP を調整するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
suppress-inactive **Example:** switch(config-router-neighbor-af)# suppress-inactive	ベスト（アクティブ）ルートだけを BGP ピアにアドバタイズします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
default-originate [**route-map** *map-name*] **Example:** switch(config-router-neighbor-af)# default-originate	BGP ピアへのデフォルト ルートを作成します。
filter-list *list-name* {**in** | **out**} **Example:** switch(config-router-neighbor-af)# filter-list BGPFilter in	着信または発信ルート アップデートに関して、この BGP ピアに AS_path フィルタ リストを適用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
prefix-list *list-name* {**in** | **out**} **Example:** switch(config-router-neighbor-af)# prefix-list PrefixFilter in	着信または発信ルート アップデートに関して、この BGP ピアにプレフィクス リストを適用します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
send-community **Example:** switch(config-router-neighbor-af)# send-community	この BGP ピアにコミュニティ属性を送信します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
send-extcommunity **Example:** switch(config-router-neighbor-af)# send-extcommunity	この BGP ピアに拡張コミュニティ属性を送信します。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

仮想化の設定

複数の VRF を作成できます。また、各 VRF で同じ BGP プロセスを使用できます。

はじめる前に

BGP 機能がイネーブルになっていることを確認します（「BGP 機能のイネーブル化」（P.5-11）を参照）。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **exit**
4. **router bgp** *as-number*
5. **vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *as-number*

7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF 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	**exit** **Example:** switch(config-vrf)# exit switch(config)#	VRF コンフィギュレーション モードを終了します。
ステップ 4	**router bgp** *as-number* **Example:** switch(config)# router bgp 65536 switch(config-router)#	AS 番号を設定して、新しい BGP プロセスを作成します。
ステップ 5	**vrf** *vrf-name* **Example:** switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	ルータ VRF コンフィギュレーション モードを開始し、この BGP インスタンスと VRF を関連付けます。
ステップ 6	**neighbor** *ip-address* **remote-as** *as-number* **Example:** switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536 switch(config-router--vrf-neighbor)#	リモート BGP ピアの IP アドレスおよび AS 番号を設定します。
ステップ 7	**copy running-config startup-config** **Example:** switch(config-router-vrf-neighbor)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成し、VRF でルータ ID を設定する例を示します。

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router bgp 65536
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536
switch(config-router-vrf-neighbor)# copy running-config startup-config
```

拡張 BGP の設定の確認

BGP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show bgp all [**summary**] [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp convergence [**vrf** *vrf-name*]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **community** {**regexp** ***expression*** | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]} [**vrf** *vrf-name*]	BGP コミュニティと一致する BGP ルートを表示します。
show bgp [**vrf** *vrf-name*] **ip** {**unicast** | **multicast**} [*ip-address*] **community-list** ***list-nam***e [**vrf** *vrf-name*]	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **extcommunity** {**regexp** ***expression*** | **generic** [**non-transitive** | **transitive**] *aa4:nn* [**exact-match**]} [**vrf** *vrf-name*]	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **extcommunity-list** ***list-nam***e [**exact-match**] [**vrf** *vrf-name*]	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] {**dampening dampened-paths** [**regexp** ***expression***]} [**vrf** *vrf-name*]	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、**clear bgp dampening** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **history-paths** [**regexp** ***expression***] [**vrf** *vrf-name*]	BGP ルート ヒストリ パスを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **filter-list** *list-name* [**vrf** *vrf-name*]	BGP フィルタ リストの情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **neighbors** [*ip-address*] [**vrf** *vrf-name*]	BGP ピアの情報を表示します。これらのネイバーを消去するには、**clear bgp neighbors** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] {**nexthop** | **nexthop-database**} [**vrf** *vrf-name*]	BGP ルート ネクストホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **policy** ***name*** [**vrf** *vrf-name*]	BGP ポリシー情報を表示します。ポリシー情報を消去するには、**clear bgp policy** コマンドを使用します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **prefix-list** *list-name* [**vrf** *vrf-name*]	プレフィクス リストと一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **received-paths** [**vrf** *vrf-name*]	ソフト再構成用に保管されている BGP パスを表示します。

コマンド	目的
show bgp ip {**unicast** | **multicast**} [*ip-address*] **regexp** *expression* [**vrf** *vrf-name*]	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp ip {**unicast** | **multicast**} [*ip-address*] **route-map** *map-name* [**vrf** *vrf-name*]	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy *name* [**vrf** *vrf-name*]	BGP ピア ポリシー情報を表示します。
show bgp peer-session ***name*** [**vrf** *vrf-name*]	BGP ピア セッション情報を表示します。
show bgp peer-template *name* [**vrf** *vrf-name*]	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、**clear bgp peer-template** コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。
show ip bgp *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。
show ip mbgp *options*	BGP のステータスと構成情報を表示します。このコマンドには複数のオプションがあります。詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報の表示

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp ip {**unicast** | **multicast**} [*ip-address*] **flap-statistics** [**vrf** *vrf-name*]	BGP ルート フラップの統計情報を表示します。これらの統計情報を消去するには、**clear bgp flap-statistics** コマンドを使用します。
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。
show bgp sessions [**vrf** *vrf-name*]	すべてのピアの BGP セッションを表示します。これらの統計情報を消去するには、**clear bgp sessions** コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

関連資料

BGP の詳細については、次の項目を参照してください。

- 第 6 章「拡張 BGP の設定」
- 第 11 章「Route Policy Manager の設定」

その他の関連資料

BGP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.6-41）
- 「管理情報ベース（MIB）」（P.6-41）

関連資料

関連項目	マニュアル名
BGP CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

管理情報ベース（MIB）

管理情報ベース（MIB）	MIB のリンク
BGP4-MIB CISCO-BGP4-MIB	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

BGP 機能の履歴

表 6-2 は、この機能のリリースの履歴です。

表 6-2　BGP 機能の履歴

機能名	リリース	機能情報
BGP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 7

RIP の設定

この章では、RIP の設定方法について説明します。

この章では、次の内容について説明します。

RIP 情報

ここでは、次の内容について説明します。

RIP の概要

RIP は UDP（ユーザ データグラム プロトコル）データ パケットを使用して、小規模なインターネット ワークでルーティング情報を交換します。RIPv2 は IPv4 をサポートしています。RIPv2 は RIPv2 プロトコルがサポートするオプションの認証機能を使用します（「RIPv2 の認証」（P.7-2）を参照）。

RIP では次の 2 種類のメッセージを使用します。

- 要求：他の RIP 対応ルータからのルート アップデートを要求するためにマルチキャスト アドレス 224.0.0.9 に送信されます。
- 応答：デフォルトでは 30 秒間隔で送信されます（「RIP コンフィギュレーションの確認」（P.7-17）を参照）。ルータも、要求メッセージの受信後に応答メッセージを送信します。応答メッセージには、RIP ルート テーブル全体が含まれます。RIP ルーティング テーブルが 1 つの応答パケットに収まらない場合、RIP は 1 つの要求に対して複数の応答パケットを送信します。

RIP はルーティング メトリックとして、*ホップ カウント*を使用します。ホップ カウントは、パケットが宛先に到達するまでに、通過できるルータの数です。直接接続されたネットワークのメトリックは 1 です。到達不能なネットワークのメトリックは 16 です。RIP はこのようにメトリックの範囲が小さいので、大規模なネットワークに適したルーティング プロトコルではありません。

RIPv2 の認証

RIP メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。Cisco NX-OS は簡易パスワードまたは MD5 認証ダイジェストをサポートしています。

認証キーのキーチェーン管理を使用することによって、インターフェイスごとに RIP 認証を設定できます。キーチェーン管理によって、MD5 認証ダイジェストまたは単純テキスト パスワード認証で使用される認証キーの変更を制御できます。キーチェーン作成の詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。

MD5 認証ダイジェストを使用するには、ローカル ルータとすべてのリモート RIP ネイバーが共有するパスワードを設定します。Cisco NX-OS は、そのメッセージ自体と暗号化されたパスワードに基づいて MD5 一方向メッセージ ダイジェストを作成し、このダイジェストを RIP メッセージ（要求または応答）とともに送信します。受信側の RIP ネイバーは、同じ暗号パスワードを使用して、ダイジェストを検証します。メッセージが変更されていない場合は、計算が一致し、RIP メッセージは有効と見なされます。

MD5 認証ダイジェストの場合はさらに、ネットワークでメッセージが再送されないように、各 RIP メッセージにシーケンス番号が組み込まれます。

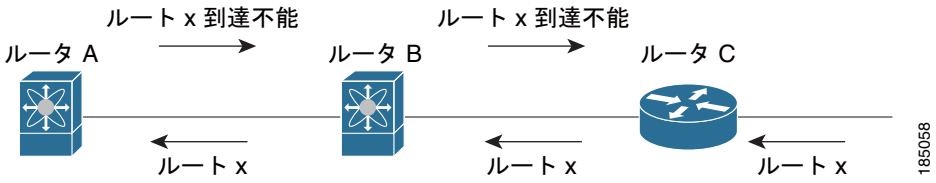
スプリット ホライズン

スプリット ホライズンを使用すると、ルートを学習したインターフェイスからは、RIP がルートをアドバタイズしないようにできます。

スプリット ホライズンは、RIP アップデートおよびクエリー パケットの送信を制御する方法です。インターフェイス上でスプリット ホライズンがイネーブルの場合、Cisco NX-OS はそのインターフェイスから学習した宛先にはアップデート パケットを送信しません。この方法でアップデート パケットを制御すると、ルーティング ループの発生する可能性が小さくなります。

ポイズン リバースを指定してスプリット ホライズンを使用すると、ルートを学習したインターフェイス経由では到達不能であると RIP が学習したルートをアドバタイズするように、インターフェイスを設定できます。図 7-1 に、ポイズン リバースをイネーブルにしてスプリット ホライズンを指定した、RIP ネットワークの例を示します。

図 7-1　スプリット ホライズン ポイズン リバースを指定した RIP



ルータ C はルート X について学習し、そのルートをルータ B にアドバタイズします。ルータ B は次に、ルート X をルータ A にアドバタイズしますが、ルータ C には、ルート X 到達不能アップデートを戻します。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

ルート フィルタリング

RIP 対応インターフェイス上でルート ポリシーを設定すると、RIP アップデートをフィルタリングできます。Cisco NX-OS は、ルート ポリシーで許可されたルートだけを使用して、ルート テーブルをアップデートします。

ルート集約

指定したインターフェイスに、複数のサマリー集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

RIP はルーティング テーブルに含まれている固有性の強いルートが多いほど、固有性の強いルートの最大メトリックと同じメトリックのインターフェイスからのサマリー アドレスをアドバタイズします。

（注）　Cisco NX-OS は、自動ルート集約をサポートしていません。

ルートの再配布

RIP を使用すると、スタティック ルートまたは他のプロトコルからのルートを再配布できます。再配布を設定するには、ルート ポリシーを使用して、RIP に渡すルートを制御します。ルート ポリシーを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

RIP ルーティング ドメインにルートを再配布しても、デフォルトでは Cisco NX-OS がそのつど、RIP ルーティング ドメインにデフォルト ルートを再配布することはありません。RIP へのデフォルト ルートを発生させ、ルート ポリシーでそのルートを制御できます。

RIP にインポートされたすべてのルートに使用する、デフォルトのメトリックも設定できます。

ロード バランシング

ロード バランシングを使用すると、ルータによって、宛先アドレスから同じ距離にあるすべてのルータ ネットワーク ポートにトラフィックが分散されます。ロード バランシングは、ネットワーク セグメントの使用率を向上させ、有効ネットワーク帯域幅を増加させます。

Cisco NX-OS は、ECMP（等コスト マルチパス）機能をサポートします。RIP ルート テーブルおよびユニキャスト RIB の等コスト パスは最大 16 です。これらのパスの一部または全部でトラフィックのロード バランシングが行われるように、RIP を設定できます。

仮想化のサポート

Cisco NX-OS は、同一システム上で動作する複数の RIP プロトコル インスタンスをサポートします。RIP は VRF（仮想ルーティングおよびフォワーディング）インスタンスをサポートします。

デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。第 9 章「レイヤ 3 仮想化の設定」を参照してください。

RIP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	RIP にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。 **（注）** レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

RIP の前提条件

RIP を使用するには、次の前提条件を満たしている必要があります。

- RIP 機能をイネーブルにする必要があります（「RIP 機能のイネーブル化」（P.7-5）を参照）。

注意事項および制約事項

RIP には、次の注意事項および制限事項があります。

- Cisco NX-OS は、RIPv1 をサポートしません。RIPv1 パケットを受信した Cisco NX-OS は、メッセージを記録してパケットを廃棄します。
- Cisco NX-OS は、RIPv1 ルータとの隣接関係を確立しません。

デフォルト設定

表 7-1 は、各 RIP パラメータに対するデフォルト設定を示します。

表 7-1　デフォルトの RIP パラメータ

パラメータ	デフォルト
ロード バランシングを行う最大パス数	16
RIP 機能	ディセーブル
スプリット ホライズン	イネーブル

RIP の設定

ここでは、次の内容について説明します。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

RIP 機能のイネーブル化

RIP を設定するには、RIP 機能をイネーブルにしておく必要があります。

手順の概要

1. **configure terminal**
2. **feature rip**
3. （任意）**show feature**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**feature rip** **Example:** switch(config)# feature rip	RIP 機能をイネーブルにします。
ステップ 3	**show feature** **Example:** switch(config)# show feature	（任意）イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

RIP 機能をディセーブルにして、関連するすべての設定を削除する場合は、**no feature rip** コマンドを使用します。

コマンド	目的
no feature rip **Example:** switch(config)# no feature rip	RIP 機能をディセーブルにして、関連するすべての設定を削除します。

RIP インスタンスの作成

RIP インスタンスを作成し、そのインスタンス用のアドレス ファミリを設定できます。

はじめる前に

RIP 機能がイネーブルになっていることを確認します（「RIP 機能のイネーブル化」（P.7-5）を参照）。

手順の概要

1. **configure terminal**
2. **router rip** *instance-tag*
3. **address-family ipv4 unicast**
4. （任意）**show ip rip** [**instance** *instance-tag*] [**vrf** *vrf-name*]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router rip** *instance-tag* **Example:** switch(config)# router RIP Enterprise switch(config-router)#	*instance tag* を設定して、新しい RIP インスタンスを作成します。
ステップ 3	**address-family ipv4 unicast** **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	この RIP インスタンスのアドレス ファミリを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 4	**show ip rip** [**instance** *instance-tag*] [**vrf** *vrf-name*] **Example:** switch(config-router-af)# show ip rip	（任意）すべての RIP インスタンスについて、RIP 要約情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-router-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

RIP インスタンスおよび関連するすべての設定を削除する場合は、**no router rip** コマンドを使用します。

コマンド	目的
no router rip *instance-tag* **Example:** switch(config)# no router rip Enterprise	RIP インスタンスおよび関連するすべての設定を削除します。

（注）　インターフェイス モードで設定した RIP コマンドを削除することも必要です。

アドレス ファミリ コンフィギュレーション モードでは、RIP に次のオプション パラメータを設定できます。

コマンド	目的
distance *value* **Example:** switch(config-router-af)# distance 30	RIP のアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトは 120 です。「アドミニストレーティブ ディスタンス」（P.1-7）を参照してください。
maximum-paths *number* **Example:** switch(config-router-af)# maximum-paths 6	RIP がルート テーブルで維持する等コスト パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルトは 16 です。

次に、IPv4 に対応する RIP インスタンスを作成し、ロード バランシングのための等コスト パス数を設定する例を示します。

```
switch# configure terminal
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# max-paths 10
switch(config-router-af)# copy running-config startup-config
```

RIP インスタンスの再起動

RIP インスタンスの再起動が可能です。再起動すると、インスタンスのすべてのネイバーが消去されます。

RIP インスタンスを再起動し、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

コマンド	目的
restart rip instance-tag **Example:** switch(config)# restart rip Enterprise	RIP インスタンスを再起動し、すべてのネイバーを削除します。

インターフェイス上での RIP の設定

RIP インスタンスにインターフェイスを追加できます。

はじめる前に

RIP 機能がイネーブルになっていることを確認します（「RIP 機能のイネーブル化」（P.7-5）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **ip rip** *instance-tag*

5. （任意）**show ip rip** [**instance** *instance-tag*] **interface** [*interface-type slot/port*] [**vrf** *vrf-name*] [**detail**]
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip router rip** *instance-tag* **Example:** switch(config-if)# ip router rip Enterprise	このインターフェイスを RIP インスタンスに関連付けます。
ステップ 5	**show ip rip** [**instance** *instance-tag*] **interface** [*interface-type slot/port*] [**vrf** *vrf-name*] [**detail**] **Example:** switch(config-if)# show ip rip Enterprise tethernet 1/2	（任意）インターフェイスの RIP 情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、RIP インスタンスにインターフェイス ethernet 1/2 を追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip router rip Enterprise
switch(config)# copy running-config startup-config
```

RIP 認証の設定

インターフェイス上で RIP パケットの認証を設定できます。

はじめる前に

RIP 機能がイネーブルになっていることを確認します（「RIP 機能のイネーブル化」（P.7-5）を参照）。

認証をイネーブルにする前に、必要に応じてキーチェーンを設定します。キーチェーンの実装の詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **ip rip authentication mode**{**text** | **md5**}
5. **ip rip authentication key-chain** *key*
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip rip authentication mode** {**text** | **md5**} **Example:** switch(config-if)# ip rip authentication mode md5	クリアテキストまたは MD5 認証ダイジェストとして、このインターフェイスにおける RIP 認証タイプを設定します。
ステップ 5	**ip rip authentication key-chain** *key* **Example:** switch(config-if)# ip rip authentication keychain RIPKey	このインターフェイス上で RIP に使用する認証キーを設定します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、キーチェーンを作成し、RIP インターフェイス上で MD5 認証を設定する例を示します。

```
switch# configure terminal
switch(config)# key chain RIPKey
switch(config)# key-string myrip
switch(config)# accept-lifetime 00:00:00 Jan 01 2000 infinite
switch(config)# send-lifetime 00:00:00 Jan 01 2000 infinite
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip rip authentication mode md5
switch(config-if)# ip rip authentication keychain RIPKey
switch(config-if)# copy running-config startup-config
```

受動インターフェイスの設定

インターフェイスを受動モードに設定することによって、ルートを受信するが、ルート アップデートの送信は行わないように RIP インターフェイスを設定できます。

受動モードで RIP インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip rip passive-interface **Example:** `switch(config-if)# ip rip passive-interface`	インターフェイスを受動モードに設定します。

ポイズン リバースを指定したスプリット ホライズンの設定

ポイズン リバースをイネーブルにすることによって、ルートを学習したインターフェイス経由では到達不能であると RIP が学習したルートをアドバタイズするように、インターフェイスを設定できます。

インターフェイス上で、ポイズン リバースを指定してスプリット ホライズンを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip rip poison-reverse **Example:** `switch(config-if)# ip rip poison-reverse`	ポイズン リバースを指定してスプリット ホライズンをイネーブルにします。ポイズン リバースを指定したスプリット ホライズンは、デフォルトでディセーブルです。

ルート集約の設定

ルーティング テーブルでサマリー アドレスによって表される集約アドレスを作成できます。Cisco NX-OS は、固有性の強いすべてのルートの中でメトリックが最小のサマリー アドレス メトリックをアドバタイズします。

インターフェイス上でサマリー アドレスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip rip summary-address *ip-prefix/mask-len* **Example:** switch(config-if)# ip router rip summary-address 192.0.2.0/24	IPv4 アドレスに対応する、RIP 用のサマリー アドレスを設定します。

ルートの再配布の設定

別のルーティング プロトコルからのルーティング情報を受け入れて、RIP ネットワークを通じてその情報を再配布するように、RIP を設定できます。再配布されたルートを任意で、デフォルト ルートとして割り当てることができます。

はじめる前に

RIP 機能がイネーブルになっていることを確認します（「RIP 機能のイネーブル化」（P.7-5）を参照）。

再配布を設定する前に、ルート マップを設定します。ルート マップ設定の詳細については、「ルート マップの設定」（P.11-12）を参照してください。

手順の概要

1. **configure terminal**
2. **router rip** *instance-tag*
3. **address-family ipv4 unicast**
4. **redistribute** {**bgp** *as* | **direct** | **eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name*
5. （任意）**default-information originate** [**always**] [**route-map** *map-name*]
6. （任意）**default-metric** *value*
7. （任意）**show ip rip route** [{*ip-prefix* [*longer*-**prefixes** | **shorter-prefixes**]] [**vrf** *vrf-name*] [**summary**]
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router rip** *instance-tag* **Example:** switch(config)# router rip Enterprise switch(config-router)#	*instance tag* を設定して、新しい RIP インスタンスを作成します。

	コマンド	目的
ステップ 3	**address-family ipv4 unicast** **Example:** switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 4	**redistribute** {**bgp** *as* | **direct** |{**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name* **Example:** switch(config-router-af)# redistribute eigrp 201 route-map RIPmap	他のプロトコルからのルートを RIP に再配布します。ルート マップの詳細については、「ルート マップの設定」（P.11-12）を参照してください。
ステップ 5	**default-information originate** [**always**] [**route-map** *map-name*] **Example:** switch(config-router-af)# default-information originate always	（任意）RIP へのデフォルト ルートを作成し、任意でルート マップで制御します。
ステップ 6	**default-metric** *value* **Example:** switch(config-router-af)# default-metric 10	（任意）再配布されたすべてのルートにデフォルト メトリックを設定します。指定できる範囲は 1 ～ 15 です。デフォルトは 1 です。
ステップ 7	**show ip rip route** [*ip-prefix* [**longer-prefixes** | **shorter-prefixes**] [**vrf** *vrf-name*] *[summary*] **Example:** switch(config-router-af)# show ip rip route	（任意）RIP のルートを表示します。
ステップ 8	**copy running-config startup-config** **Example:** switch(config-router-af)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、EIGRP を RIP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router rip Enterprise
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map RIPmap
switch(config-router-af)# copy running-config startup-config
```

仮想化の設定

複数の VRF を作成できます。また、各 VRF で同じ RIP インスタンスを使用することも、複数の RIP インスタンスを使用することも可能です。VRF に RIP インターフェイスを割り当てます。

（注）　インターフェイスの VRF を設定したあとに、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

はじめる前に

RIP 機能がイネーブルになっていることを確認します（「RIP 機能のイネーブル化」（P.7-5）を参照）。

手順の概要

1. **configure terminal**
2. **vrf** *vrf-name*
3. **exit**
4. **router rip** *instance-tag*
5. **vrf context** *vrf_name*
6. （任意）**address-family ipv4 unicast**
7. （任意）**redistribute** {**bgp** *as* | **direct** | {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name*
8. **interface ethernet** *slot/port*
9. **no switchport**
10. **vrf member** *vrf-name*
11. **ip-address** *ip-prefix/length*
12. **ip router rip** *instance-tag*
13. （任意）**show ip rip** [**instance** *instance-tag*] **interface** [*interface-type slot/port*] [**vrf** *vrf-name*]
14. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf** *vrf-name* **Example:** switch(config)# vrf RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成します。
ステップ 3	**exit** **Example:** switch(config-vrf)# exit switch(config)#	VRF コンフィギュレーション モードを終了します。
ステップ 4	**router rip** *instance-tag* **Example:** switch(config)# router rip Enterprise switch(config-router)#	instance tag を設定して、新しい RIP インスタンスを作成します。

	コマンド	目的
ステップ 5	**vrf context** *vrf-name* **Example:** switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	新しい VRF を作成し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**address-family ipv4 unicast** **Example:** switch(config-router-vrf)# address-family ipv4 unicast switch(config-router-vrf-af)#	（任意）この RIP インスタンスの VRF アドレス ファミリを設定します。
ステップ 7	**redistribute** {**bgp** *as* | **direct** | {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} **route-map** *map-name* **Example:** switch(config-router-vrf-af)# redistribute eigrp 201 route-map RIPmap	（任意）他のプロトコルからのルートを RIP に再配布します。ルート マップの詳細については、「ルート マップの設定」（P.11-12）を参照してください。
ステップ 8	**interface ethernet** *slot/port* **Example:** switch(config-router-vrf-af)# interface ethernet 1/2 switch(config-if)#	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 9	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 10	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 11	**ip address** *ip-prefix/length* **Example:** switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 12	**ip router rip** *instance-tag* **Example:** switch(config-if)# ip router rip Enterprise	このインターフェイスを RIP インスタンスに関連付けます。
ステップ 13	**show ip rip** [**instance** *instance-tag*] **interface** [*interface-type slot/port*] [**vrf** *vrf-name*] **Example:** switch(config-if)# show ip rip Enterprise ethernet 1/2	（任意）インターフェイスの RIP 情報を表示します。（VRF 内）。
ステップ 14	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# exit
switch(config)# router rip Enterprise
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)# address-family ipv4 unicast
switch(config-router-vrf-af)# redistribute eigrp 201 route-map RIPmap
switch(config-router-vrf-af)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router rip Enterprise
switch(config-if)# copy running-config startup-config
```

RIP の調整

ネットワーク要件に合わせて RIP を調整できます。RIP では複数のタイマーを使用して、ルーティング アップデート間隔、ルートが無効になるまでの時間の長さ、およびその他のパラメータを決定します。これらのタイマーを調整すると、インターネットワークのニーズに適合するように、ルーティング プロトコルのパフォーマンスを調整できます。

（注）　ネットワーク上のすべての RIP 対応ルータで、RIP タイマーに同じ値を設定する必要があります。

RIP を調整するには、アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
timers basic *update timeout holddown garbage-collection* **Example:** `switch(config-router-af)# timers basic 40 120 120 100`	RIP タイマーを秒数で設定します。パラメータは次のとおりです。 • update：指定できる範囲は 5 ～任意の正の整数。デフォルトは 30 です。 • timeout：ルートの無効を宣言するまでに、Cisco NX-OS が待機する時間。タイムアウト インターバルが終了するまでに、このルートのアップデート情報を Cisco NX-OS が受信しなかった場合、Cisco NX-OS はルートの無効を宣言します。指定できる範囲は 1 ～任意の正の整数です。デフォルトは 180 です。 • holddown：無効ルートに関するよりよいルート情報を Cisco NX-OS が無視する時間。指定できる範囲は 0 ～任意の正の整数です。デフォルトは 180 です。 • garbage-collection：Cisco NX-OS がルートを無効として表示してから、Cisco NX-OS がそのルートをルーティング テーブルから削除するまでの時間。指定できる範囲は 1 ～任意の正の整数です。デフォルトは 120 です。

RIP を調整するには、インターフェイス コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
ip rip metric-offset *value* **Example:** switch(config-if)# ip rip metric-offset 10	このインターフェイスで受信する各ルータのメトリックに値を追加します。指定できる範囲は 1 ～ 15 です。デフォルトは 1 です。
ip rip route-filter {prefix-list *list-name* **| route-map** *map-name*| [**in** | **out**] **Example:** switch(config-if)# ip rip route-filter route-map InputMap in	着信または発信 RIP アップデートをフィルタリングするための、ルート マップを指定します。

RIP コンフィギュレーションの確認

RIP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip rip instance [*instance-tag*] [**vrf** *vrf-name*]	RIP インスタンスの状態を表示します。
show ip rip [**instance** *instance-tag*] **interface** *slot/port* **detail** [**vrf** *vrf-name*]	インターフェイスの RIP ステータスを表示します。
show ip rip [**instance** *instance-tag*] **neighbor** [*interface-type number*] [**vrf** *vrf-name*]	RIP ネイバー テーブルを表示します。
show ip} **rip** [**instance** *instance-tag*] **route** [*ip-prefix/lengh* [**longer-prefixes** | **shorter--prefixes]] [summary**] [**vrf** *vrf-name*]	RIP ルート テーブルを表示します。
show running-configuration rip	現在実行中の RIP コンフィギュレーションを表示します。

RIP 統計情報の表示

RIP 統計情報設定表示するには、次のコマンドを使用します。

コマンド	目的
show ip rip [**instance** *instance-tag*] **policy statistics redistribute** {**bgp** *as* | **direct** | {**eigrp** | **ospf** | **ospfv3** | **rip**} *instance-tag* | **static**} [**vrf** *vrf-name*]	RIP ポリシー ステータスを表示します。
show ip rip [**instance** *instance-tag*] **statistics** *interface-type number*] [**vrf** *vrf-name*]	RIP の統計情報を表示します。

ポリシーの統計情報を消去するには、**clear ip rip policy** コマンドを使用します。

RIP の統計情報を消去するには、**clear ip rip statistics** コマンドを使用します。

RIP の設定例

VRF で Enterprise RIP インスタンスを作成し、その RIP インスタンスにイーサネット インターフェイス 1/2 を追加する例を示します。さらに、enthernet interface 1/2 の認証を設定し、この RIP ドメインに EIGRP を再配布します。

```
vrf context NewVRF
!
 feature rip
 router rip Enterprise
  vrf NewVRF
   address-family ip unicast
    redistribute eigrp 201 route-map RIPmap
    max-paths 10
!
interface ethernet 1/2
 no switchport
 vrf NewVRF
 ip address 192.0.2.1/16
 ip router rip Enterprise
 ip rip authentication mode md5
 ip rip authentication keychain RIPKey
```

関連資料

ルート マップの詳細については、第 11 章「Route Policy Manager の設定」を参照してください。

その他の関連資料

RIP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.7-19）
- 「標準」（P.7-19）

関連資料

関連項目	マニュアル名
RIP CLI コマンド	『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

RIP 機能の履歴

表 7-2 は、この機能のリリースの履歴です。

表 7-2　RIP 機能の履歴

機能名	リリース	機能情報
RIP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 8

スタティック ルーティングの設定

この章では、スイッチ上でスタティック ルーティングを設定する方法について説明します。

この章では、次の内容について説明します。

スタティック ルーティングの概要

ルータは、ユーザが手動で設定したルート テーブル エントリのルート情報を使用するか、またはダイナミック ルーティング アルゴリズムで計算されたルート情報を使用して、パケットを転送します。

スタティック ルートは、2 つのルータ間の明示パスを定義するものであり、自動的にはアップデートされません。ネットワークに変更があった場合は、ユーザが手動でスタティック ルートを再設定する必要があります。スタティック ルートは、ダイナミック ルートに比べて使用する帯域幅が少なくなります。ルーティング アップデートの計算や分析に CPU サイクルを使用しません。

必要に応じて、スタティック ルートでダイナミック ルートを補うことができます。スタティック ルートをダイナミック ルーティング アルゴリズムに再配布できますが、ダイナミック ルーティング アルゴリズムで計算されたルーティング情報をスタティック ルーティング テーブルに再配布できません。

スタティック ルートは、ネットワーク トラフィックが予測可能で、ネットワーク設計が単純な環境で使用します。スタティック ルートはネットワークの変化に対応できないので、大規模でたえず変化しているネットワークでは、スタティック ルートを使用すべきではありません。大部分のネットワークは、ルータ間の通信にダイナミック ルートを使用しますが、特殊な状況でスタティック ルートを 1 つか 2 つ設定する場合があります。スタティック ルートは、最終手段としてのゲートウェイ（ルーティング不能なすべてのパケットの送信先となるデフォルト ルータ）を指定する場合にも便利です。

ここでは、次の内容について説明します。

管理ディスタンス

アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に、2 つ以上のルートが存在する場合に、最適なパスを選択するために、ルータが使用するメトリックです。複数のプロトコルがユニキャスト ルーティング テーブルに同じルートを追加した場合に、アドミニストレーティブ ディスタンスを手がかりに、他のルーティング プロトコル（またはスタティック ルート）ではなく、特定のルーティング プロトコル（またはスタティック ルート）が選択されます。各ルーティング プロトコルは、アドミニストレーティブ ディスタンス値を使用して、信頼性の高い順にプライオリティが与えられます。

スタティック ルート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 1 です。ルータは値の小さいルートが最短であると見なすので、スタティック ルートがダイナミック ルートより優先されます。ダイナミック ルートでスタティック ルートを上書きする場合は、スタティック ルートにアドミニストレーティブ ディスタンスを指定します。たとえば、アドミニストレーティブ ディスタンスが 120 のダイナミック ルートが 2 つある場合に、ダイナミック ルートでスタティック ルートを上書きするには、スタティック ルートに 120 より大きいアドミニストレーティブ ディスタンスを指定します。

直接接続のスタティック ルート

直接接続のスタティック ルートで指定しなければならないのは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）だけです。ルータは宛先が出力インターフェイスに直接接続されているものと見なし、パケットの宛先をネクストホップ アドレスとして使用します。ネクストホップは、ポイントツーポイント インターフェイスの場合に限り、インターフェイスにできます。ブロードキャスト インターフェイスの場合は、ネクストホップを IPv4 アドレスにする必要があります。

完全指定のスタティック ルート

完全指定のスタティック ルートでは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）またはネクスト ホップ アドレスのどちらかを指定する必要があります。完全指定のスタティック ルートを使用できるのは、出力インターフェイスがマルチアクセス インターフェイスで、ネクストホップ アドレスを特定する必要がある場合です。ネクストホップ アドレスは、指定された出力インターフェイスに直接接続する必要があります。

フローティング スタティック ルート

フローティング スタティック ルートは、ダイナミック ルートをバックアップするためにルータが使用するスタティック ルートです。フローティング スタティック ルートには、バックアップするダイナミック ルートより大きいアドミニストレーティブ ディスタンスを設定する必要があります。この場合、ルータはフローティング スタティック ルートよりダイナミック ルートを優先させます。フローティング スタティック ルートは、ダイナミック ルートが失われた場合の代用として使用できます。

（注）　デフォルトでは、ルータはダイナミック ルートよりスタティック ルートを優先させます。スタティック ルートの方がダイナミック ルートより、アドミニストレーティブ ディスタンスが小さいからです。

スタティック ルートのリモート ネクスト ホップ

リモート（非直接接続）ネクストホップを指定したスタティック ルートの場合、ルータに直接接続されていないネイバー ルータのネクストホップ アドレスを指定できます。データ転送時に、スタティック ルートにリモート ネクストホップがあると、そのネクスト ホップがユニキャスト ルーティング テーブルで繰り返し使用され、リモート ネクストホップに到達可能な、対応する直接接続のネクスト ホップ（複数可）が特定されます。

仮想化のサポート

スタティック ルートは Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

スタティック ルーティングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	スタティック ルーティングにライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。 （注）　レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

スタティック ルーティングの前提条件

スタティック ルーティングの前提条件は、次のとおりです。

- スタティック ルートのネクストホップ アドレスが到達不能な場合、そのスタティック ルートはユニキャスト ルーティング テーブルに追加されません。

注意事項および制約事項

スタティック ルーティング設定時の注意事項および制約事項は、次のとおりです。

- スタティック ルートのネクストホップ アドレスとしてインターフェイスを指定できるのは、GRE トンネルなどのポイントツーポイント インターフェイスの場合に限られます。

デフォルト設定

表 8-1 に、スタティック ルーティング パラメータのデフォルト設定を示します。

表 8-1　デフォルトのスタティック ルーティング パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	1
RIP 機能	ディセーブル

スタティック ルーティングの設定

ここでは、次の内容について説明します。

- 「スタティック ルートの設定」（P.8-4）
- 「仮想化の設定」（P.8-5）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スタティック ルートの設定

ルータ上でスタティック ルートを設定できます。

手順の概要

1. **configure terminal**
2. **ip route** {*ip-prefix* | *ip-addr ip-mask*} {[*next-hop* | *nh-prefix*] | [*interface next-hop* | *nh-prefix*]} [**tag** *tag-value* [*pref*]]
3. （任意）**show ip static-route**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip route** {*ip-prefix* | *ip-addr ip-mask*} {[*next-hop* | *nh-prefix*] | [*interface next-hop* | *nh-prefix*]} [**tag** *tag-value* [*pref*] **Example:** switch(config)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクストホップ アドレスを設定できます。*preference* 値でアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。
ステップ 3	**show ip static-route** **Example:** switch(config)# show ip static-route	（任意）スタティック ルート情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

スタティック ルートの設定例を示します。

```
switch# configure terminal
switch(config)# ip route 192.0.2.0/8 192.0.2.10
switch(config)# copy running-config startup-config
```

スタティック ルートを削除するには、**no ip static-route** コマンドを使用します。

仮想化の設定

VRF でスタティック ルートを設定できます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip route** {*ip-prefix* | *ip-addr ip-mask*} {*next-hop* | *nh-prefix* | *interface*} [**tag** *tag-value* [*pref*]
4. （任意）**show ip static-route vrf** *vrf-nam*e
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **Example:** switch(config)# vrf context StaticVrf	VRF を作成し、VRF コンフィギュレーション モードを開始します。
ステップ 3	**ip route** {*ip-prefix* | *ip-addr ip-mask*} {*next-hop* | *nh-prefix* | *interface*} [**tag** *tag-value* [*pref*] **Example:** switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクスト ホップ アドレスを設定できます。*preference* 値でアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。
ステップ 4	**show ip static-route vrf** *vrf-name* **Example:** switch(config-vrf)# show ip static-route	（任意）スタティック ルート情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-vrf)# copy running-config startup-config	（任意）この設定の変更を保存します。

スタティック ルートの設定例を示します。

```
switch# configure terminal
switch(config)# vrf context StaticVrf
switch(config-vrf)# ip route 192.0.2.0/8 192.0.2.10
switch(config-vrf)# copy running-config startup-config
```

スタティック ルーティングの設定確認

スタティック ルーティングの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip static-route	設定されているスタティック ルートを表示します。

設定：スタティック ルーティングの例

次に、スタティック ルーティングの設定例を示します。

```
configure terminal
 ip route 192.0.2.0/8 192.0.2.10
 copy running-config startup-config
```

その他の関連資料

スタティック ルーティングの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.8-7）

関連資料

関連項目	マニュアル名
スタティック ルーティング CLI	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

スタティック ルーティングの機能の履歴

表 8-2 は、この機能のリリースの履歴です。

表 8-2　スタティック ルーティングの機能の履歴

機能名	リリース	機能情報
スタティック ルーティング	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 9

レイヤ 3 仮想化の設定

この章では、レイヤ 3 仮想化の設定手順について説明します。

この章では、次の内容について説明します。

レイヤ 3 仮想化

ここでは、次の内容について説明します。

レイヤ 3 仮想化の概要

Cisco NX-OS は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。各 VRF には、IPv4 に対応するユニキャストおよびマルチキャスト ルート テーブルを備えた、独立したアドレス スペースが 1 つずつあり、他の VRF と無関係にルーティングを決定できます。

ルータごとに、デフォルト VRF および管理 VRF があります。すべてのレイヤ 3 インターフェイスおよびルーティング プロトコルは、ユーザが別の VRF に割り当てないかぎり、デフォルト VRF に存在します。管理 VRF に mgmt0 インターフェイスが存在します。スイッチは、VRF-Lite 機能を使用してカスタマー エッジ（CE）スイッチで複数の VRF をサポートします。VRF-Lite によって、サービス プロバイダーは 1 つのインターフェイスを使用して、重複する IP アドレスを持つ複数のバーチャル プライベート ネットワーク（VPN）をサポートできます。

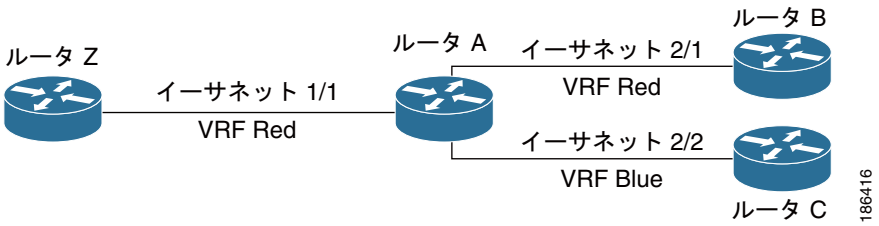
（注）　スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

VRF およびルーティング

すべてのユニキャストおよびマルチキャスト ルーティング プロトコルは VRF をサポートします。VRF でルーティング プロトコルを設定する場合は、同じルーティング プロトコル インスタンスの別の VRF のルーティング パラメータに依存しないルーティング パラメータをその VRF に設定します。

VRF にインターフェイスおよびルーティング プロトコルを割り当てることによって、仮想レイヤ 3 ネットワークを作成できます。インターフェイスが存在する VRF は 1 つだけです。図 9-1 に、1 つの物理ネットワークが 2 つの VRF からなる 2 つの仮想ネットワークに分割されている例を示します。ルータ Z、A、および B は、VRF Red にあり、1 つのアドレス ドメインを形成しています。これらのルータは、ルータ C が含まれないルート アップデートを共有します。ルータ C は別の VRF で設定されているからです。

図 9-1　　ネットワーク内の VRF



Cisco NX-OS はデフォルトで、着信インターフェイスの VRF を使用して、ルート検索に使用するルーティング テーブルを選択します。ルート ポリシーを設定すると、この動作を変更し、Cisco NX-OS が着信パケットに使用する VRF を設定できます。

Cisco NX-OS は、VRF 間のルート リーク（インポートまたはエクスポート）を防止します。

VRF-Lite

VRF-Lite の機能によって、サービス プロバイダーは、VPN 間で重複した IP アドレスを使用できる複数の VPN をサポートできます。VRF-Lite は入力インターフェイスを使用して異なる VPN のルートを区別し、各 VRF に 1 つまたは複数のレイヤ 3 インターフェイスを対応付けて仮想パケット転送テーブルを形成します。VRF のインターフェイスは、イーサネット ポートなどの物理インターフェイス、または VLAN SVI などの論理インターフェイスにすることができますが、レイヤ 3 インターフェイスは、一度に複数の VRF に属することはできません。

（注）　VRF-Lite の実装では、マルチプロトコル ラベル スイッチング（MPLS）および MPLS コントロール プレーンはサポートされません。

（注）　VRF-Lite インターフェイスは、レイヤ 3 インターフェイスである必要があります。

VRF 認識サービス

Cisco NX-OS アーキテクチャの基本的な特徴として、すべての IP ベースの機能が VRF を認識することがあげられます。

次の VRF 認識サービスは、特定の VRF を選択することによって、リモート サーバに接続したり、選択した VRF に基づいて情報をフィルタリングすることができます。

- AAA：詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- Call Home：詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- HSRP：詳細については、第 12 章「HSRP の設定」を参照してください。
- HTTP：詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2*』を参照してください。
- Licensing：詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。
- NTP：詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- RADIUS：詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- ping および traceroute：詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2*』を参照してください。
- SSH：詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2*』を参照してください。
- SNMP：詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- Syslog：詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- TACACS+：詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。
- TFTP：詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2*』を参照してください。
- VRRP：詳細については、第 13 章「VRRP の設定」を参照してください。

各サービスで VRF サポートを設定する詳細については、各サービスの適切なコンフィギュレーション ガイドを参照してください。

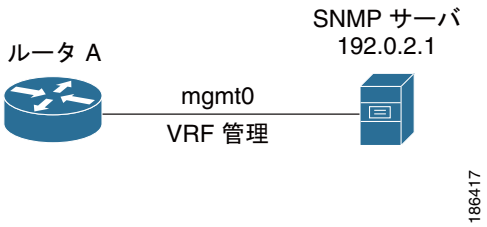
ここで説明する内容は、次のとおりです。

到達可能性

到達可能性は、サービスを提供するサーバに到達するために必要なルーティング情報がどの VRF にあるかを示します。たとえば、管理 VRF で到達可能な SNMP サーバを設定できます。ルータ上でサーバ アドレスを設定する場合は、サーバに到達するために Cisco NX-OS が使用しなければならない VRF も設定します。

図 9-2 に、管理 VRF を介して到達できる SNMP サーバを示します。SNMP サーバ ホスト 192.0.2.1 には管理 VRF を使用するように、ルータ A を設定します。

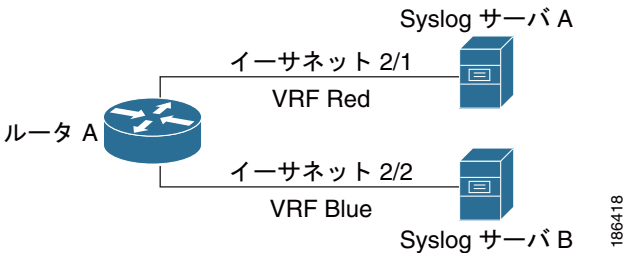
図 9-2　サービス VRF の到達可能性



フィルタリング

フィルタリングによって、VRF に基づいて VRF 認識サービスに渡す情報のタイプを制限できます。たとえば、Syslog サーバが特定の VRF をサポートするように設定できます。図 9-3 に示す 2 つの Syslog サーバは、それぞれ 1 つの VRF をサポートしています。Syslog サーバ A は VRF Red で設定されているので、Cisco NX-OS は VRF Red で生成されたシステム メッセージだけを Syslog サーバ A に送信します。

図 9-3　サービス VRF のフィルタリング

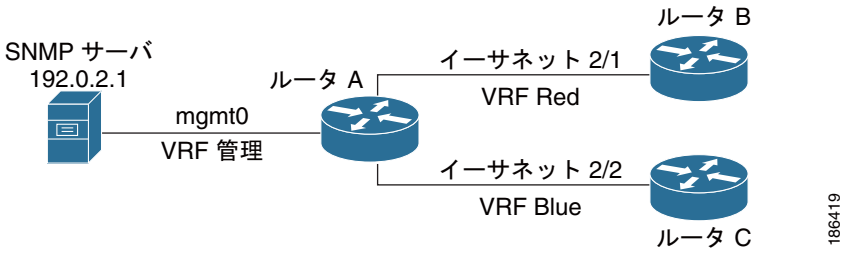


到達可能性とフィルタリングの組み合わせ

VRF 認識サービスの到達可能性とフィルタリングを組み合わせることができます。そのサービスに接続するために Cisco NX-OS が使用する VRF とともに、サービスがサポートする VRF も設定できます。デフォルト VRF でサービスを設定する場合は、任意で、すべての VRF をサポートするようにサービスを設定できます。

図 9-4 に、管理 VRF 上で到達できる SNMP サーバを示します。たとえば、SNMP サーバが VRF Red からの SNMP 通知だけをサポートするように設定できます。

図 9-4　サービス VRF の到達可能性とフィルタリング



VRF のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	VRF にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。 **（注）** NX-OS 基本ライセンスではデフォルトの VRF を使用でき、mgmt0 ポートには管理 VRF を使用できます。2 つのデフォルト VRF が自動的に作成されます。VRF-lite では追加 VRF を作成できます。追加 VRF は、レイヤ 3 LAN エンタープライズ ライセンスが必要です。

注意事項および制約事項

VRF 設定時の注意事項と制約事項は次のとおりです。

- インターフェイスを既存の VRF のメンバにすると、Cisco NX-OS はあらゆるレイヤ 3 設定を削除します。VRF にインターフェイスを追加したあとで、すべてのレイヤ 3 パラメータを設定する必要があります。
- 管理 VRF に mgmt0 インターフェイスを追加し、そのあとで mgmt0 の IP アドレスおよびその他のパラメータを設定します。
- VRF が存在しないうちに VRF のインターフェイスを設定した場合は、VRF を作成するまで、そのインターフェイスは運用上のダウンになります。
- Cisco NX-OS はデフォルトで、デフォルト VRF および管理 VRF を作成します。mgmt0 は管理 VRF のメンバにする必要があります。
- **write erase boot** コマンドを実行しても、管理 VRF 設定は削除されません。**write erase** コマンドを使用してから **write erase boot** コマンドを使用する必要があります。

VRF-lite には、次の注意事項と制限事項があります。

- VRF-lite を備えたスイッチは、各 VRF に対してそれぞれ、グローバル ルーティング テーブルとは異なる IP ルーティング テーブルを持ちます。

- VRF-lite が異なる VRF テーブルを使用するため、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- VRF-lite では、一部の MPLS-VRF 機能（ラベル交換、LDP の隣接関係、またはラベル付きパケット）がサポートされていません。
- 複数の仮想レイヤ 3 インターフェイスを VRF-lite スイッチに接続できます。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- レイヤ 3 TCAM リソースは、すべての VRF 間で共有されます。各 VRF が十分な CAM 領域を持つようにするには、**maximum routes** コマンドを使用します。
- VRF を使用したスイッチは、1 つのグローバル ネットワークと最大 64 の VRF をサポートできます。サポートされるルートの総数は、TCAM のサイズに制限されます。
- VRF-lite は、BGP、RIP、スタティック ルーティング、EIGRP、OSPF をサポートします。
- VRF-Lite は、パケット スイッチング レートに影響しません。
- マルチキャストを同時に同一のレイヤ 3 インターフェイス上に設定することはできません。
- VRF-lite は IPv4 ネットワーク上でのみサポートされます。

デフォルト設定

表 9-1 に、VRF パラメータのデフォルト設定を示します。

表 9-1　デフォルトの VRF パラメータ

パラメータ	デフォルト
設定されている VRF	デフォルト、管理
ルーティング コンテキスト	デフォルト VRF

VRF の設定

ここで説明する内容は、次のとおりです。

- 「VRF の作成」（P.9-6）
- 「インターフェイスへの VRF メンバシップの割り当て」（P.9-8）
- 「ルーティング プロトコルに関する VRF パラメータの設定」（P.9-9）
- 「VRF 認識サービスの設定」（P.9-11）
- 「VRF スコープの設定」（P.9-12）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

VRF の作成

スイッチに VRF を作成できます。

手順の概要

1. **configure terminal**
2. **vrf context** *name*
3. **ip route** {*ip-prefix* | *ip-addr ip-mask*} {[*next-hop* | *nh-prefix*] | [*interface next-hop* | *nh-prefix*]} [**tag** *tag-value* [*pref*]]
4. （任意）**show vrf** [*vrf-name*]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *name* **Example:** switch(config)# vrf context Enterprise switch(config-vrf)#	新しい VRF を作成し、VRF コンフィギュレーション モードを開始します。*name* には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 3	**ip route** {*ip-prefix* | *ip-addr ip-mask*} {[*next-hop* | *nh-prefix*] | [*interface next-hop* | *nh-prefix*]} [**tag** *tag-value* [*pref*] **Example:** switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクスト ホップ アドレスを設定できます。*preference* 値でアドミニストレーティブ ディスタンスを設定します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。
ステップ 4	**show vrf** [*vrf-name*] **Example:** switch(config-vrf)# show vrf Enterprise	（任意）VRF 情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

VRF および関連する設定を削除するには、**no vrf context** コマンドを使用します。

コマンド	目的
no vrf context *name* **Example:** switch(config)# no vrf context Enterprise	VRF および関連するすべての設定を削除します。

グローバル コンフィギュレーション モードで使用できるコマンドはすべて、VRF コンフィギュレーション モードでも使用できます。

次に、VRF を作成し、VRF にスタティック ルートを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2
switch(config-vrf)# exit
switch(config)# copy running-config startup-config
```

インターフェイスへの VRF メンバシップの割り当て

インターフェイスを VRF のメンバにできます。

はじめる前に

VRF 用のインターフェイスを設定したあとで、インターフェイスに IP アドレスを割り当てます。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrf member** *vrf-name*
5. **ip-address** *ip-prefix/length*
6. （任意）**show vrf** *vrf-name* **interface** *interface-type number*
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。

	コマンド	目的
ステップ 5	**ip address** *ip-prefix/length* **Example:** switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 6	**show vrf** *vrf-name* **interface** *interface-type number* **Example:** switch(config-vrf)# show vrf Enterprise interface ethernet 1/2	（任意）VRF 情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# copy running-config startup-config
```

ルーティング プロトコルに関する VRF パラメータの設定

1 つまたは複数の VRF にルーティング プロトコルを関連付けることができます。ルーティング プロトコルに関する VRF の設定については、該当する章を参照してください。ここでは、詳細な設定手順の例として、OSPFv2 プロトコルを使用します。

手順の概要

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **vrf** *vrf-name*
4. （任意）**maximum-paths** *paths*
5. **interface** *interface-type slot/port*
6. **no switchport**
7. **vrf member** *vrf-name*
8. **ip address** *ip-prefix/length*
9. **ip router ospf** i*nstance-tag* **area** *area-id*
10. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *instance-tag* **Example:** switch(config-vrf)# router ospf 201 switch(config-router)#	新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。
ステップ 3	**vrf** *vrf-name* **Example:** switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	VRF 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	**maximum-paths** *paths* Example: switch(config-router-vrf)# maximum-paths 4	（任意）この VRF のルート テーブル内の宛先への、同じ OSPFv2 パスの最大数を設定します。ロード バランシングに使用されます。
ステップ 5	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	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 6	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 7	**vrf member** *vrf-name* **Example:** switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 8	**ip address** *ip-prefix/length* **Example:** switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 9	**ip router ospf** *instance-tag* **area** *area-id* **Example:** switch(config-if)# ip router ospf 201 area 0	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 10	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
```

```
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# exit
switch(config)# router ospf 201
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)# maximum-paths 4
switch(config-router-vrf)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config-if)# exit
switch(config)# copy running-config startup-config
```

VRF 認識サービスの設定

VRF 認識サービスの到達可能性およびフィルタリングを設定できます。VRF 用サービスの設定手順を扱っている、該当する章またはコンフィギュレーション ガイドへのリンクについては、「VRF 認識サービス」（P.9-3）を参照してください。ここでは、サービスの詳細な設定手順の例として、SNMP および IP ドメイン リストを使用します。

手順の概要

1. **configure terminal**
2. **snmp-server host** *ip-address* [**filter_vrf** *vrf-name*] [**use-vrf** *vrf-name*]
3. **vrf context** [*vrf-name*]
4. **ip domain-list** *domain-name* [**all-vrfs**][**use-vrf** *vrf-name*]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *ip-address* [**filter-vrf** *vrf-name*] [**use-vrf** *vrf-name*] **Example:** switch(config)# snmp-server host 192.0.2.1 use-vrf Red switch(config-vrf)#	グローバル SNMP サーバを設定し、サービスに接続するために Cisco NX-OS が使用する VRF を設定します。選択した VRF からこのサーバへの情報をフィルタリングするには、**filter-vrf** キーワードを使用します。
ステップ 3	**vrf context** *vrf-name* **Example:** switch(config)# vrf context Blue switch(config-vrf)#	新しい VRF を作成します。

	コマンド	目的
ステップ 4	**ip domain-list** *domain-name* [**all-vrfs**][**use-vrf** *vrf-name*] **Example:** switch(config-vrf)# ip domain-list List all-vrfs use-vrf Blue switch(config-vrf)#	VRF でドメイン リストを設定し、さらに任意で、指定されたドメイン名に接続するために Cisco NX-OS が使用する VRF を設定します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、VRF Red で到達可能な SNMP ホスト 192.0.2.1 に、すべての VRF の SNMP 情報を送信する例を示します。

```
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 for-all-vrfs use-vrf Red
switch(config)# copy running-config startup-config
```

次に、VRF Red で到達可能な SNMP ホスト 192.0.2.12 に対して、VRF Blue の SNMP 情報をフィルタリングする例を示します。

```
switch# configure terminal
switch(config)# vrf definition Blue
switch(config-vrf)# snmp-server host 192.0.2.12 use-vrf Red
switch(config)# copy running-config startup-config
```

VRF スコープの設定

すべての EXEC コマンド（**show** コマンドなど）に対応する VRF スコープを設定できます。VRF スコープを設定すると、EXEC コマンド出力のスコープが設定された VRF に自動的に限定されます。このスコープは、一部の EXEC コマンドで使用できる VRF キーワードによって上書きできます。

VRF スコープを設定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
routing-context vrf *vrf-name* **Example:** switch# routing-context vrf red switch%red#	すべての EXEC コマンドに対応するルーティング コンテキストを設定します。デフォルトのルーティング コンテキストはデフォルト VRF です。

デフォルトの VRF スコープに戻すには、EXEC モードで次のコマンドを使用します。

コマンド	目的
routing-context vrf default **Example:** switch%red# routing-context vrf default switch#	デフォルトのルーティング コンテキストを設定します。

VRF コンフィギュレーションの確認

VRF の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show vrf [*vrf-name*]	すべてまたは 1 つの VRF の情報を表示します。
show vrf [*vrf-name*] **detail**	すべてまたは 1 つの VRF の詳細情報を表示します。
show vrf [*vrf-name*] [**interface** ***interface-type slot/port***]	インターフェイスの VRF ステータスを表示します。

設定：VRF の例

次に、VRF Red を設定し、その VRF に SNMP サーバを追加し、VRF Red に OSPF インスタンスを追加する例を示します。

```
configure terminal
vrf context Red
 snmp-server host 192.0.2.12 use-vrf Red
router ospf 201
interface ethernet 1/2
 no switchport
 vrf member Red
 ip address 192.0.2.1/16
 ip router ospf 201 area 0
```

次に、VRF Red および Blue を設定し、各 VRF に OSPF インスタンスを追加し、各 OSPF インスタンスの SNMP コンテキストを作成する例を示します。

```
configure terminal
!Create the VRFs
vrf context Red
vrf context Blue
!Create the OSPF instances and associate them with each VRF
feature ospf
router ospf Lab
 vrf Red
router ospf Production
 vrf Blue
!Configure one interface to use ospf Lab on VRF Red
interface ethernet 1/2
 no switchport
 vrf member Red
 ip address 192.0.2.1/16
 ip router ospf Lab area 0
 no shutdown
!Configure another interface to use ospf Production on VRF Blue
interface ethernet 10/2
 no switchport
 vrf member Blue
 ip address 192.0.2.1/16
 ip router ospf Production area 0
 no shutdown
!configure the SNMP server
snmp-server user admin network-admin auth md5 nbv-12345
snmp-server community public ro
```

```
!Create the SNMP contexts for each VRF
snmp-server context lab instance Lab vrf Red
snmp-server context production instance Production vrf Blue
```

この例で、VRF Red の OSPF インスタンス Lab の OSPF-MIB 値にアクセスするには、SNMP コンテキスト **lab** を使用します。

関連資料

VRF の詳細については、次の項目を参照してください。

- *『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 4.2』*
- *『Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)』*

その他の関連資料

仮想化の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.9-14）
- 「標準」（P.9-14）

関連資料

関連項目	マニュアル名
VRF CLI	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

VRF 機能の履歴

表 9-2 は、この機能のリリースの履歴です。

表 9-2　VRF 機能の履歴

機能名	リリース	機能情報
VRF	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 10

ユニキャスト RIB および FIB の管理

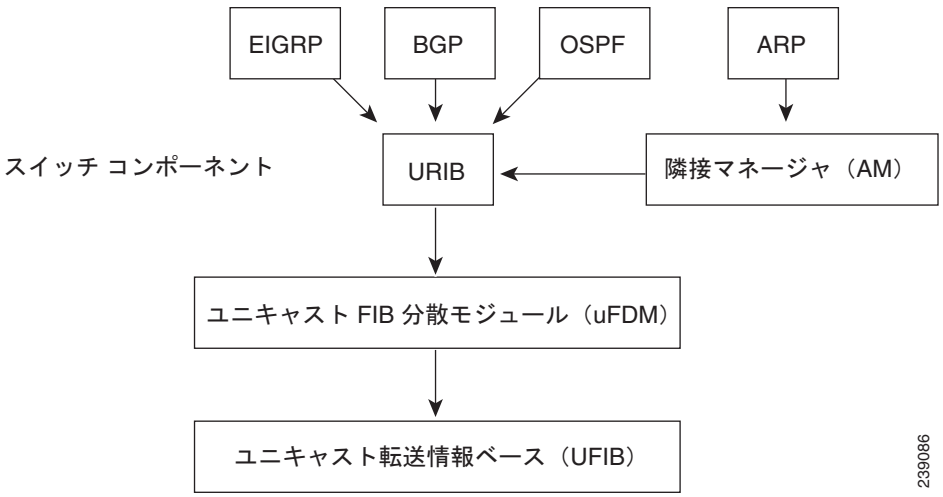
この章では、Cisco NX-OS スイッチのユニキャスト Routing Information Base（RIB; ルーティング情報ベース）および Forwarding Information Base（FIB; 転送情報ベース）のルートを管理する方法について説明します。

この章では、次の内容について説明します。

ユニキャスト RIB および FIB について

ユニキャスト RIB（IPv4 RIB）および FIB は、図 10-1 に示すように、Cisco NX-OS の転送アーキテクチャの一部です。

図 10-1　Cisco NX-OS 転送アーキテクチャ



ユニキャスト RIB は、直接接続のルート、スタティック ルート、ダイナミック ユニキャスト ルーティング プロトコルで検出されたルートを含むルーティング テーブルを維持しています。また、アドレス解決プロトコル（ARP）などの送信元から、隣接情報を収集します。ユニキャスト RIB は、ルートに最適なネクスト ホップを決定し、さらにユニキャスト FIB Distribution Module（FDM; FIB 分散モジュール）のサービスを使用して、ユニキャスト Forwarding Information Base（FIB; 転送情報ベース）にデータを入力します。

各ダイナミック ルーティング プロトコルは、タイム アウトしたあらゆるルートについて、ユニキャスト RIB を更新する必要があります。そのあと、ユニキャスト RIB はそのルートを削除し、そのルートに最適なネクストホップを再計算します（代わりに使用できるパスがある場合）。

ここでは、次の内容について説明します。

レイヤ 3 整合性チェッカー

まれな状況において、各モジュールのユニキャスト RIB と FIB の間に不整合が発生することがあります。Cisco NX-OS は、レイヤ 3 整合性チェッカーをサポートします。この機能は、各インターフェイス モジュールのユニキャスト IPv4 RIB と FIB の間の不整合を検出します。不整合には次のようなものがあります。

- 欠落したプレフィクス
- 余分なプレフィクス
- ネクストホップ アドレスの誤り
- ARP またはネイバー探索（ND）キャッシュ内の不正なレイヤ 2 リライト文字列

レイヤ 3 整合性チェッカーは、FIB のエントリと Adjacency Manager（AM; 隣接マネージャ）から取得した最新の隣接情報を比較し、不整合があれば記録します。次に整合性チェッカーは、ユニキャスト RIB のプレフィクスをモジュールの FIB と比較し、不整合があればログに記録します。「レイヤ 3 整合性チェッカーのトリガー」（P.10-6）を参照してください。

不整合は手動で解消できます。「FIB 内の転送情報の消去」（P.10-8）を参照してください。

FIB テーブル

ハードウェアは TCAM テーブルとハッシュ テーブルの 2 つのテーブルを提供します。TCAM テーブルは、Longest Prefix Match（LPM; 最長プレフィクス照合）ルートと /32 ユニキャスト ルートの間で共有されます。ハッシュ テーブルは /32 ユニキャスト エントリとマルチキャスト エントリの間で共有されます。各テーブルには約 8000 のルートがあります。

仮想化のサポート

ユニキャスト RIB および FIB は、Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング / 転送インスタンス）をサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

ユニキャスト RIB および FIB のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ユニキャスト RIB および FIB にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ユニキャスト RIB および FIB の管理

ここでは、次の内容について説明します。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

モジュールの FIB 情報の表示

スイッチの FIB 情報を表示できます。

手順の詳細

スイッチの FIB 情報を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip fib adjacency **Example:** `switch# show ip fib adjacency`	IPv4 の隣接情報を表示します。
show forwarding ipv4 adjacency **Example:** `switch# show forwarding ipv4 adjacency`	IPv4 の隣接情報を表示します。

コマンド	目的
show ip fib interfaces **Example:** switch# show ip fib interfaces	IPv4 の FIB インターフェイス情報を表示します。
show ip fib route **Example:** switch# show ip fib route	IPv4 のルート テーブルを表示します。
show forwarding ipv4 route **Example:** switch# show forwarding ipv4 route	IPv4 のルート テーブルを表示します。

次に、スイッチの FIB の内容を表示する例を示します。

```
switch# show ip fib route

IPv4 routes for table default/base

------------------+------------------+----------------------
Prefix            | Next-hop         | Interface
------------------+------------------+----------------------
0.0.0.0/32          Drop               Null0
255.255.255.255/32  Receive            sup-eth1
```

ユニキャスト FIB のロード シェアリングの設定

OSPF（Open Shortest Path First）などのダイナミック ルーティング プロトコルは、Equal-Cost Multipath（ECMP; 等コスト マルチパス）によるロード シェアリングをサポートしています。ルーティング プロトコルは、そのプロトコルに設定されたメトリックに基づいて最適なルートを決定し、そのプロトコルに設定された最大数までのパスをユニキャスト RIB に組み込みます。ユニキャスト RIB は、RIB に含まれるすべてのルーティング プロトコル パスのアドミニストレーティブ ディスタンスを比較し、ルーティング プロトコルによって組み込まれたすべてのパス セットから最適なパス セットを選択します。ユニキャスト RIB は、この最適なパス セットを FIB に組み込み、転送プレーンで使用できるようにします。

転送プレーンは、ロード シェアリングのアルゴリズムを使用して、FIB に組み込まれたパスのいずれかを選択し、それを特定のデータ パケットに使用します。

ロード シェアリングの次の設定項目をグローバルに設定できます。

- ロード シェアリング モード：宛先のアドレスとポート、または送信元と宛先のアドレスとポートに基づいて、最適なパスを選択します。
- 汎用 ID：ハッシュ アルゴリズムのランダム シードを設定します。汎用 ID を設定する必要はありません。ユーザが設定しなかった場合は、Cisco NX-OS が汎用 ID を選択します。

（注） ロード シェアリングでは、特定のフローに含まれるすべてのパケットに対して同じパスが使用されます。フローは、ユーザが設定したロード シェアリング方式によって定義されます。たとえば、送信元/宛先のロード シェアリングを設定すると、送信元 IP アドレスと宛先 IP アドレスのペアが同じであるすべてのパケットが同じパスをたどります。

ユニキャスト FIB のロード シェアリング アルゴリズムを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip load-sharing address {**destination port destination** | **source-destination** [**port source-destination**]} [**universal-id** *seed*] **Example:** `switch(config)# ip load-sharing address source-destination`	データ トラフィックに対するユニキャスト FIB のロード シェアリング アルゴリズムを設定します。*universal-id* の範囲は 1 ～ 4294967295 です。

ユニキャスト FIB のロード シェアリング アルゴリズムを表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip load-sharing **Example:** `switch(config)# show ip load-sharing`	データ トラフィックに対するユニキャスト FIB のロード シェアリング アルゴリズムを表示します。

ユニキャスト RIB および FIB が特定の送信元アドレス/宛先アドレスに使用するルートを表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show routing hash *source-addr dest-addr* [*source-port dest-port*] [**vrf** *vrf-name*] **Example:** `switch# show routing hash 192.0.2.1 10.0.0.1`	ユニキャスト RIB および FIB が特定の送信元/宛先アドレス ペアに使用するルートを表示します。送信元アドレスと宛先アドレスの形式は x.x.x.x です。送信元ポートと宛先ポートの範囲は 1 ～ 65535 です。VRF 名には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。

次に、特定の送信元/宛先ペアのために選択されたルートを表示する例を示します。

```
switch# show routing hash 10.0.0.5 30.0.0.2
  Load-share parameters used for software forwarding:
  load-share mode: address source-destination port source-destination
  Universal-id seed: 0xe05e2e85
  Hash for VRF "default"
  Hashing to path *20.0.0.2 (hash: 0x0e), for route:
```

ルーティング情報と隣接情報の表示

ルーティング情報と隣接情報を表示できます。

ルーティング情報と隣接情報を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show ip route [*route-type* | **interface** *int-type number* | **next-hop**] **Example:** switch# show ip route	ユニキャスト ルート テーブルを表示します。*route-type* 引数には、1 つのルート プレフィクス、direct、static、またはダイナミック ルーティング プロトコルを指定します。**?** コマンドを使用すると、サポートされているインターフェイスを表示できます。
show ip adjacency [*prefix* | *interface-type number* [**summary**]| **non-best**] [**detail**] [**vrf** *vrf-id*] **Example:** switch# show ip adjacency	隣接関係テーブルを表示します。引数の範囲は次のとおりです。 • *prefix*：任意の IPv4 プレフィクス アドレス。 • *interface-type number*：**?** コマンドを使用すると、サポートされているインターフェイスを表示できます。 • *vrf-id*：最大 32 文字の英数字文字列。大文字と小文字は区別されます。
show ip routing [*route-type* | **interface** *int-type number* | **next-hop** | **recursive-next-hop** | **summary** | **updated** {**since** | **until**} *time*] **Example:** switch# show routing summary	ユニキャスト ルート テーブルを表示します。*route-type* 引数には、1 つのルート プレフィクス、direct、static、またはダイナミック ルーティング プロトコルを指定します。**?** コマンドを使用すると、サポートされているインターフェイスを表示できます。

次に、ユニキャスト ルート テーブルを表示する例を示します。

```
switch# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

192.168.0.2/24, ubest/mbest: 1/0, attached
    *via 192.168.0.32, Eth1/5, [0/0], 22:34:09, direct
192.168.0.32/32, ubest/mbest: 1/0, attached
    *via 192.168.0.32, Eth1/5, [0/0], 22:34:09, local
```

次に、隣接情報を表示する例を示します。

```
switch# show ip adjacency

IP Adjacency Table for VRF default
Total number of entries: 2
Address         Age       MAC Address     Pref Source     Interface       Best
10.1.1.1        02:20:54  00e0.b06a.71eb  50   arp        mgmt0           Yes
10.1.1.253      00:06:27  0014.5e0b.81d1  50   arp        mgmt0           Yes
```

レイヤ 3 整合性チェッカーのトリガー

レイヤ 3 整合性チェッカーを手動でトリガーできます。

レイヤ 3 整合性チェッカーを手動でトリガーにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
test [**ipv4**] [**unicast] forwarding inconsistency** [**vrf** *vrf-name*] [**module** {*slot*| **all**}] **Example:** switch(config)# test forwarding inconsistency	レイヤ 3 整合性チェックを開始します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。*slot* の範囲は 1 ～ 10 です。

レイヤ 3 整合性チェッカーを停止するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
test forwarding [**ipv4**] [**unicast**] **inconsistency** [**vrf** *vrf-name*] [**module** {*slot*| **all**}] **stop** **Example:** switch(config)# test forwarding inconsistency stop	レイヤ 3 整合性チェックを停止します。*vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。*slot* の範囲は 1 ～ 10 です。

レイヤ 3 の不整合を表示するには、任意のモードで次のコマンドを使用します。

コマンド	目的
show forwarding [**ipv4**] **inconsistency** [**vrf** *vrf-name*] [**module** {*slot*| **all**}] **Example:** switch(config)# show forwarding inconsistency	レイヤ 3 整合性チェックの結果を表示します。*vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。*slot* の範囲は 1 ～ 10 です。

FIB 内の転送情報の消去

FIB 内の 1 つまたは複数のエントリを消去できます。FIB のエントリを消去しても、ユニキャスト RIB に影響はありません。

注意　**clear forwarding** コマンドを実行すると、スイッチ上の転送は中断されます。

FIB 内のエントリ（レイヤ 3 の不整合を含む）を消去するには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear forwarding {**ipv4**} **route** {* | *prefix*} [**vrf** *vrf-name*] [**module** {*slot*| **all**}] **Example:** `switch(config)# clear forwarding ipv4 route *`	FIB から 1 つまたは複数のエントリを消去します。ルートのオプションは次のとおりです。 • * : すべてのルート • *prefix* : 任意の IP プレフィクス。 *vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。*slot* の範囲は 1 ～ 10 です。

ルートのメモリ要件の見積もり

一連のルートおよびネクストホップ アドレスが使用するメモリを見積もることができます。

ルートのメモリ要件を見積もるには、任意のモードで次のコマンドを使用します。

コマンド	目的
show routing memory estimate routes *num-routes* **next-hops** *num-nexthops* **Example:** `switch# show routing memory estimate routes 1000 next-hops 1`	ルートのメモリ要件を表示します。*num-routes* の範囲は 1000 ～ 1000000 です。*num-nexthops* の範囲は 1 ～ 16 です。

ユニキャスト RIB 内のルートの消去

ユニキャスト RIB から 1 つまたは複数のルートを消去できます。

注意　***** キーワードはルーティングに破壊的な影響を与えます。

ユニキャスト RIB 内の 1 つまたは複数のエントリを消去するには、任意のモードで次のコマンドを使用します。

コマンド	目的
clear ip route {* | {*route* | *prefix/length*}[*next-hop interface*]} [**vrf** *vrf-name*] **Example:** `switch(config)# clear ip route 10.2.2.2`	ユニキャスト RIB とすべてのモジュール FIB から 1 つまたは複数のルートを消去します。ルートのオプションは次のとおりです。 • *****：すべてのルート • *route*：個々の IP ルート。 • *prefix/length*：任意の IP プレフィクス。 • *next-hop*：ネクストホップ アドレス • *interface*：ネクストホップ アドレスに到達するためのインターフェイス *vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
clear routing [**multicast** | **unicast**] [**ip** | **ipv4**] {* | {*route* | *prefix/length*}[*next-hop interface*]} [**vrf** *vrf-name*] **Example:** `switch(config)# clear routing ip 10.2.2.2`	ユニキャスト RIB から 1 つまたは複数のルートを消去します。ルートのオプションは次のとおりです。 • *****：すべてのルート • *route*：個々の IP ルート。 • *prefix/length*：任意の IP プレフィクス。 • *next-hop*：ネクストホップ アドレス • *interface*：ネクストホップ アドレスに到達するためのインターフェイス *vrf-name* には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。

ユニキャスト RIB および FIB の確認

ユニキャスト RIB および FIB の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show forwarding adjacency	モジュールの隣接関係テーブルを表示します。
show forwarding distribution {**clients** | **fib-state**}	FIB の分散情報を表示します。
show forwarding interfaces module *slot*	モジュールの FIB 情報を表示します。

コマンド	目的
show forwarding ipv4 route	FIB 内のルートを表示します。
show hardware forwarding dynamic-allocation status	TCAM 割り当てに関する情報を表示します。
show ip adjacency	隣接関係テーブルを表示します。
show ip route	ユニキャスト RIB から受け取った IPv4 ルートを表示します。
show routing	ユニキャスト RIB から受け取ったルートを表示します。

その他の関連資料

ユニキャスト RIB および FIB の管理に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.10-10）
- 「ユニキャスト RIB および FIB 機能の履歴」（P.10-10）

関連資料

関連項目	マニュアル名
ユニキャスト RIB および FIB の CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

ユニキャスト RIB および FIB 機能の履歴

表 10-1 は、この機能のリリースの履歴です。

表 10-1　ユニキャスト RIB および FIB 機能の履歴

機能名	リリース	機能情報
ユニキャスト RIB および FIB	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 11

Route Policy Manager の設定

ここでは、Cisco NX-OS スイッチで Route Policy Manager を設定する方法について説明します。

この章では、次の内容について説明します。

Route Policy Manager の概要

Route Policy Manager は、ルート マップおよび IP プレフィクス リストをサポートします。この機能は、ルート再配布に使用されます。プレフィクス リストには、1 つまたは複数の IPv4 ネットワーク プレフィクスおよび関連付けられたプレフィクス長の値を指定します。プレフィクス リストは、BGP（ボーダー ゲートウェイ プロトコル）テンプレート、ルート フィルタリング、またはルーティング ドメイン間で交換されるルートの再配布などの機能で、単独で使用できます。

ルート マップは、ルートおよび IP パケットの両方に適用できます。ルート フィルタリングおよび再配布は、ルート マップを使用してルートを渡します。

ここでは、次の内容について説明します。

プレフィクス リスト

プレフィクス リストを使用すると、アドレスまたはアドレス範囲を許可または拒否できます。プレフィクス リストによるフィルタリングでは、ルートまたはパケットのプレフィクスと、プレフィクス リストに指定されているプレフィクスの照合が行われます。特定のプレフィクスがプレフィクス リストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。

プレフィクス リストに複数のエントリを設定し、エントリと一致したプレフィクスを許可または拒否できます。各エントリにはシーケンス番号が関連付けられています。この番号はユーザが設定できます。シーケンス番号がユーザにより設定されていない場合、Cisco NX-OS によりシーケンス番号が自動設定されます。Cisco NX-OS はシーケンス番号が最も小さいエントリから順番にプレフィクス リストを評価します。Cisco NX-OS は指定されたプレフィクスと最初に一致するエントリを処理します。一致すると、Cisco NX-OS は許可または拒否文を処理し、残りのプレフィクス リストは評価しません。

（注）　プレフィクス リストが空の場合は、すべてのルートが許可されます。

MAC リスト

MAC リストを使用すると、MAC アドレスまたはアドレス範囲を許可または拒否できます。MAC リストは MAC アドレスとオプションの MAC マスクのリストです。MAC マスクはワイルドカード マスクで、ルート マップが MAC リストのエントリと一致すると論理的に MAC アドレスと AND 結合されます。MAC リストによるフィルタリングでは、パケットの MAC アドレスと MAC リスト内の MAC リストが照合されます。特定の MAC アドレスが MAC リストのどのエントリとも一致しなかった場合、実質的に拒否されたものと見なされます。

MAC リストに複数のエントリを設定し、エントリと一致した MAC アドレスを許可または拒否できます。各エントリにはシーケンス番号が関連付けられています。この番号はユーザが設定できます。シーケンス番号がユーザにより設定されていない場合、Cisco NX-OS によりシーケンス番号が自動設定されます。Cisco NX-OS はシーケンス番号が最も小さいエントリから順番に MAC リストを評価します。Cisco NX-OS は指定された MAC アドレスと最初に一致するエントリを処理します。一致すると、Cisco NX-OS は permit 文または deny 文を処理し、残りの MAC リストは評価しません。

ルート マップ

ルート マップは、ルートの再配布に使用できます。ルート マップ エントリは、一致基準および設定基準のリストからなります。一致基準では、着信ルートまたはパケットの一致条件を指定します。設定基準では、一致基準を満たした場合のアクションを指定します。

同じルート マップに複数のエントリを設定できます。これらのエントリには、同じルート マップ名を指定し、シーケンス番号で区別します。

一意のルート マップ名の下に 1 つまたは複数のルート マップ エントリをシーケンス番号に従って並べ、ルート マップを作成します。ルート マップ エントリのパラメータは、次のとおりです。

- シーケンス番号
- アクセス権：許可または拒否
- 一致基準
- 設定変更

ルート マップではデフォルトで、最小のシーケンス番号から順にルートまたは IP パケットが処理されます。**continue** 文を使用すると、次に処理するルート マップ エントリを決定できるので、別の順序で処理するようにルート マップを設定できます。

一致基準

さまざまな基準を使用して、ルート マップのルートまたは IP パケットを照合できます。BGP コミュニティ リストのように、特定のルーティング プロトコルだけに適用できる基準もありますが、IP 送信元または宛先アドレスなど、その他の基準はあらゆるルートまたは IP パケットに使用できます。

ルート マップに従ってルートまたはパケットを処理する場合、Cisco NX-OS は設定されている個々の match 文とルートまたはパケットを比較します。ルートまたはパケットが設定されている基準と一致した場合、Cisco NX-OS はルート マップ内で一致するエントリに対する許可または拒否設定、および設定されている設定基準に基づいて、このルートやパケットを処理します。

一致のカテゴリおよびパラメータは、次のとおりです。

- BGP パラメータ：AS 番号、AS パス、コミュニティ属性、または拡張コミュニティ属性に基づく一致。
- プレフィクス リスト：アドレスまたはアドレス範囲に基づく一致。
- マルチキャスト パラメータ：ランデブー ポイント、グループ、または送信元に基づく一致。
- その他のパラメータ：IP ネクストホップ アドレスまたはパケット長に基づく一致。

設定変更

ルートまたはパケットがルート マップ エントリと一致すると、設定した 1 つまたは複数の set 文に基づいて、そのルートまたはパケットを変更できます。

設定変更は次のとおりです。

- BGP パラメータ：AS パス、タグ、コミュニティ、拡張コミュニティ、ダンプニング、ローカル プリファレンス、オリジン、または重み値属性の変更。
- メトリック：ルート メトリック、ルート タグ、またはルート タイプの変更。
- その他のパラメータ：フォワーディング アドレスまたは IP ネクストホップ アドレスの変更。

アクセス リスト

IP アクセス リストでは、次のような IP パケット フィールドとパケットを照合できます。

- 送信元または宛先 IPv4 アドレス
- プロトコル
- 優先順位
- ToS

ACL の詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。

BGP の AS 番号

BGP ピアとの照合に使用する AS 番号のリストを設定できます。BGP ピアがリスト内の AS 番号と一致し、さらに他の BGP ピア設定と一致する場合、BGP はセッションを作成します。BGP ピアがリスト内の AS 番号と一致しない場合は、BGP はピアを無視します。AS 番号は AS 番号の範囲のリストとして設定できます。また、AS パス リストを使用して AS 番号を正規表現と比較することもできます。

BGP の AS パス リスト

AS パス リストを設定すると、着信または発信 BGP ルート アップデートをフィルタリングできます。ルート アップデートに AS パス リストのエントリと一致する AS パス属性が含まれている場合、ルータは設定されている許可または拒否条件に基づいてルートを処理します。ルート マップの中で AS パス リストを設定できます。

同じ AS パス リスト名を使用することによって、AS パス リストで複数の AS パス エントリを設定できます。ルータは最初に一致したエントリを処理します。

BGP のコミュニティ リスト

ルート マップのコミュニティ リストを使用すると、BGP コミュニティに基づいて BGP ルート アップデートをフィルタリングできます。コミュニティ属性はコミュニティ リストに基づいて照合できます。また、コミュニティ属性はルート マップを使用して設定できます。

コミュニティ リストには、1 つまたは複数のコミュニティ属性を指定します。同じコミュニティ リスト エントリに複数のコミュニティ属性を設定した場合、BGP ルートが一致と見なされるには、指定されたすべてのコミュニティ属性と一致しなければなりません。

同じコミュニティ リスト名を使用することによって、コミュニティ リストのそれぞれ個別のエントリとして、複数のコミュニティ属性を設定することもできます。この場合、ルータは最初に BGP ルートと一致したコミュニティ属性を、そのエントリの許可または拒否設定に基づいて処理します。

コミュニティ リストのコミュニティ属性は、次の形式のいずれか 1 つで設定できます。

- 名前付きコミュニティ属性（**internet**、**no-export** など）。
- *aa:nn* 形式（最初の 2 バイトは 2 バイトの AS 番号、最後の 2 バイトはユーザが定義するネットワーク番号を表します）。
- 正規表現。

正規表現の詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。

BGP の拡張コミュニティ リスト

拡張コミュニティ リストでは 4 バイトの AS 番号がサポートされています。拡張コミュニティ リストのコミュニティ属性は、次のいずれかの形式で設定できます。

- *aa4:nn* 形式（最初の 4 バイトは 4 バイトの AS 番号、最後の 2 バイトはユーザが定義するネットワーク番号を表します）。
- 正規表現。

正規表現の詳細については、『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』を参照してください。

Cisco NX-OS は汎用の特定拡張コミュニティ リストをサポートしています。このリストを使用すると、4 バイトの AS 番号に対して通常のコミュニティ リストと同様の機能を使用できます。汎用の特定拡張コミュニティ リストには次のプロパティを設定できます。

- Transitive：BGP はコミュニティ属性を自律システム間に伝達します。
- Nontransitive：BGP はコミュニティ属性を削除してからルートを他の自律システムに伝達します。

ルートの再配布およびルート マップ

ルート マップを使用すると、ルーティング ドメイン間でルートの再配布を制御できます。ルート マップではルートの属性を照合し、一致基準を満たすルートだけを再配布します。設定変更を使用することによって、再配布時に、ルート マップでルート属性を変更することもできます。

ルータは再配布されたルートを各ルート マップ エントリと照合します。match 文が複数ある場合は、ルートがすべての一致基準を満たしている必要があります。ルートがルート マップ エントリで定義されている一致基準を満たす場合は、エントリで定義されているアクションが実行されます。ルートが基準と一致しなかった場合、ルータは後続のルート マップ エントリとルートを比較します。ルートの処理は、ルートがルート マップのいずれかのエントリと一致するか、どのエントリとも一致せずすべてのエントリによる処理が完了するまで継続します。ルータがルート マップの全エントリとルートを比較しても一致しなかった場合、ルータはそのルートを受け付けるか（着信ルート マップ）またはルートを転送します（発信ルート マップ）。

Route Policy Manager のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	Route Policy Manager にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

注意事項および制約事項

Route Policy Manager 設定時の注意事項および制約事項は、次のとおりです。

- ルート マップが空の場合は、すべてのルートが拒否されます。
- プレフィクス リストが空の場合は、すべてのルートが許可されます。
- ルート マップ エントリに match 文がない場合、ルート マップ エントリのアクセス権（許可または拒否）によって、すべてのルートまたはパケットの処理結果が決まります。
- ルート マップ エントリの match 文の中で参照されたポリシー（プレフィクス リストなど）から no-match または deny-match が戻った場合、Cisco NX-OS は match 文を失敗として、次のルート マップ エントリを処理します。
- ルート マップを変更しても、ルート マップ コンフィギュレーション サブモードを終了するまでは、Cisco NX-OS によりすべての変更が保留されます。その後、Cisco NX-OS がすべての変更をプロトコル クライアントに送信すると、変更が有効になります。
- ルート マップは定義する前に使用できるので、設定変更を終えるときには、すべてのルート マップが存在していることを確認してください。

- 再配布およびフィルタリングを行う場合、ルート マップの使用状況を確認できます。各ルーティング プロトコルには、これらの統計情報を表示する機能があります。

デフォルト設定

表 11-1 に、Route Policy Manager のデフォルト設定を示します。

表 11-1　Route Policy Manager のデフォルト パラメータ

パラメータ	デフォルト
Route Policy Manager	イネーブル

Route Policy Manager の設定

Route Policy Manager の設定では、次の内容を扱います。

- 「IP プレフィクス リストの設定」（P.11-6）
- 「MAC リストの設定」（P.11-7）
- 「AS パス リストの設定」（P.11-8）
- 「コミュニティ リストの設定」（P.11-9）
- 「拡張コミュニティ リストの設定」（P.11-11）
- 「ルート マップの設定」（P.11-12）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

IP プレフィクス リストの設定

IP プレフィクス リストでは、プレフィクスおよびプレフィクス長のリストに対して IP パケットまたはルートを照合します。IPv4 の IP プレフィクス リストを作成できます。

指定したプレフィクス長と完全に一致するプレフィクス リスト エントリのみを対象とするよう設定できます。また、指定したプレフィクス長の範囲に該当するすべてのプレフィクスを対象とすることもできます。

ge キーワードと **lt** キーワードを使用すると、プレフィクス長の範囲を指定できます。着信パケットまたはルートがプレフィクス リストと一致すると判定されるのは、プレフィクスが一致する場合、およびプレフィクス長が **ge** キーワードの値（設定されている場合）以上で **lt** キーワードの値（設定されている場合）以下の場合です。

手順の概要

1. **configure terminal**
2. （任意）**ip prefix-list** *name* **description** *string*
3. **ip prefix-list** *name* [**seq** *number*] [{**permit** | **deny**} *prefix* {[**eq** *prefix-length*] | [**ge** *prefix-length*] [**le** *prefix-length*]}]

4. （任意）**show ip prefix-list** *name*
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip prefix-list** *name* **description** *string* **Example:** switch(config)# ip prefix-list AllowPrefix description allows engineering server	（任意）プレフィクス リストについての情報ストリングを追加します。
ステップ 3	**ip prefix-list** *name* [**seq** *number*] [{**permit** | **deny**} *prefix* {[**eq** *prefix-length*] | [**ge** *prefix-length*] [**le** *prefix-length*]}] **Example:** switch(config)# ip prefix-list AllowPrefix seq 10 permit 192.0.2.0 eq 24	IPv4 プレフィクス リストを作成するか、または既存のプレフィクス リストにプレフィクスを追加します。プレフィクス長の照合は次のように行われます。 • eq：*prefix length* の値と完全に一致するものが対象。 • ge：設定された *prefix length* 以上のプレフィクス長が対象。 • le：設定された *prefix length* 以下のプレフィクス長が対象。
ステップ 4	**show ip prefix-list** *name* **Example:** switch(config)# show ip prefix-list AllowPrefix	（任意）プレフィクス リスト情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、2 つのエントリからなる IPv4 プレフィクス リストを作成し、BGP ネイバーにプレフィクス リストを適用する例を示します。

```
switch# configure terminal
switch(config)# ip prefix-list allowprefix seq 10 permit 192.0.2.0/24 eq 24
switch(config)# ip prefix-list allowprefix seq 20 permit 209.165.201.0/27 eq 27
switch(config)# router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65535:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

MAC リストの設定

MAC リストを設定すると、特定の範囲の MAC アドレスを許可または拒否できます。

手順の概要

1. **configure terminal**
2. **mac-list** *name* [**seq** *number*] {**permit** | **deny**} *mac-address* [*mac-mask*]
3. （任意）**show mac-list** *name*
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**mac-list** *name* [**seq** *number*] {**permit** | **deny**} *mac-address* {mac-mask] **Example:** switch(config)# mac-list AllowMac seq 1 permit 0022.5579.a4c1 ffff.ffff.0000	MAC リストを作成するか、既存の MAC リストに MAC アドレスを追加します。*seq* の範囲は 1 ～ 4294967294 です。*mac-mask* は照合する MAC アドレスの部分を表し、MAC アドレス形式である必要があります。
ステップ 3	**show mac-list** *name* **Example:** switch(config)# show mac-list AllowMac	（任意）MAC リストの情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	（任意）この設定の変更を保存します。

AS パス リストの設定

発信および着信 BGP ルートの両方に、AS パス リスト フィルタを指定できます。各フィルタは、正規表現を使用するアクセス リストです。正規表現が ASCII ストリングとして表されたルートの AS パス属性と一致した場合は、許可または拒否条件が適用されます。

手順の概要

1. **configure terminal**
2. **ip as-path access-list** *name* {**deny** | **permit**} *expression*
3. （任意）**show ip as-path list** *name*
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip as-path access-list** *name* {**deny** | **permit**} *expression* **Example:** switch(config)# ip as-path access-list Allow40 permit 40	正規表現を使用して BGP AS パス リストを作成します。
ステップ 3	**show ip as-path-access-list** *name* **Example:** switch(config)# show ip as-path-access-list Allow40	（任意）AS パス アクセス リスト情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、2 つのエントリからなる AS パス リストを作成し、BGP ネイバーに AS パス リストを適用する例を示します。

```
switch# configure terminal
switch(config)# ip as-path access-list AllowAS permit 64510
switch(config)# ip as-path access-list AllowAS permit 64496
switch(config)# copy running-config startup-config
switch(config)# router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65535:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list AllowAS in
```

コミュニティ リストの設定

コミュニティ リストを使用すると、コミュニティ属性に基づいて BGP ルートをフィルタリングできます。コミュニティ番号は *aa:nn* 形式の 4 バイト値です。最初の 2 バイトは AS 番号を表し、最後の 2 バイトはユーザ定義のネットワーク番号です。

同じコミュニティ リスト文で複数の値を設定した場合、コミュニティ リスト フィルタを満足させるには、すべてのコミュニティ値が一致しなければなりません。複数の値をそれぞれ個別のコミュニティ リスト文で設定した場合は、最初に条件が一致したリストが処理されます。

コミュニティ リストを match 文で使用すると、コミュニティ属性に基づいて BGP ルートをフィルタリングできます。

手順の概要

1. **configure terminal**

2. **ip community-list standard** *list-name* {**deny** | **permit**} [*community-list*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]
   または
   ip community-list expanded *list-name* {**deny** | **permit**} *expression*
3. （任意）**show ip community-list** *name*
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip community-list standard** *list-name* {**deny** | **permit**} [*community-list*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] **Example:** switch(config)# ip community-list standard BGPCommunity permit no-advertise 65536:20	標準 BGP コミュニティ リストを作成します。*list-name* には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。*community-list* には、1 つ以上のコミュニティを *aa:nn* 形式で指定できます。
	ip community-list expanded *list-name* {**deny** | **permit**} *expression* **Example:** switch(config)# ip community-list expanded BGPComplex deny 50000:[0-9][0-9]_	正規表現を使用して拡張 BGP AS コミュニティ リストを作成します。
ステップ 3	**show ip community-list** *name* **Example:** switch(config)# show ip community-list BGPCommunity	（任意）コミュニティ リストの情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、2 つのエントリからなるコミュニティ リストの作成例を示します。

```
switch# configure terminal
switch(config)# ip community-list standard BGPCommunity permit no-advertise 65536:20
switch(config)# ip community-list standard BGPCommunity permit local-AS no-export
switch(config)# copy running-config startup-config
```

拡張コミュニティ リストの設定

拡張コミュニティ リストを使用すると、コミュニティ属性に基づいて BGP ルートをフィルタリングできます。コミュニティ番号は *aa4:nn* 形式の 6 バイト値です。最初の 4 バイトは AS 番号を表し、最後の 2 バイトはユーザ定義のネットワーク番号です。

同じ拡張コミュニティ リスト文で複数の値を設定した場合、拡張コミュニティ リスト フィルタの条件を満たすには、すべての拡張コミュニティ値が一致しなければなりません。複数の値をそれぞれ個別の拡張コミュニティ リスト文で設定した場合は、最初に条件が一致したリストが処理されます。

拡張コミュニティ リストを match 文で使用すると、拡張コミュニティ属性に基づいて BGP ルートをフィルタリングできます。

手順の概要

1. **configure terminal**
2. **ip extcommunity-list standard** *list-name* {**deny** | **permit**} **4bytegeneric** {**transitive** | **non-transitive**} *aa4:nn*
   または
   ip extcommunit-list expanded *list-name* {**deny** | **permit**} *expression*
3. （任意）**show ip extcommunity-list** *name*
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip extcommunity-list standard** *list-name* {**deny** | **permit**} **4bytegeneric** {**transitive** | **nontransitive**} *community1* [*community2...*] **Example:** switch(config)# ip extcommunity-list standard BGPExtCommunity permit 4bytegeneric transitive 65536:20	標準 BGP 拡張コミュニティ リストを作成します。*community* には、1 つ以上の拡張コミュニティを *aa4:nn* 形式で指定できます。
	ip extcommunity-list expanded *list-name* {**deny** | **permit**} *expression* **Example:** switch(config)# ip extcommunity-list expanded BGPExtComplex deny 1.5:[0-9][0-9]_	正規表現を使用して拡張 BGP 拡張コミュニティ リストを作成します。

	コマンド	目的
ステップ 3	**show ip community-list** *name* **Example:** switch(config)# show ip community-list BGPCommunity	（任意）拡張コミュニティ リストの情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、汎用の特定拡張コミュニティ リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip extcommunity-list standard test1 permit 4bytegeneric transitive
65536:40 65536:60
switch(config)# copy running-config startup-config
```

ルート マップの設定

ルート マップは、ルートの再配布またはルート フィルタリングに使用できます。ルート マップには、複数の一致基準と複数の設定基準を含めることができます。

BGP にルート マップを設定すると、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュのトリガーになります。

手順の概要

1. **configure terminal**
2. **route-map** *map-name* [**permit** | **deny**] [*seq*]
3. （任意）**continue** *seq*
4. （任意）**exit**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**route-map** *map-name* [**permit** | **deny**] [*seq*] **Example:** switch(config)# route-map Testmap permit 10 switch(config-route-map)#	ルート マップを作成するか、または既存のルート マップに対応するルート マップ コンフィギュレーション モードを開始します。*seq* を使用して、ルート マップ エントリを順序付けます。

	コマンド	目的
ステップ 3	**continue** *seq* **Example:** switch(config-route-map)# continue 10	（任意）ルート マップで次を処理するシーケンス文を決定します。使用するのは、フィルタリングおよび再配布の場合だけです。
ステップ 4	**exit** **Example:** switch(config-route-map)# exit	（任意）ルート マップ コンフィギュレーション モードを終了します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

ルート マップ コンフィギュレーション モードで、オプションとして、ルート マップに次の match パラメータを設定できます。

（注）　**default-information originate** コマンドでは、オプションのルート マップの **match** 文は無視されます。

コマンド	目的
match as-path *name* [*name...*] **Example:** switch(config-route-map)# match as-path Allow40	1 つまたは複数の AS パス リストと照合。AS パス リストは、**ip as-path access-list** コマンドで作成します。
match as-number {*number* [*,number...*] | **as-path-list** *name* [*name...*]} **Example:** switch(config-route-map)# match as-number 33,50-60	1 つまたは複数の AS 番号または AS パス リストと照合。AS パス リストは、**ip as-path access-list** コマンドで作成します。指定できる範囲は 1 ～ 65535 です。AS パス リスト名には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
match community *name* [*name...*][***exact-match***] **Example:** switch(config-route-map)# match community BGPCommunity	1 つまたは複数のコミュニティ リストと照合。コミュニティ リストは、**ip community-list** コマンドで作成します。
match extcommunity *name* [*name...*][***exact-match***] **Example:** switch(config-route-map)# match extcommunity BGPextCommunity	1 つまたは複数の拡張コミュニティ リストと照合。コミュニティ リストは、**ip extcommunity-list** コマンドで作成します。
match interface *interface-type number* [*interface-type number...*] **Example:** switch(config-route-map)# match interface e 1/2	設定済みのインターフェイスのいずれかからのネクストホップと照合。**?** を使用すると、サポートされているインターフェイスの種類のリストを検索できます。

コマンド	目的
match ip address prefix-list *name* [*name...*] **Example:** switch(config-route-map)# match ip address prefix-list AllowPrefix	1 つまたは複数の IPv4 プレフィクス リストと照合。プレフィクス リストは **ip prefix-list** コマンドを使用して作成します。
match ip multicast [**source** *ipsource*] [[**group** *ipgroup*] [*rp iprp*]] **Example:** switch(config-route-map)# match ip multicast rp 192.0.2.1	マルチキャスト送信元、グループ、またはランデブー ポイントに基づいて IPv4 マルチキャスト パケットを照合。
match ip next-hop prefix-list *name* [*name...*] **Example:** switch(config-route-map)# match ip next-hop prefix-list AllowPrefix	1 つまたは複数の IP プレフィクス リストに対して、ルートの IPv4 ネクストホップ アドレスを照合。プレフィクス リストは **ip prefix-list** コマンドを使用して作成します。
match ip route-source prefix-list *name* [*name...*] **Example:** switch(config-route-map)# match ip route-source prefix-list AllowPrefix	1 つまたは複数の IP プレフィクス リストに対して、ルートの IPv4 ルート送信元アドレスを照合。プレフィクス リストは **ip prefix-list** コマンドを使用して作成します。
match mac-list *name* [*name...*] **Example:** switch(config-route-map)# match mac-list AllowMAC	1 つまたは複数の MAC リストと照合。MAC リストは **mac-list** コマンドを使用して作成します。
match metric *value* [**+-** *deviation.*] [*value..*] **Example:** switch(config-route-map)# match mac-list AllowMAC	ルート メトリック値を 1 つまたは複数のメトリック値または値の範囲と照合。メトリック範囲は +-*deviation* 引数を使用して設定します。ルート マップは次の範囲に該当するすべてのルート メトリックと照合されます。 *value - deviation* ～ *value + deviation*。
match route-type *route-type* **Example:** switch(config-route-map)# match route-type level 1 level 2	ルート タイプと照合。*route-type* は、次のうちの 1 つまたは複数にできます。 • external • internal • level-1 • level-2 • local • nssa-external • type-1 • type-2

コマンド	目的
match tag *tagid* [*tagid...*] **Example:** switch(config-route-map)# match tag 2	フィルタリングまたは再配布に関する 1 つまたは複数のタグとルートを照合。
match vlan *vlan-id* [*vlan-range*] **Example:** switch(config-route-map)# match vlan 3, 5-10	VLAN と照合。

ルート マップ コンフィギュレーション モードで、オプションとして、ルート マップに次の set パラメータを設定できます。

コマンド	目的
set as-path {**tag** | **prepend** {**last-as** *number* | *as-1* [*as-2...*]}} **Example:** switch(config-route-map)# set as-path prepend 10 100 110	BGP ルートの AS パス属性を変更します。最後の AS 番号として設定された *number* または特定の AS パス値としてのストリング（*as-1 as-2...as-n*）をプリペンドできます。
set comm-list *name* **delete** **Example:** switch(config-route-map)# set comm-list BGPCommunity delete	着信または発信 BGP ルート アップデートのコミュニティ属性から、コミュニティを削除します。コミュニティ リストは **ip community-list** コマンドを使用して作成します。
set community {**none** | **additive** | **local-AS** | **no-advertise** | **no-export** | *community-1* [community-2...]} **Example:** switch(config-route-map)# set community local-AS	BGP ルート アップデートのコミュニティ属性を設定します。 **（注）** ルート マップ属性の同じシーケンスで、**set community** コマンドと **set comm-list delete** コマンドを両方使用すると、設定処理より先に削除処理が実行されます。 **（注）** **send-community** コマンドを BGP ネイバー アドレス ファミリ コンフィギュレーション モードで使用して、BGP コミュニティ属性を BGP ピアにプロパゲートします。
set dampening *halflife reuse suppress duration* **Example:** switch(config-route-map)# set dampening 30 1500 10000 120	BGP ルート ダンプニング パラメータを設定します。 • *halflife* : 指定できる範囲は 1 ～ 45 分です。デフォルトは 15 です。 • *reuse* : 指定できる範囲は 1 ～ 20000 秒です。デフォルトは 750 です。 • *suppress* : 指定できる範囲は 1 ～ 20000 です。デフォルトは 2000 です。 • *duration* : 指定できる範囲は 1 ～ 255 分です。デフォルトは 60 です。

コマンド	目的
set extcomm-list *name* **delete** **Example:** switch(config-route-map)# set extcomm-list BGPextCommunity delete	着信または発信 BGP ルート アップデートの拡張コミュニティ属性から、コミュニティを削除します。拡張コミュニティ リストは **ip extcommunity-list** コマンドを使用して作成します。
set extcommunity generic {**transitive** | **nontransitive**} {**none** | **additive**] *community-1* [community-2...]} **Example:** switch(config-route-map)# set extcommunity generic transitive 1.0:30	BGP ルート アップデートの拡張コミュニティ属性を設定します。 **（注）** ルート マップ属性の同じシーケンスで、**set extcommunity** コマンドと **set extcomm-list delete** コマンドを両方使用すると、設定処理より先に削除処理が実行されます。 **（注）** BGP 拡張コミュニティ属性を BGP ピアに伝達するには、BGP ネイバー アドレス ファミリ コンフィギュレーション モードで **send-community** コマンドを使用します。
set forwarding-address **Example:** switch(config-route-map)# set forwarding-address	OSPF のフォワーディング アドレスを設定します。
set level {**backbone** | **level-1** | **level-1-2** | **level-2**} **Example:** switch(config-route-map)# set level backbone	IS-IS 用にルートをインポートするエリアを設定します。IS-IS のオプションは level-1、level-1-2、または level-2 です。デフォルトは level-1 です。
set local-preference *value* **Example:** switch(config-route-map)# set local-preference 4000	BGP ローカル プリファレンス値を設定します。指定できる範囲は 0 ～ 4294967295 です。
set metric [**+** | **-**]*bandwidth-metric* **Example:** switch(config-route-map)# set metric +100	既存のメトリック値を増減します。メトリックは Kb/s 単位です。指定できる範囲は 0 ～ 4294967295 です。
set metric *bandwidth* [*delay reliability load mtu*] **Example:** switch(config-route-map)# set metric 33 44 100 200 1500	ルート メトリック値を設定します。 メトリックは次のとおりです。 • *metric0*：帯域幅（kbps）。指定できる範囲は 0 ～ 4294967295 です。 • *metric1*：遅延（10 マイクロ秒単位）。 • *metric2*：信頼性。指定できる範囲は 0 ～ 255（100% の信頼性）です。 • *metric3*：ロード。指定できる範囲は 1 ～ 200（100% のロード）です。 • *metric4*：パスの MTU。指定できる範囲は 1 ～ 4294967295 です。

コマンド	目的
set metric-type {**external** | **internal** | **type-1** | **type-2**} **Example:** switch(config-route-map)# set metric-type internal	宛先ルーティング プロトコルのメトリック タイプを設定します。オプションは次のとおりです。 external：IS-IS 外部メトリック internal：BGP の MED として IGP メトリックを使用 type-1：OSPF 外部タイプ 1 メトリック type-2：OSPF 外部タイプ 2 メトリック
set origin {**egp** *as-number* | **igp** | **incomplete**} **Example:** switch(config-route-map)# set origin incomplete	BGP オリジン属性を設定します。EGP *as-number* の範囲は 0 ～ 65535 です。
set tag *name* **Example:** switch(config-route-map)# set tag 33	宛先ルーティング プロトコルのタグ値を設定します。*name* パラメータは符号なし整数です。
set weight *count* **Example:** switch(config-route-map)# set weight 33	BGP ルートの重み値を設定します。指定できる範囲は 0 ～ 65535 です。

set metric-type internal コマンドは発信ポリシーおよび eBGP ネイバーのみに作用します。同じ BGP ピア発信ポリシーに **metric** コマンドと **metric-type internal** コマンドを両方設定した場合、Cisco NX-OS は **metric-type internal** コマンドを無視します。

Route Policy Manager の設定確認

Route Policy Manager の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip community-list [*name*]	コミュニティ リストの情報を表示します。
show ip extcommunity-list [*name*]	拡張コミュニティ リストの情報を表示します。
show [**ip**] **prefix-list** [*name*]	IPv4 プレフィクス リストの情報を表示します。
show route-map [*name*]	ルート マップの情報を表示します。

Route Policy Manager の設定例

次に、アドレス ファミリを使用して BGP を設定し、ネイバー 209.0.2.1 からのユニキャストおよびマルチキャスト ルートがアクセス リスト 1 と一致した場合に、受け付けられるようにする例を示します。

```
router bgp 64496
  address-family ipv4 unicast
    network 192.0.2.0/24
    network 209.165.201.0/27 route-map filterBGP
```

```
route-map filterBGP
 match ip next-hop prefix-list AllowPrefix
ip prefix-list AllowPrefix 10 permit 192.0.2.0 eq 24
ip prefix-list AllowPrefix 20 permit 209.165.201.0 eq 27
```

関連資料

Route Policy Manager の詳細については、次の項目を参照してください。

- 第 5 章「ベーシック BGP の設定」

その他の関連資料

IP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.11-18）
- 「標準」（P.11-18）

関連資料

関連項目	マニュアル名
Route Policy Manager CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

Route Policy Manager の機能の履歴

表 11-2 は、この機能のリリースの履歴です。

表 11-2　BGP 機能の履歴

機能名	リリース	機能情報
Route Policy Manager	5.0(3)N1(1)	この機能が導入されました。

PART 3

ファーストホップ冗長プロトコル

CHAPTER 12

HSRP の設定

この章では、Cisco NX-OS スイッチにホットスタンバイ ルータ プロトコル（HSRP）を設定する方法について説明します。

この章では、次の内容について説明します。

HSRP について

HSRP はファーストホップ冗長プロトコル（FHRP）であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイ ルータを選択します。ルータ グループでは、アクティブ ルータはパケットをルーティングするルータです。スタンバイ ルータは、アクティブ ルータで障害が発生した場合、または事前に設定された条件が満たされた場合に、引き継ぐルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で適切ではありません。HSRP は、そうしたホスト上にフェールオーバー サービスを提供します。

ここでは、次の内容について説明します。

HSRP の概要

HSRP を使用する場合、HSRP 仮想 IP アドレス（実際のルータの IP アドレスではなく）をホストのデフォルト ルータとして設定します。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 アドレスです。

ネットワーク セグメントで HSRP を設定する場合は、HSRP グループの仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つをアクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛てのパケットを受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが、HSRP グループの MAC アドレスおよび IP アドレスの制御を代行します。HSRP はこの時点で、新しいスタンバイ ルータの選択も行います。

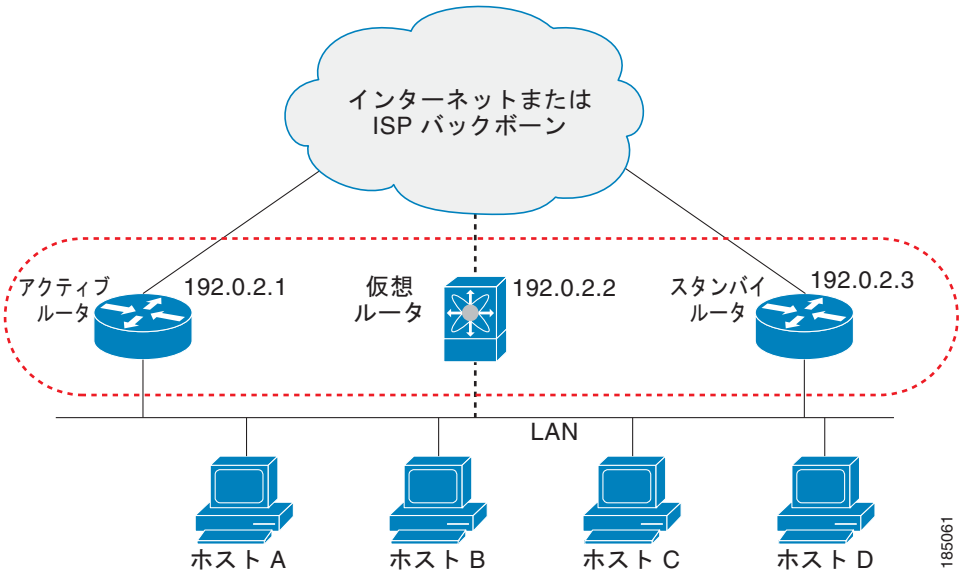
HSRP ではプライオリティ メカニズムを使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

HSRP が動作するインターフェイスは、マルチキャスト UDP（ユーザ データグラム プロトコル）ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブ ルータになります。アクティブ ルータとスタンバイ ルータ間のパケット転送機能の移行は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。

図 12-1 に、HSRP 対応として設定されたネットワークを示します。仮想 MAC アドレスおよび仮想 IP アドレスを共有することによって、2 つ以上のインターフェイスを単一のバーチャル ルータとして動作させることができます。

図 12-1　2 つの対応ルータからなる HSRP トポロジ



仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルト ルータになります。アクティブ ルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、デフォルト ルータとして仮想ルータの IP アドレス（仮想 IP アドレス）を使用して、ホストを設定します。アクティブ ルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイ ルータが引き継いで仮想アドレスに応答し、アクティブ ルータになってアクティブ ルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。

（注）　ルーテッド ポートで受信した HSRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。これには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2（VLAN）インターフェイスで受信した HSRP 仮想 IP アドレス宛のパケットは、アクティブ ルータ上で終端します。

IPv4 の HSRP

HSRP ルータは HSRP hello パケットを交換することによって、相互に通信します。これらのパケットは、UDP ポート 1985 上の宛先 IP マルチキャスト アドレス 224.0.0.2（すべてのルータと通信するための予約済みマルチキャスト アドレス）に送信されます。アクティブ ルータは設定された IP アドレスおよび HSRP 仮想 MAC アドレスから hello パケットを得るのに対して、スタンバイ ルータは設定された IP アドレスおよびインターフェイス MAC アドレスから hello パケットを取得します。インターフェイス MAC アドレスは、Burned-In Address（BIA）のこともあれば、そうではないこともあります。BIA は、MAC アドレスの下位 6 バイトで、ネットワーク インターフェイス カード（NIC）の製造元によって割り当てられます。

ホストはデフォルト ルータが HSRP 仮想 IP アドレスとして設定されているので、HSRP 仮想 IP アドレスに関連付けられた MAC アドレスと通信する必要があります。この MAC アドレスは、仮想 MAC アドレス 0000.0C07.ACxy です。この場合、xy はそれぞれのインターフェイスに基づく、16 進数の HSRP グループ番号です。たとえば、HSRP グループ 1 は 0000.0C07.AC01 という HSRP 仮想 MAC アドレスを使用します。隣接 LAN セグメント上のホストは、標準のアドレス解決プロトコル（ARP）プロセスを使用して、関連付けられた MAC アドレスを解決します。

HSRP バージョン 2 では新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 では、このマルチキャスト アドレスが 224.0.0.2 です。HSRP バージョン 2 では、拡張グループ番号範囲 0 ～ 4095 を使用できます。また、新しい MAC アドレス範囲 0000.0C9F.F000 ～ 0000.0C9F.FFFF を使用します。

HSRP のバージョン

Cisco NX-OS は、デフォルトで HSRP バージョン 1 をサポートします。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ～ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ～ 4095 です。
- IPv4 では IPv4 マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。HSRP バージョン 1 では、このマルチキャスト アドレスが 224.0.0.2 です。
- IPv4 の場合、MAC アドレス範囲 0000.0C9F.000 ～ 0000.0C9F.FFFF を使用します。HSRP バージョン 1 は、MAC アドレス範囲 0000.0C07.AC00 ～ 0000.0C07.ACFF を使用します。
- MD 5 認証のサポートが追加されました。

HSRP のバージョンを変更すると、Cisco NX-OS がグループを再初期化します。新しい仮想 MAC アドレスがグループに与えられるからです。

HSRP バージョン 2 では HSRP バージョン 1 とは異なるパケット フォーマットを使用します。パケット フォーマットは Type-Length-Value（TLV）です。HSRP バージョン 1 ルータは、HSRP バージョン 2 パケットを受信しても無視します。

HSRP 認証

HSRP message digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズム方式の認証は、HSRP スプーフィング ソフトウェアから保護し、業界標準である MD5 アルゴリズムを使用して、信頼性およびセキュリティを向上させます。HSRP は IPv4 アドレスを認証 TLV に含めます。

HSRP メッセージ

HSRP が設定されたルータは、次の 3 種類のマルチキャスト メッセージを交換できます。

- hello : hello メッセージは、ルータの HSRP プライオリティおよびステート情報を他の HSRP ルータに伝えます。
- coup : スタンバイ ルータがアクティブ ルータの機能を引き受けるときに、coup メッセージを送信します。
- resign : このメッセージは、アクティブ ルータであるルータがシャットダウン直前、またはプライオリティの高いルータから hello または coup メッセージが送信されたときに、ルータから送信されます。

HSRP ロード シェアリング

HSRP では、1 つのインターフェイス上で複数のグループを設定できます。オーバーラップする 2 つの IPv4 HSRP グループを設定すると、期待されるデフォルト ルータの冗長性を HSRP から提供しながら、接続ホストからのトラフィックのロード シェアリングが可能です。図 12-2 に、ロード シェアリングが行われる HSRP IPv4 構成の例を示します。

図 12-2　HSRP ロード シェアリング

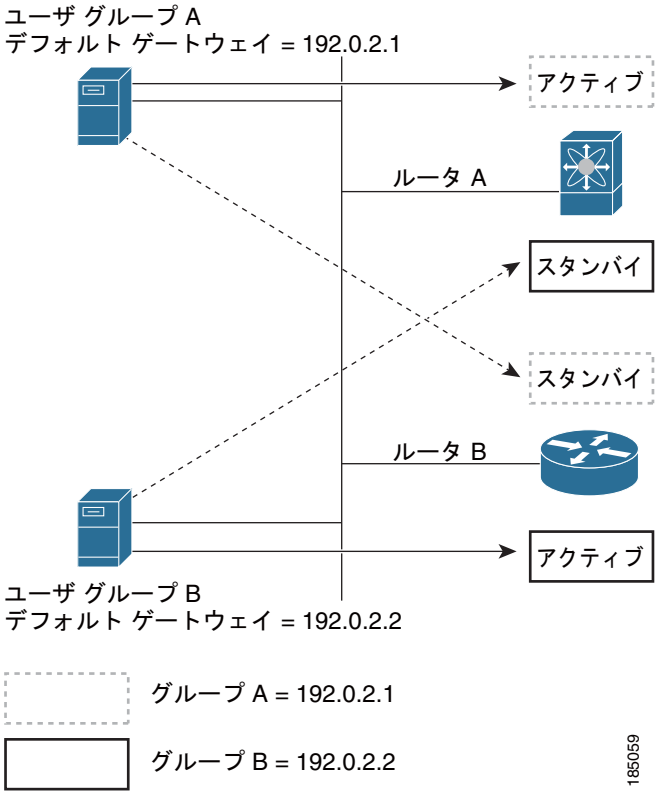


図 12-2 に、ルータ A、ルータ B、および 2 つの HSRP グループを示します。ルータ A はグループ A のアクティブ ルータであり、グループ B のスタンバイ ルータです。同様に、ルータ B はグループ B のアクティブ ルータであり、グループ A のスタンバイ ルータです。両方のルータがアクティブであるかぎり、HSRP は両方のルータにわたって、ホストからのトラフィックのロード バランシングを図ります。どちらかのルータで障害が発生すると、残りのルータが引き続き、両方のホストのトラフィックを処理します。

オブジェクト トラッキングおよび HSRP

オブジェクト トラッキングを使用すると、別のインターフェイスの動作状態に基づいて、HSRP インターフェイスのプライオリティを変更できます。オブジェクト トラッキングによって、メイン ネットワークへのインターフェイスで障害が発生した場合に、スタンバイ ルータにルーティングできます。

トラッキング可能なオブジェクトは、インターフェイスのライン プロトコル ステートまたは IP ルートの到達可能性の 2 種類です。指定したオブジェクトがダウンすると、設定された値だけ、Cisco NX-OS が HSRP プライオリティを引き下げます。詳細については、「HSRP オブジェクト トラッキングの設定」（P.12-13）を参照してください。

vPC と HSRP

HSRP は、Virtual Port Channel（vPC; 仮想ポート チャネル）と連携します。vPC 使用すると、2 つの異なる Cisco Nexus 5000 シリーズ スイッチに物理的に接続するリンクは、その他のスイッチから単一のポート チャネルに見えるようになります。vPC の詳細については、『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.0(3)N1(1)*』を参照してください。

vPC は、アクティブ HSRP ルータとスタンバイ HSRP ルータの両方を通じてトラフィックを転送します。スタンバイ HSRP ルータのプライオリティにおけるしきい値を設定して、vPC トランクに対するトラフィックがフェールオーバーするタイミングを決定できます。「HSRP プライオリティの設定」（P.12-15）を参照してください。

（注） プライマリ vPC ピア スイッチの HSRP をアクティブに、セカンダリ vPC スイッチの HSRP をスタンバイにそれぞれ設定する必要があります。

仮想化のサポート

HSRP は Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。

インターフェイスの VRF メンバシップを変更すると、Cisco NX-OS によって HSRP を含め、すべてのレイヤ 3 設定が削除されます。

詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

HSRP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	HSRP にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。 **（注）** レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

HSRP の前提条件

HSRP には、次の前提条件があります。

- HSRP グループを設定してイネーブルにするには、その前に HSRP 機能をスイッチでイネーブルにする必要があります。

注意事項および制約事項

HSRP 設定時の注意事項および制約事項は、次のとおりです。

- 最小 hello タイマー値は 250 ミリ秒です。
- 最小ホールド タイマー値は 750 ミリ秒です。
- HSRP を設定するインターフェイスに IP アドレスを設定し、そのインターフェイスをイネーブルにしてからでなければ、HSRP はアクティブになりません。
- IPv4 では、仮想 IP アドレスは、インターフェイス IP アドレスと同じサブネットになければなりません。
- 同一インターフェイス上では、複数のファーストホップ冗長プロトコルを設定しないことを推奨します。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。
- バージョン 1 で認められるグループ番号範囲（0 ～ 255）を超えるグループを設定している場合は、バージョン 2 からバージョン 1 への変更はできません。
- インターフェイス VRF メンバシップまたはポート チャネル メンバシップを変更した場合、またはポート モードをレイヤ 2 に変更した場合は、Cisco NX-OS によってインターフェイス上のすべてのレイヤ 3 設定が削除されます。
- Virtual Port Channel（vPC; 仮想ポート チャネル）を使用して仮想 MAC アドレスを設定する場合、両方の vPC ピアに同じ仮想 MAC アドレスを設定する必要があります。
- vPC メンバである VLAN インターフェイスで HSRP MAC アドレスのバーンドイン オプションは使用できません。

デフォルト設定

表 12-1 に、HSRP パラメータのデフォルト設定を示します。

表 12-1　デフォルトの HSRP パラメータ

パラメータ	デフォルト
HSRP	ディセーブル
認証	バージョン 1 の場合はテキストとしてイネーブル、パスワードは cisco
HSRP バージョン	バージョン 1
プリエンプト	ディセーブル
プライオリティ	100
仮想 MAC アドレス	HSRP グループ番号から生成

HSRP の設定

ここでは、次の内容について説明します。

- 「HSRP 機能のイネーブル化」（P.12-8）

- 「HSRP バージョン設定」（P.12-8）
- 「IPv4 の HSRP グループの設定」（P.12-9）
- 「HSRP 仮想 MAC アドレスの設定」（P.12-11）
- 「HSRP の認証」（P.12-11）
- 「HSRP オブジェクト トラッキングの設定」（P.12-13）
- 「HSRP プライオリティの設定」（P.12-15）
- 「HSRP のカスタマイズ」（P.12-16）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

HSRP 機能のイネーブル化

HSRP グループを設定してイネーブルにするには、その前に HSRP 機能をグローバルでイネーブルにする必要があります。

手順の詳細

HSRP 機能をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
feature hsrp **Example:** `switch(config)# feature hsrp`	HSRP をイネーブルにします。

HSRP 機能をディセーブルにして、関連付けられている設定をすべて削除するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no feature hsrp **Example:** `switch(config)# no feature hsrp`	HSRP をディセーブルにします。

HSRP バージョン設定

HSRP のバージョンを設定できます。既存グループのバージョンを変更すると、仮想 MAC アドレスが変更されるので、Cisco NX-OS がそれらのグループの HSRP を再初期化します。HSRP のバージョンは、インターフェイス上のすべてのグループに適用されます。

HSRP のバージョンを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
hsrp version {**1** | **2**} **Example:** switch(config-if)# hsrp version 2	HSRP バージョンを設定します。デフォルトはバージョン 1 です。

IPv4 の HSRP グループの設定

IPv4 インターフェイス上で HSRP グループを設定し、その HSRP グループに仮想 IP アドレスおよび仮想 MAC アドレスを設定できます。

はじめる前に

HSRP 機能がイネーブルになっていることを確認します（「HSRP 機能のイネーブル化」（P.12-8）を参照）。

グループのいずれかのメンバ インターフェイス上で仮想 IP アドレスを設定すると、Cisco NX-OS によって HSRP がイネーブルになります。HSRP グループをイネーブルにする前に、認証、タイマー、プライオリティなどの HSRP 属性を設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip** *ip-address/length*
5. **hsrp** *group-number* [**ipv4**]
6. **ip** [*ip-address* [**secondary**]]
7. **exit**
8. **no shutdown**
9. （任意）**show hsrp** [**group** *group-number*] [**ipv4**]
10. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip** *ip-address/length* **Example:** switch(config-if)# ip 192.0.2.2/8	インターフェイスの IPv4 アドレスを設定します。
ステップ 5	**hsrp** *group-number* [**ipv4**] **Example:** switch(config-if)# hsrp 2 switch(config-if-hsrp)#	HSRP グループを作成し、HSRP コンフィギュレーション モードを開始します。HSRP バージョン 1 で指定できる範囲は 0 ～ 255 です。HSRP バージョン 2 で指定できる範囲は 0 ～ 4095 です。デフォルト値は 0 です。
ステップ 6	**ip** [*ip-address* [**secondary**]] **Example:** switch(config-if-hsrp)# ip 192.0.2.1	HSRP グループの仮想 IP アドレスを設定し、グループをイネーブルにします。このアドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。
ステップ 7	**exit** **Example:** switch(config-if-hsrp)# exit	HSRP コンフィギュレーション モードを終了します。
ステップ 8	**no shutdown** **Example:** switch(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 9	**show hsrp** [**group** *group-number*] [**ipv4**] **Example:** switch(config-if)# show hsrp group 2	（任意）HSRP 情報を表示します。
ステップ 10	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	（任意）この設定の変更を保存します。

（注）　設定完了後にインターフェイスをイネーブルにするには、**no shutdown** コマンドを使用する必要があります。

次に Ethernet 1/2 上で HSRP グループを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip 192.0.2.2/8
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 192.0.2.1
switch(config-if-hsrp)# exit
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

HSRP 仮想 MAC アドレスの設定

設定されたグループ番号に基づいて HSRP が生成したデフォルト仮想 MAC アドレスを変更できます。

（注）　vPC リンクの vPC ピアの両方で同じ仮想 MAC アドレスを設定する必要があります。

HSRP グループの仮想 MAC アドレスを手動で設定するには、HSRP コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
mac-address *string* **Example:** `switch(config-if-hsrp)# mac-address 5000.1000.1060`	HSRP グループの仮想 MAC アドレスを設定します。ストリングには標準の MAC アドレス フォーマット（xxxx.xxxx.xxxx）を使用します。

仮想 MAC アドレスに BIA（バーンドイン MAC アドレス）を使用するように HSRP を設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
hsrp use-bia [**scope interface**] **Example:** `switch(config-if)# hsrp use-bia`	HSRP 仮想 MAC アドレスにインターフェイスの BIA を使用するように、HSRP を設定します。任意で **scope interface** キーワードを使用すると、このインターフェイス上のすべてのグループに BIA を使用するように HSRP を設定できます。

HSRP の認証

クリアテキストまたは MD5 ダイジェスト認証を使用してプロトコルを認証するように、HSRP を設定できます。MD5 認証ではキーチェーンを使用します（『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(3)N1(1)*』を参照）。

はじめる前に

HSRP 機能がイネーブルになっていることを確認します（「HSRP 機能のイネーブル化」（P.12-8）を参照）。

HSRP グループのすべてのメンバに同じ認証およびキーを設定する必要があります。

MD5 認証を使用する場合は、キーチェーンが作成してあることを確認します。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **hsrp** *group-number* [**ipv4**]
5. **authentication text** *string*
   または
   authentication md5 {**key-chain** *key-chain* | **key-string** {**0** | **7**} *text* [**timeout** *seconds*]}
6. （任意）**show hsrp** [**group** *group-number*]
7. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

ステップ 4	**hsrp** *group-number* [**ipv4**]
	
	Example:
	`switch(config-if)# hsrp 2`
	`switch(config-if-hsrp)#`
		HSRP グループを作成し、HSRP 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	**authentication text** *string* **Example:** `switch(config-if-hsrp)# authentication text mypassword`	このインターフェイス上で、HSRP のクリアテキスト認証を設定します。
	authentication md5 {**key-chain** *key-chain* | **key-string** {**0** | **7**} *text* [**timeout** *seconds*]} **Example:** `switch(config-if-hsrp)# authentication md5 key-chain hsrp-keys`	このインターフェイス上で、HSRP の MD5 認証を設定します。キーチェーンまたはキー ストリングを使用できます。キー ストリングを使用する場合は、HSRP が新しいキーだけを受け付けるように、任意でタイムアウトを設定できます。指定できる範囲は 0 ～ 32767 秒です。

	コマンド	目的
ステップ 6	**show hsrp** [**group** *group-number*] **Example:** switch(config-if-hsrp)# show hsrp group 2	（任意）HSRP 情報を表示します。
ステップ 7	**copy running-config startup-config** **Example:** switch(config-if-hsrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、キーチェーン作成後に HSRP の MD5 認証を Ethernet 1/2 上で設定する例を示します。

```
switch# configure terminal
switch(config)# key chain hsrp-keys
switch(config-keychain)# key 0
switch(config-keychain-key)# key-string 7 zqdest
switch(config-keychain-key) accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
switch(config-keychain-key) key 1
switch(config-keychain-key) key-string 7 uaeqdyito
switch(config-keychain-key) accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
switch(config-keychain-key)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# hsrp 2
switch(config-if-hsrp)# authenticate md5 key-chain hsrp-keys
switch(config-if-hsrp)# copy running-config startup-config
```

HSRP オブジェクト トラッキングの設定

他のインターフェイスまたはルータの可用性に基づいて、プライオリティが調整されるように HSRP グループを設定できます。スイッチがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、スイッチのプライオリティはダイナミックに変更されます。トラッキング プロセスはトラッキング対象オブジェクトに定期的にポーリングを実行し、値の変化をすべて記録します。値が変化すると、HSRP がプライオリティを再計算します。HSRP インターフェイスにプリエンプトを設定している場合は、プライオリティの高い HSRP インターフェイスがアクティブ ルータになります。

HSRP では、トラッキング対象のオブジェクトおよびトラック リストをサポートします。トラック リストの詳細については、第 14 章「オブジェクト トラッキングの設定」を参照してください。

はじめる前に

HSRP 機能がイネーブルになっていることを確認します（「HSRP 機能のイネーブル化」（P.12-8）を参照）。

手順の概要

1. **configure terminal**
2. **track** *object-id* **interface** *interface-type number* {**ip routing** | **line-protocol**}
   または
   track *object-id* **ip route** *ip-prefix/length* **reachability**

3. **interface** *interface-type slot/port*
4. **no switchport**
5. **hsrp** *group-number* [**ipv4**]
6. **priority** [*value*]
7. **track** *object-number* [**decrement** *value*]
8. **preempt** [**delay minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]
9. （任意）**show hsrp interface** *interface-type number*
10. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-id* **interface** *interface-type number* {**ip routing** | **line-protocol**} **Example:** switch(config)# track 1 interface ethernet 2/2 line-protocol switch(config-track#	この HSRP インターフェイスが追跡するインターフェイスを設定します。インターフェイスのステート変化は次のように、この HSRP のプライオリティを左右します。 • HSRP コンフィギュレーション モードで、**track** コマンドで使用するインターフェイスおよび対応するオブジェクト番号を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップかどうかが追跡されます。**ip** キーワードを指定すると、インターフェイス上で IP ルーティングがイネーブルであり、IP アドレスが設定されているかどうかもチェックされます。
	track *object-id* **ip route** *ip-prefix/length* **reachability** **Example:** switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。*object-id* の範囲は 1 ～ 500 です。
ステップ 3	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 5	**hsrp** *group-number* [**ipv4**] **Example:** switch(config-if)# hsrp 2 switch(config-if-hsrp)#	HSRP グループを作成し、HSRP コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 6	**priority** [*value*] **Example:** switch(config-if-hsrp)# priority 254	HSRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 100 です。
ステップ 7	**track** *object-number* [**decrement** *value*] **Example:** switch(config-if-hsrp)# track 1 decrement 20	HSRP インターフェイスの重み付けを左右する、トラッキング対象のオブジェクトを指定します。 *value* 引数には、トラッキング対象のオブジェクトで障害が発生した場合に、HSRP インターフェイスのプライオリティから差し引く値を指定します。指定できる範囲は 1 ～ 255 です。デフォルトは 10 です。
ステップ 8	**preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** switch(config-if-hsrp)# preempt delay minimum 60	現在のアクティブ ルータよりプライオリティが高い場合に、HSRP グループのアクティブ ルータとして引き継ぐようにルータを設定します。このコマンドは、デフォルトではディセーブルです。指定できる範囲は 0 ～ 3600 秒です。
ステップ 9	**show hsrp interface** *interface-type number* **Example:** switch(config-if-hsrp)# show hsrp interface ethernet 1/2	（任意）インターフェイスの HSRP 情報を表示します。
ステップ 10	**copy running-config startup-config** **Example:** switch(config-if-hsrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、Ethernet 1/2 上で HSRP オブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 interface ethernet 2/2 line-protocol
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# hsrp 2
switch(config-if-hsrp)# track 1 decrement 20
switch(config-if-hsrp)# copy running-config startup-config
```

HSRP プライオリティの設定

インターフェイス上で HSRP プライオリティを設定できます。HSRP では、プライオリティを使用して、アクティブ ルータとして動作する HSRP グループ メンバを決定します。vPC 対応インターフェイスで HSRP を設定する場合は、上限および下限のしきい値を設定して、vPC トランクに対するフェールオーバーのタイミングを制御できます。スタンバイ ルータのプライオリティが下限しきい値を下回ると、HSRP はすべてのスタンバイ ルータ トラフィックを vPC トランクを介して送信し、アクティブ HSRP ルータを通じて転送します。HSRP では、スタンバイ HSRP ルータ プライオリティが上限しきい値を超えるまで、この状況を維持します。

HSRP プライオリティを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
priority *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*] **Example:** `switch(config-if-hsrp)# priority 60 forwarding-threshold lower 40 upper 50`	HSRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。*level* の範囲は 0 ～ 255 です。デフォルトは 100 です。オプションで、vPC トランクにフェールオーバーする時点を決定するために vPC が使用するしきい値の上限と下限を設定します。*lower-value* の範囲は 1 ～ 255 です。デフォルトは 1 です。*upper-value* の範囲は 1 ～ 255 です。デフォルトは 255 です。

HSRP のカスタマイズ

任意で、HSRP の動作をカスタマイズできます。仮想 IP アドレスを設定することによって、HSRP グループをイネーブルにすると、そのグループがただちに動作可能になることに注意してください。HSRP をカスタマイズする前に HSRP グループをイネーブルにした場合、機能のカスタマイズが完了しないうちに、ルータがグループの制御を引き継いでアクティブ ルータになる可能性があります。HSRP のカスタマイズを予定している場合は、HSRP グループをイネーブルにする前に行ってください。

HSRP をカスタマイズするには、HSRP コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
name *string* **Example:** `switch(config-if-hsrp)# name HSRP-1`	HSRP グループの IP 冗長名を指定します。*string* は 1 ～ 255 文字です。デフォルト ストリングのフォーマットは、 hsrp-<interface-short-name>-<group-id> です。たとえば、hsrp-Eth2/1-1 です。

コマンド	目的
preempt [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] **Example:** `switch(config-if-hsrp)# preempt delay minimum 60`	現在のアクティブ ルータよりもプライオリティが高い場合に、HSRP グループのアクティブ ルータとして引き継ぐようにルータを設定します。このコマンドは、デフォルトではディセーブルです。指定できる範囲は 0 ～ 3600 秒です。
timers [**msec**] *hellotime* [**msec**] *holdtime* **Example:** `switch(config-if-hsrp)# timers 5 18`	次のように、この HSRP メンバーの hello タイムおよびホールド タイムを設定します。 • *hellotime* : hello パケットを送信してから、次の hello パケットを送信するまでのインターバル。指定できる範囲は 1 ～ 254 秒です。 • *holdtime* : hello パケットの情報が無効と見なされるまでのインターバル。指定できる範囲は 3 ～ 255 です。 オプションの **msec** キーワードでは、引数をデフォルトの秒単位ではなく、ミリ秒単位で表すことを指定します。タイマーの範囲（ミリ秒）は次のとおりです。 • *hellotime* : hello パケットを送信してから、次の hello パケットを送信するまでのインターバル。指定できる範囲は 255 ～ 999 ミリ秒です。 • *holdtime* : hello パケットの情報が無効と見なされるまでのインターバル。指定できる範囲は 750 ～ 3000 ミリ秒です。

HSRP をカスタマイズするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
hsrp delay minimum *seconds* **Example:** `switch(config-if)# hsrp delay minimum 30`	グループがイネーブルになってから、グループに参加するまでに HSRP が待機する最小時間を指定します。指定できる範囲は 0 ～ 10000 秒です。デフォルトは 0 です。
hsrp delay reload *seconds* **Example:** `switch(config-if)# hsrp delay reload 30`	リロード後、グループに参加するまでに HSRP が待機する最小時間を指定します。指定できる範囲は 0 ～ 10000 秒です。デフォルトは 0 です。

HSRP 設定の確認

HSRP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hsrp [**group** *group-number*]	すべてのグループまたは特定のグループの HSRP ステータスを表示します。
show hsrp delay [**interface** ***interface-type slot/port***]	すべてのインターフェイスまたは特定のインターフェイスの HSRP 遅延値を表示します。
show hsrp [**interface** ***interface-type slot/port***]	インターフェイスの HSRP ステータスを表示します。
show hsrp [**group** ***group-number***] [**interface** ***interface-type slot/port***] [**active] [all**] [**init**] [**learn**] [**listen**] [**speak**] [**standby**]	ステートが active、init、listen、または standby のバーチャル フォワーダについて、グループまたはインターフェイスの HSRP ステータスを表示します。disabled を含めてすべてのステートを表示する場合は、**all** キーワードを使用します。
show hsrp [**group** ***group-number***] [**interface** ***interface-type slot/port***] **active**] [**all**] [**init**] [**learn**] [**listen**] [**speak**] [**standby**] **brief**	ステートが active、init、listen、または standby のバーチャル フォワーダについて、グループまたはインターフェイスの HSRP ステータスの要約を表示します。disabled を含めてすべてのステートを表示する場合は、**all** キーワードを使用します。

HSRP の設定例

次に、MD5 認証およびインターフェイス トラッキングを指定して、インターフェイス上で HSRP をイネーブルにする例を示します。

```
key chain hsrp-keys
 key 0
   key-string 7 zqdest
  accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
   send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
   key-string 7 uaeqdyito
   accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
   send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
feature hsrp
track 2 interface ethernet 2/2 ip
interface ethernet 1/2
 no switchport
 ip address 192.0.2.2/8
 hsrp 1
  authenticate md5 key-chain hsrp-keys
  priority 90
  track 2 decrement 20
  ip-address 192.0.2.10
 no shutdown
```

その他の関連資料

HSRP の実装に関する詳細は、次の各項を参照してください。

- 「関連資料」（P.12-19）
- 「MIB」（P.12-19）

関連資料

関連項目	マニュアル名
VRRP の設定	第 13 章「VRRP の設定」
HSRP CLI コマンド	『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』

MIB

管理情報ベース（MIB）	MIB のリンク
CISCO-HSRP-MIB	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

HSRP 機能の履歴

表 12-2 は、この機能のリリースの履歴です。

表 12-2　HSRP 機能の履歴

機能名	リリース	機能情報
HSRP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 13

VRRP の設定

この章では、スイッチ上で仮想ルータ冗長プロトコル（VRRP）を設定する方法について説明します。

この章では、次の内容について説明します。

VRRP の概要

VRRP を使用すると、仮想 IP アドレスを共有するルータ グループを設定することによって、ファーストホップ IP ルータで透過的フェールオーバーが可能になります。VRRP ではそのグループのマスター ルータが選択され、仮想 IP アドレスへのすべてのパケットが処理できるようになります。残りのルータはスタンバイになり、マスター ルータで障害が発生した場合に処理を引き継ぎます。

ここでは、次の内容について説明します。

VRRP の動作

LAN クライアントは、ダイナミック プロセスまたはスタティック設定を使用することによって、特定のリモート宛先へのファーストホップにするルータを決定できます。ダイナミック ルータ ディスカバリの例を示します。

- プロキシ ARP：クライアントはアドレス解決プロトコル（ARP）を使用して到達すべき宛先を取得します。ルータは独自の MAC アドレスで ARP 要求に応答します。
- ルーティング プロトコル：クライアントはダイナミック ルーティング プロトコルのアップデート（RIP など）を受信し、独自のルーティング テーブルを形成します。
- IRDP クライアント：クライアントはインターネット制御メッセージ プロトコル（ICMP）ルータ ディスカバリ クライアントを実行します。

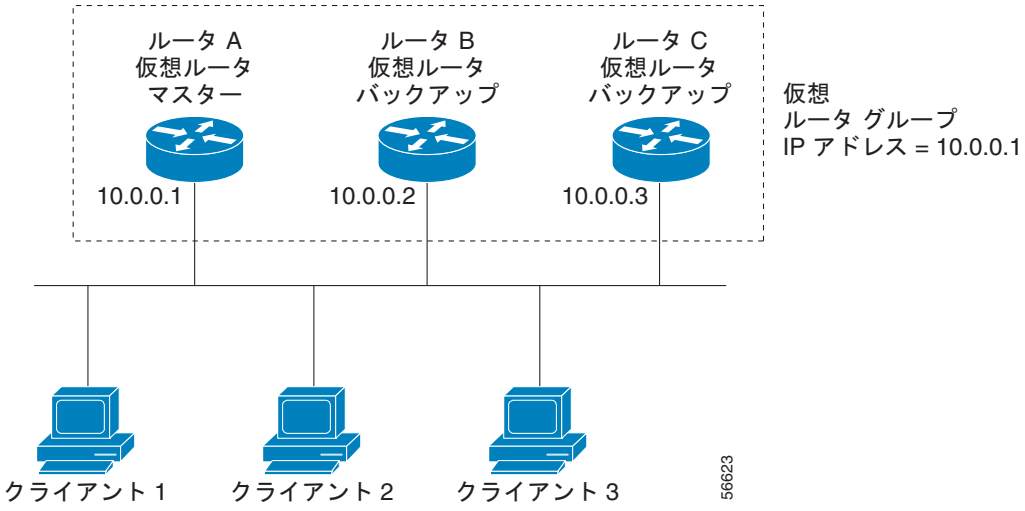
ダイナミック ディスカバリ プロトコルのデメリットは、LAN クライアントにある程度、設定および処理のオーバーヘッドが発生することです。また、ルータで障害が発生した場合に、別のルータへの切り替え処理が遅くなる可能性があります。

ダイナミック ディスカバリ プロトコルの代わりに、クライアント上でデフォルト ルータをスタテイックに設定することもできます。この方法を使用すると、クライアントの設定および処理が簡素化されますが、シングルポイント障害が生じます。デフォルト ゲートウェイで障害が発生した場合、LAN クライアントの通信はローカル IP ネットワーク セグメントに限定され、ネットワークの他の部分から切り離されます。

VRRP では、ルータ グループ（VRRP グループ）が単一の仮想 IP アドレスを共有できるようにすることによって、スタティック設定に伴う問題を解決できます。さらに、デフォルト ゲートウェイとして仮想 IP アドレスを指定して、LAN クライアントを設定できます。

図 13-1 に、基本的な VLAN トポロジを示します。この例では、ルータ A、B、および C が VRRP グループを形成します。グループの IP アドレスは、ルータ A のイーサネット インターフェイスに設定されているアドレス（10.0.0.1）と同じです。

図 13-1　基本的な VRRP トポロジ



仮想 IP アドレスにルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A がマスター（別名、IP アドレス オーナー）です。ルータ A はマスターとして、VRRP グループの仮想 IP アドレスを所有し、送信されたパケットをこの IP アドレスに転送します。クライアント 1 ～ 3 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

ルータ B および C の役割はバックアップです。マスターで障害が発生すると、プライオリティが最も高いバックアップ ルータがマスターになり、仮想 IP アドレスを引き継いで、LAN ホストへのサービスが途切れないようにします。ルータ A が回復すると、再びマスターになります。詳細については、「VRRP ルータのプライオリティおよびプリエンプト」を参照してください。

（注）　ルーテッド ポートで受信した VRRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがマスター VRRP ルータであるのかバックアップ VRRP ルータであるのかは関係ありません。これには ping トラフィックと Telnet トラフィックが含まれます。VRRP 仮想 IP アドレス宛てのレイヤ 2（VLAN）インターフェイスで受信したパケットは、マスタ ルータで終端します。

VRRP の利点

VRRP の利点は、次のとおりです。

- 冗長性：複数のルータをデフォルト ゲートウェイ ルータとして設定できるので、ネットワークにシングルポイント障害が発生する確率が下がります。
- ロード シェアリング：複数のルータで LAN クライアントとの間のトラフィックを分担できます。トラフィックの負荷が使用可能なルータ間でより公平に分担されます。
- マルチ VRRP グループ：プラットフォームがマルチ MAC アドレスをサポートする場合、ルータの物理インターフェイス上で、最大 255 の VRRP グループをサポートします。マルチ VRRP グループによって、LAN トポロジで冗長性およびロード シェアリングを実現できます。
- マルチ IP アドレス：セカンダリ IP アドレスを含めて、複数の IP アドレスを管理できます。イーサネット インターフェイス上で複数のサブネットを設定している場合は、各サブネットで VRRP を設定できます。
- プリエンプト：障害マスターを引き継いでいたバックアップ ルータより、さらにプライオリティが高いバックアップ ルータが使用可能になったときに、プライオリティが高い方を優先させることができます。
- アドバタイズメント プロトコル：VRRP アドバタイズメントに、専用の IANA（インターネット割り当て番号局）規格マルチキャスト アドレス（224.0.0.18）を使用します。このアドレッシング方式によって、マルチキャストを提供するルータ数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA は VRRP に IP プロトコル番号 112 を割り当てています。
- VRRP トラッキング：インターフェイスのステートに基づいて VRRP プライオリティを変更することによって、最適な VRRP ルータがグループのマスターになることが保証されます。

マルチ VRRP グループ

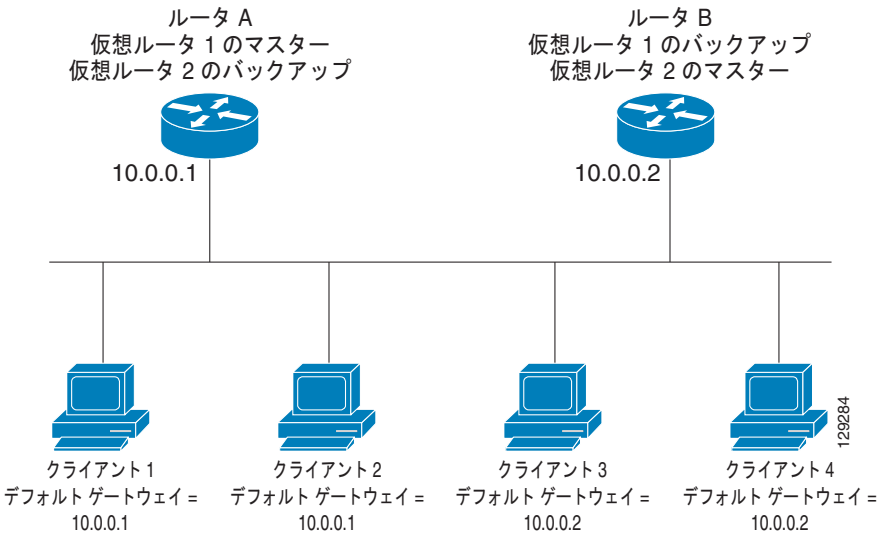
物理インターフェイス上で、最大 255 の VRRP グループを設定できます。ルータ インターフェイスがサポートできる VRRP グループの実際の数は、次の要因によって決まります。

- ルータの処理能力
- ルータのメモリの能力

ルータ インターフェイス上で複数の VRRP グループが設定されたトポロジでは、インターフェイスはある VRRP グループのマスター、および他の 1 つまたは複数の VRRP グループのバックアップとして動作可能です。

図 13-2 に、ルータ A および B がクライアント 1 ～ 4 との間でトラフィックを共有するように VRRP が設定されている LAN トポロジを示します。ルータ A と B の一方で障害が発生した場合、もう一方がバックアップとして機能します。

図 13-2　ロード シェアリングおよび冗長構成の VRRP トポロジ



このトポロジには、オーバーラップする 2 つの VRRP グループに対応する 2 つの仮想 IP アドレスが含まれています。VRRP グループ 1 では、ルータ A が IP アドレス 10.0.0.1 のオーナーであり、マスターです。ルータ B はルータ A のバックアップです。クライアント 1 ～ 2 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

VRRP グループ 2 では、ルータ B が IP アドレス 10.0.0.2 のオーナーであり、マスターです。ルータ A はルータ B のバックアップです。クライアント 3 ～ 4 には、デフォルト ゲートウェイの IP アドレス 10.0.0.2 が設定されています。

VRRP ルータのプライオリティおよびプリエンプト

VRRP 冗長構成の重要なポイントは、VRRP ルータのプライオリティです。プライオリティによって、各 VRRP ルータが果たす役割が決まり、マスター ルータで障害が発生した場合のアクションが決まるからです。

VRRP ルータが仮想 IP アドレスおよび物理インターフェイスの IP アドレスを所有する場合、そのルータはマスターとして機能します。マスターのプライオリティは 255 です。

プライオリティによって、VRRP ルータがバックアップ ルータとして動作するかどうかが決まり、さらに、マスターで障害が発生した場合にマスターになる順序も決まります。

たとえば、ルータ A が LAN トポロジにおけるマスターであり、そのルータ A で障害が発生した場合、VRRP はバックアップ B が引き継ぐのか、バックアップ C が引き継ぐのかを判断する必要があります。ルータ B にプライオリティ 101 が設定されていて、ルータ C がデフォルトのプライオリティ 100 の場合、VRRP はルータ B をマスターになるべきルータとして選択します。ルータ B の方がプライオリティが高いからです。ルータ B および C にデフォルトのプライオリティ 100 が設定されている場合は、VRRP は IP アドレスが大きい方のバックアップをマスターになるべきルータとして選択します。

VRRP ではプリエンプトを使用して、VRRP バックアップ ルータがマスターになってからのアクションを決定します。プリエンプトはデフォルトでイネーブルなので、VRRP は新しいマスターよりプライオリティの高いバックアップがオンラインになると、バックアップに切り替えます。たとえば、ルータ A がマスターであり、そのルータ A で障害が発生した場合、VRRP は（プライオリティの順位が次である）ルータ B を選択します。ルータ C がルータ B より高いプライオリティでオンラインになると、ルータ B で障害が発生していなくても、VRRP はルータ C を新しいマスターとして選択します。

プリエンプトをディセーブルにした場合、VRRP が切り替わるのは、元のマスターが回復した場合、または新しいマスターで障害が発生した場合に限られます。

vPC および VRRP

VRRP は Virtual Port Channels（vPC; 仮想ポート チャネル）と相互運用しています。vPC 使用すると、2 つの異なる Cisco Nexus 5000 シリーズ スイッチに物理的に接続するリンクは、その他のスイッチから単一のポート チャネルに見えるようになります。vPC の詳細については、『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.0(2)N2(1)*』を参照してください。

vPC はマスター VRRP ルータとバックアップ VRRP ルータの両方を使用してトラフィックを転送します。バックアップ VRRP ルータのプライオリティのしきい値を設定することにより、トラフィックをどの時点で vPC トランクにフェールオーバーさせるかを決定できます。「VRRP プライオリティの設定」（P.13-9）を参照してください。

（注）　プライマリ vPC ピア スイッチの VRRP をアクティブに、セカンダリ vPC スイッチの VRRP をスタンバイにそれぞれ設定する必要があります。

VRRP のアドバタイズメント

VRRP マスターは同じグループ内の他の VRRP ルータに、VRRP アドバタイズメントを送信します。アドバタイズメントは、マスターのプライオリティおよびステートを伝達します。Cisco NX-OS は VRRP アドバタイズメントを IP パケットにカプセル化して、VRRP グループに割り当てられた IP マルチキャスト アドレスに送信します。Cisco NX-OS がアドバタイズメントを送信する間隔はデフォルトでは 1 秒ですが、ユーザ側で別のアドバタイズ インターバルを設定できます。

VRRP 認証

VRRP は、次の認証方式をサポートします。

- 認証なし
- プレーン テキスト認証

VRRP は次の場合に、パケットを拒否します。

- 認証方式がルータと着信パケットの間で異なっている。
- テキスト認証ストリングがルータと着信パケットの間で異なっている。

VRRP トラッキング

VRRP は次の 2 つのトラッキング オプションをサポートしています。

- ネイティブ インターフェイス トラッキング：インターフェイスのステートを追跡し、そのステートを使用して VRRP グループの VRRP ルータのプライオリティを判別します。インターフェイスがダウンしている場合、またはインターフェイスにプライマリ IP アドレスがない場合、トラッキング対象ステートはダウンとなります。
- オブジェクト トラッキング：設定されたオブジェクトのステートを追跡し、そのステートを使用して VRRP グループの VRRP ルータのプライオリティを判別します。オブジェクト トラッキングの詳細については、第 14 章「オブジェクト トラッキングの設定」を参照してください。

トラッキング対象ステート（インターフェイスまたはオブジェクト）がダウンになると、VRRP はユーザがトラッキング対象ステートに対して新しいプライオリティをどのように設定するかに基づいて、プライオリティをアップデートします。トラッキング対象ステートがオンラインになると、VRRP は仮想ルータ グループの元のプライオリティを復元します。

たとえば、ネットワークへのアップリンクがダウンした場合、別のグループ メンバーが VRRP グループのマスターとして引き継げるように、VRRP グループ メンバーのプライオリティを引き下げなければならないことがあります。詳細については、「VRRP インターフェイス ステート トラッキングの設定」（P.13-15）を参照してください。

（注）　VRRP はレイヤ 2 インターフェイスのトラッキングをサポートしていません。

仮想化のサポート

VRRP は VRF（仮想ルーティングおよびフォワーディング）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。

インターフェイスの VRF メンバシップを変更すると、Cisco NX-OS によって VRRP を含め、すべてのレイヤ 3 設定が削除されます。

詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

VRRP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	VRRP にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。 （注）　レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。

注意事項および制約事項

VRRP 設定時の注意事項および制約事項は、次のとおりです。

- 管理インターフェイス上で VRRP を設定できません。
- VRRP がイネーブルの場合は、ネットワーク上のスイッチ全体で VRRP 設定を複製する必要があります。

- 同一インターフェイス上では、複数のファーストホップ冗長プロトコルを設定しないことを推奨します。
- VRRP を設定するインターフェイスに IP アドレスを設定し、そのインターフェイスをイネーブルにしてからでなければ、VRRP はアクティブになりません。
- インターフェイス VRF メンバシップまたはポート チャネル メンバシップを変更した場合、またはポート モードをレイヤ 2 に変更した場合は、Cisco NX-OS によってインターフェイス上のすべてのレイヤ 3 設定が削除されます。
- VRRP でレイヤ 2 インターフェイスを追跡するよう設定した場合、レイヤ 2 をシャットダウンしてからインターフェイスを再度イネーブル化することにより、VRRP プライオリティを更新してレイヤ 2 インターフェイスのステートを反映させる必要があります。

デフォルト設定

表 13-1 に、VRRP パラメータのデフォルト設定を示します。

表 13-1　デフォルトの VRRP パラメータ

パラメータ	デフォルト
アドバタイズ インターバル	1 秒
認証	認証なし
プリエンプト	イネーブル
プライオリティ	100
VRRP 機能	ディセーブル

VRRP の設定

ここでは、次の内容について説明します。

- 「VRRP 機能のイネーブル化」（P.13-7）
- 「VRRP グループの設定」（P.13-8）
- 「VRRP プライオリティの設定」（P.13-9）
- 「VRRP 認証の設定」（P.13-11）
- 「アドバタイズメント パケットのタイム インターバル設定」（P.13-13）
- 「プリエンプトのディセーブル化」（P.13-14）
- 「VRRP インターフェイス ステート トラッキングの設定」（P.13-15）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

VRRP 機能のイネーブル化

VRRP グループを設定してイネーブルにするには、その前に VRRP 機能をグローバルでイネーブルにする必要があります。

VRRP 機能をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
feature vrrp **Example:** `switch(config)# feature vrrp`	VRRP をイネーブルにします。

VRRP 機能をディセーブルにして、関連付けられている設定をすべて削除するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no feature vrrp **Example:** `switch(config)# no feature vrrp`	VRRP 機能をディセーブルにします。

VRRP グループの設定

VRRP グループを作成し、仮想 IP アドレスを割り当て、グループをイネーブルにすることができます。

VRRP グループに設定できる仮想 IPv4 アドレスは 1 つです。マスター VRRP ルータはデフォルトで、仮想 IP アドレスを直接の宛先とするパケットを廃棄します。これは、VRRP マスターがパケットを転送するネクストホップ ルータとしてのみ想定されているからです。アプリケーションによって、Cisco NX-OS が仮想ルータ IP 宛てのパケットを受け付けるようにする必要があります。仮想 IP アドレスに secondary オプションを使用すると、ローカル ルータが VRRP マスターの場合に、これらのパケットを受け付けます。

VRRP グループを設定した場合は、そのグループをアクティブにするために、グループを明示的にイネーブルにする必要があります。

はじめる前に

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **address** *ip-address* [**secondary**]
6. **no shutdown**
7. （任意）**show vrrp**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# switch(config-if)# interface ethernet 2/1	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	仮想ルータ グループを作成します。指定できる範囲は 1 ～ 255 です。
ステップ 5	**address** *ip-address* [**secondary**] **Example:** switch(config-if-vrrp)# address 192.0.2.8	指定の VRRP グループに仮想 IPv4 アドレスを設定します。このアドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。 **secondary** オプションは、VRRP ルータが仮想ルータの IP アドレスに送信されたパケットを受け付けて、アプリケーションに配信することをアプリケーションが要求する場合に限られます。
ステップ 6	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 7	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	（任意）VRRP 情報を表示します。
ステップ 8	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

VRRP プライオリティの設定

仮想ルータの有効なプライオリティ範囲は 1 ～ 254 です（1 が最下位、254 が最上位のプライオリティ）。バックアップのデフォルトのプライオリティ値は 100 です。インターフェイス アドレスがプライマリ仮想 IP アドレスと同じスイッチ（マスター）の場合、デフォルト値は 255 です。

vPC がイネーブルになっているインターフェイスで VRRP を設定する場合、オプションでしきい値の上限と下限を設定し、どの時点で vPC トランクにフェールオーバーするかを制御できます。バックアップ ルータのプライオリティがしきい値の下限を下回ると、VRRP はバックアップ ルータのすべてのトラフィックを vPC 経由で送信し、マスター VRRP ルータから転送します。バックアップ VRRP ルータのプライオリティがしきい値の上限を超えるまで、VRRP はこの処理を継続します。

はじめる前に

VRRP 機能がイネーブルになっていることを確認します（「VRRP の設定」（P.13-7）を参照）。

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*]
7. **no shutdown**
8. （任意）**show vrrp**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

ステップ 4	**vrrp** *number*
	
	Example:
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

	コマンド	目的
ステップ 5	**shutdown** **Example:** switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	VRRP グループをディセーブルにします。デフォルトでは、ディセーブルです。
ステップ 6	**priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*] 例： switch(config-if-vrrp)# priority 60 forwarding-threshold lower 40 upper 50	VRRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。*level* の範囲は 1 ～ 254 です。バックアップの場合、デフォルトは 100 です。インターフェイス IP アドレスが仮想 IP アドレスと等しいマスターの場合は 255 です。 オプションで、vPC トランクにフェールオーバーする時点を決定するために vPC が使用するしきい値の上限と下限を設定します。*lower-value* の範囲は 1 ～ 255 です。デフォルトは 1 です。*upper-value* の範囲は 1 ～ 255 です。デフォルトは 255 です。
ステップ 7	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 8	**show vrrp** ***Example:*** switch(config-if-vrrp)# show vrrp	（任意）VRRP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

VRRP 認証の設定

VRRP グループに単純なテキスト認証を設定できます。

はじめる前に

ネットワークのすべての VRRP スイッチで認証設定が同じであることを確認します。

VRRP 機能がイネーブルになっていることを確認します（「VRRP の設定」（P.13-7）を参照）。

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*

5. **shutdown**
6. **authentication text** *password*
7. **no shutdown**
8. （任意）**show vrrp**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

ステップ 4	**vrrp** *number*
	
	Example:
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 5	**shutdown**
	
	Example:
	`switch(config-if-vrrp)# shutdown`
	`switch(config-if-vrrp)#`
		VRRP グループをディセーブルにします。デフォルトでは、ディセーブルです。

ステップ 6	**authentication text** *password* **Example:** `switch(config-if-vrrp)# authentication md5 prd555oln47espn0 spi 0x0`	単純なテキスト認証オプションを指定し、キーネーム パスワードを指定します。キーネームの範囲は 1 ～ 255 文字です。16 文字以上を推奨します。テキスト パスワードは、英数字で最大 8 文字です。

ステップ 7	**no shutdown**
	
	Example:
	`switch(config-if-vrrp)# no shutdown`
	`switch(config-if-vrrp)#`
		VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。

ステップ 8	**show vrrp** **Example:** `switch(config-if-vrrp)# show vrrp`	（任意）VRRP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **Example:** `switch(config-if-vrrp)# copy running-config startup-config`	（任意）この設定の変更を保存します。

アドバタイズメント パケットのタイム インターバル設定

アドバタイズメント パケットのタイム インターバルを設定できます。

はじめる前に

VRRP 機能がイネーブルになっていることを確認します（「VRRP の設定」（P.13-7）を参照）。

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **advertisement-interval** *seconds*
7. **no shutdown**
8. （任意）**show vrrp**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport** **Example:** `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

ステップ 4	**vrrp** ***number***
	
	Example:
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 5	**shutdown**
	
	Example:
	`switch(config-if-vrrp)# shutdown`
	`switch(config-if-vrrp)#`
		VRRP グループをディセーブルにします。デフォルトでは、ディセーブルです。

	コマンド	目的
ステップ 6	**advertisement-interval** *seconds* **Example:** switch(config-if-vrrp)# advertisement-interval 15	アドバタイズメント フレームの送信間隔を秒数で設定します。範囲は 1 ～ 254 です。デフォルトは 1 秒です。
ステップ 7	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 8	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	（任意）VRRP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

プリエンプトのディセーブル化

VRRP グループ メンバのプリエンプトをディセーブルにできます。プリエンプトをディセーブルにすると、プライオリティの高いバックアップ ルータがプライオリティの低いマスター ルータのかわりにマスターになることはありません。プリエンプトはデフォルトでイネーブルです。

はじめる前に

VRRP 機能がイネーブルになっていることを確認します（「VRRP の設定」（P.13-7）を参照）。

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **no preempt**
7. **no shutdown**
8. （任意）**show vrrp**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	仮想ルータ グループを作成します。
ステップ 5	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 6	**no preempt** **Example:** switch(config-if-vrrp)# no preempt	プリエンプト オプションをディセーブルにして、プライオリティが上位のバックアップが使用されてもマスターが変わらないようにします。
ステップ 7	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 8	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	（任意）VRRP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

VRRP インターフェイス ステート トラッキングの設定

インターフェイスのステート追跡機能では、スイッチ内の他のインターフェイスのステートに基づいて、仮想ルータのプライオリティが変更されます。トラッキング対象のインターフェイスがダウンしたり、IP アドレスが削除されると、Cisco NX-OS はトラッキング プライオリティ値を仮想ルータに割り

当てます。トラッキング対象のインターフェイスがオンライン状態になり、IP アドレスがこのインターフェイスに設定されると、Cisco NX-OS は仮想ルータに設定されていたプライオリティを復元します（「VRRP プライオリティの設定」（P.13-9）を参照）。

（注）　インターフェイス ステート トラッキングを動作させるには、インターフェイス上でプリエンプトをイネーブルにする必要があります。

（注）　VRRP はレイヤ 2 インターフェイスのトラッキングをサポートしていません。

はじめる前に

VRRP 機能がイネーブルになっていることを確認します（「VRRP の設定」（P.13-7）を参照）。

インターフェイス上で IP アドレスが設定されていることを確認します（「IPv4 アドレス指定の設定」（P.2-7）を参照）。

仮想ルータがイネーブルになっていることを確認します（「VRRP グループの設定」（P.13-8）を参照）。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **track interface** *type number* **priority** *value*
7. **no shutdown**
8. （任意）**show vrrp**
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** **Example:** switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。

	コマンド	目的
ステップ 4	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	仮想ルータ グループを作成します。
ステップ 5	**shutdown** **Example:** switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	VRRP グループをディセーブルにします。デフォルトでは、ディセーブルです。
ステップ 6	**track interface** type *number* **priority** *value* **Example:** switch(config-if-vrrp)# track interface ethernet 2/10 priority 254	VRRP グループのインターフェイス プライオリティ トラッキングをイネーブルにします。プライオリティの範囲は 1 ～ 254 です。
ステップ 7	**no shutdown** **Example:** switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	VRRP グループをイネーブルにします。デフォルトでは、ディセーブルです。
ステップ 8	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	（任意）VRRP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	（任意）この設定の変更を保存します。

VRRP の設定確認

VRRP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show vrrp	すべてのグループについて、VRRP ステータスを表示します。
show vrrp vr *group-number*	1 つの VRRP グループについて、VRRP ステータスを表示します。
show vrrp vr *number* **interface** *interface-type port* **configuration**	インターフェイスの仮想ルータ設定を表示します。
show vrrp vr *number* **interface** *interface-type port* **status**	インターフェイスの仮想ルータ ステータスを表示します。

VRRP 統計情報の表示

VRRP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show vrrp vr *number* **interface** *interface-type port* **statistics**	仮想ルータ情報を表示します。
show vrrp statistics	VRRP の統計情報を表示します。

特定のインターフェイスについて、IPv4 VRRP 統計情報を消去するには、**clear vrrp vr** コマンドを使用します。

VRRP の設定例

この例では、ルータ A およびルータ B はそれぞれ 3 つの VRRP グループに所属しています。コンフィギュレーションにおいて、各グループのプロパティは次のとおりです。

- グループ 1 :
  - 仮想 IP アドレスは 10.1.0.10 です。
  - ルータ A はプライオリティ 120 で、このグループのマスターになります。
  - アドバタイズ インターバルは 3 秒です。
  - プリエンプトはイネーブルです。
- グループ 5 :
  - ルータ B はプライオリティ 200 で、このグループのマスターになります。
  - アドバタイズ インターバルは 30 秒です。
  - プリエンプトはイネーブルです。
- グループ 100 :
  - ルータ A は、IP アドレスが上位（10.1.0.2）なので、このグループのマスターになります。
  - アドバタイズ インターバルはデフォルトの 1 秒です。
  - プリエンプトはディセーブルです。

ルータ A

```
interface ethernet 1/0
   no switchport
    ip address 10.1.0.2/16
    no shutdown
     vrrp 1
      priority 120
      authentication text cisco
      advertisement-interval 3
      address 10.1.0.10
      no shutdown
     vrrp 5
      priority 100
      advertisement-interval 30
      address 10.1.0.50
      no shutdown
```

```
    vrrp 100
     no preempt
     address 10.1.0.100
     no shutdown
```

ルータ B

```
interface ethernet 1/0
 no switchport
 ip address 10.2.0.1/2
 no shutdown
    vrrp 1
     priority 100
     authentication text cisco
     advertisement-interval 3
     address 10.2.0.10
     no shutdown

    vrrp 5
     priority 200
     advertisement-interval 30
     address 10.2.0.50
     no shutdown
    vrrp 100
     no preempt
     address 10.2.0.100
     no shutdown
```

その他の関連資料

VRRP の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.13-19）

関連資料

関連項目	マニュアル名
HSRP の設定	第 12 章「HSRP の設定」
VRRP CLI コマンド	『*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x*』

VRRP 機能の履歴

表 13-2 は、この機能のリリースの履歴です。

表 13-2　VRRP 機能の履歴

機能名	リリース	機能情報
VRRP	5.0(3)N1(1)	この機能が導入されました。

CHAPTER 14

オブジェクト トラッキングの設定

この章では、Cisco NX-OS スイッチ上でオブジェクト トラッキングを設定する方法について説明します。

この章では、次の内容について説明します。

オブジェクト トラッキング情報

オブジェクト トラッキングを使用すると、インターフェイス ライン プロトコル ステート、IP ルーティング、ルート到達可能性などの、スイッチ上の特定のオブジェクトをトラッキングし、トラッキング対象オブジェクトのステートが変化したときに対処できます。この機能により、ネットワークのアベイラビリティが向上し、オブジェクトがダウン状態となった場合の回復時間が短縮されます。

ここでは、次の内容について説明します。

オブジェクト トラッキングの概要

オブジェクト トラッキング機能を使用すると、トラッキング対象オブジェクトを作成できます。複数のクライアントでこのオブジェクトを使用し、トラッキング対象オブジェクトが変化したときのクライアント動作を変更できます。複数のクライアントがそれぞれの関心をトラッキング プロセスに登録し、同じオブジェクトをトラッキングし、オブジェクトのステートが変化したときに異なるアクションを実行します。

クライアントには次の機能が含まれます。

- ホットスタンバイ冗長プロトコル（HSRP）
- 仮想ルータ冗長プロトコル（VRRP）

オブジェクト トラッキングは、トラッキング対象オブジェクトのステータスをモニタし、変更があった場合は関係クライアントに伝えます。各トラッキング対象オブジェクトは、一意の番号で識別します。クライアントはこの番号を使用して、トラッキング対象オブジェクトのステートが変化したときに実行するアクションを設定できます。

Cisco NX-OS がトラッキングするオブジェクト タイプは、次のとおりです。

- インターフェイス ライン プロトコル ステート：ライン プロトコル ステートがアップまたはダウンかどうかをトラッキングします。
- インターフェイス IP ルーティング ステート：インターフェイスに IPv4 アドレスが設定されていて、IPv4 ルーティングがイネーブルでアクティブかどうかをトラッキングします。
- IP ルート到達可能性：IPv4 ルートが存在していて、ローカル スイッチから到達可能かどうかをトラッキングします。

たとえば、HSRP を設定すると、冗長ルータの 1 つをネットワークの他の部分に接続するインターフェイスのライン プロトコルをトラッキングできます。そのリンクがダウンした場合、影響のある HSRP ルータのプライオリティを変更できます。

オブジェクト トラッキング リスト

オブジェクト トラッキング リストを使用すると、複数のオブジェクトのステートをまとめてトラッキングできます。オブジェクト トラッキング リストは次の機能をサポートします。

- ブール「and」機能：トラッキング リスト オブジェクトがアップになるには、トラッキング リスト内に定義された各オブジェクトがアップ状態である必要があります。
- ブール「or」機能：トラッキング対象オブジェクトがアップになるには、トラッキング リスト内に定義された少なくとも 1 つのオブジェクトがアップ状態である必要があります。
- しきい値パーセンテージ：トラッキング対象リストに含まれるアップ オブジェクトのパーセンテージが、アップ状態になるトラッキング リストの設定されたアップしきい値を上回っている必要があります。トラッキング対象リストに含まれるダウン オブジェクトのパーセンテージが設定されたトラッキング リストのダウンしきい値を上回っている場合、トラッキング対象リストはダウンとしてマークされます。
- しきい値の重み：トラッキング対象リスト内の各オブジェクトに重み値を割り当て、トラッキング リストに重みしきい値を割り当てます。すべてのアップ オブジェクトの重み値の合計がトラッキング リストの重みアップしきい値を超えている場合、トラッキング リストはアップ状態になります。すべてのダウン オブジェクトの重み値の合計がトラッキング リストの重みダウンしきい値を超えている場合、トラッキング リストはダウン状態になります。

他のエンティティ（たとえば、仮想ポート チャネル（vPC））は、オブジェクト トラッキング リストを使用することにより、vPC を作成する複数のピア リンクのステートに基づいて vPC のステートを変更できます。vPC の詳細については、『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

トラック リストの詳細については、「ブール式を使用したオブジェクト トラッキング リストの設定」（P.14-6）を参照してください。

仮想化のサポート

オブジェクト トラッキングは VRF（仮想ルーティングおよびフォワーディング）インスタンスをサポートします。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS によりデフォルト VRF が使用されます。Cisco NX-OS はデフォルトで、デフォルト VRF のオブジェクトのルート到達可能ステートをトラッキングします。別の VRF のオブジェクトをトラッキングする場合は、その VRF のメンバとしてオブジェクトを設定する必要があります（「非デフォルト VRF のオブジェクト トラッキング設定」（P.14-13）を参照）。

詳細については、第 9 章「レイヤ 3 仮想化の設定」を参照してください。

オブジェクト トラッキングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	オブジェクト トラッキングにライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

注意事項および制約事項

オブジェクト トラッキング設定時の注意事項および制約事項は、次のとおりです。

- 最大 500 のトラッキング対象オブジェクトをサポートします。
- イーサネット、サブインターフェイス、トンネル、ポート チャネル、ループバック インターフェイス、および VLAN インターフェイスをサポートします。
- HSRP グループごとに 1 つのトラッキング対象オブジェクトをサポートします。

デフォルト設定

表 14-1 に、オブジェクト トラッキング パラメータのデフォルト設定を示します。

表 14-1　デフォルトのオブジェクト トラッキング パラメータ

パラメータ	デフォルト
Tracked Object VRF	デフォルト VRF のメンバ

オブジェクト トラッキングの設定

ここでは、次の内容について説明します。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

インターフェイスのオブジェクト トラッキング設定

インターフェイスのライン プロトコルまたは IPv4 ルーティングのステートをトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track** *object-id* **interface** *interface-type number* {**ip routing** | **line-protocol**}
3. （任意）**show track** [*object-id*]
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**track** *object-id* **interface** *interface-type number* {**ip routing** | **line-protocol**}
	
	Example:
	`switch(config)# track 1 interface ethernet 1/2 line-protocol`
	`switch(config-track#`
		インターフェイスのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。*object-id* の範囲は 1 ～ 500 です。

	コマンド	目的
ステップ 3	**show track** [*object-id*] **Example:** switch(config-track)# show track 1	（任意）オブジェクト トラッキング情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

Ethernet 1/2 上でライン プロトコル ステートのオブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 interface ethernet 1/2 line-protocol
switch(config-track)# copy running-config startup-config
```

Ethernet 1/2 上で IPv4 ルーティング ステートのオブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 2 interface ethernet 1/2 ip routing
switch(config-track)# copy running-config startup-config
```

ルート到達可能性のオブジェクト トラッキング設定

IP ルートの存在および到達可能性をトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track** *object-id* **ip route** *prefix/length* **reachability**
3. （任意）**show track** [*object-id*]
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-id* **ip route** *prefix/length* **reachability** **Example:** switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。*object-id* の範囲は 1 ～ 500 です。IP のプレフィクス フォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。

	コマンド	目的
ステップ 3	**show track** [*object-id*] **Example:** switch(config-track)# show track 1	（任意）オブジェクト トラッキング情報を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

デフォルト VRF で、IPv4 ルートのオブジェクト トラッキングを設定する例を示します。

```
switch# configure terminal
switch(config)# track 4 ip route 192.0.2.0/8 reachability
switch(config-track)# copy running-config startup-config
```

ブール式を使用したオブジェクト トラッキング リストの設定

複数のトラッキング対象オブジェクトを含むオブジェクト トラッキング リストを設定できます。トラッキング対象リストには 1 つまたは複数のオブジェクトが含まれます。ブール式では、「and」または「or」演算子を使用して 2 種類の演算を実行できます。たとえば、「and」演算子を使用して 2 つのインターフェイスをトラッキングする場合、「アップ」は両方のインターフェイスがアップであることを意味し、「ダウン」はどちらかのインターフェイスがダウンであることを意味します。

手順の概要

1. **configure terminal**
2. **track** *track-number* **list boolean** {**and** | **or**}
3. **object** *object-number* [**not**]
4. （任意）**show track**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list boolean** {**and** | **or**} **Example:** switch(config)# track 1 list boolean and switch(config-track#	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。トラッキング対象リストのステートがブール式に基づいて決まることを指定します。キーワードは次のとおりです。 • **and**：すべてのオブジェクトがアップの場合にリストがアップになり、1 つ以上のオブジェクトがダウンの場合にリストがダウンになることを指定します。たとえば、2 つのインターフェイスをトラッキングする場合、「アップ」は両方のインターフェイスがアップであることを意味し、「ダウン」はどちらかのインターフェイスがダウンであることを意味します。 • **or**：少なくとも 1 つのオブジェクトがアップの場合にリストがアップになることを指定します。たとえば、2 つのインターフェイスをトラッキングする場合、「アップ」はどちらかのインターフェイスがアップであることを意味し、「ダウン」は両方のインターフェイスがダウンであることを意味します。 *track-number* の範囲は 1 ～ 500 です。
ステップ 3	**object** *object-id* [**not**] **Example:** switch(config-track)# object 10	トラッキング リストにトラッキング対象オブジェクトを追加します。*object-id* の範囲は 1 ～ 500 です。オプションの **not** キーワードを指定すると、トラッキング対象オブジェクトのステートが否定されます。 **（注）** 例では、オブジェクト 10 がアップのときに、トラッキング対象リストがオブジェクト 10 をダウンとして検出します。
ステップ 4	**show track** **Example:** switch(config-track)# show track	（任意）オブジェクト トラッキング情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、複数のオブジェクトを含むトラッキング リストをブール「and」で設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list boolean and
switch(config-track)# object 10
switch(config-track)# object 20 not
```

パーセンテージしきい値を使用したオブジェクト トラッキング リストの設定

パーセンテージしきい値を含むオブジェクト トラッキング リストを設定できます。トラッキング対象リストには 1 つまたは複数のオブジェクトが含まれます。トラッキング リストがアップ状態になるには、アップ オブジェクトのパーセンテージがトラッキング リストに設定されたパーセントしきい値を超えている必要があります。たとえば、追跡対象リストに 3 つのオブジェクトが含まれており、アップしきい値を 60 % に設定した場合は、2 つのオブジェクト（全オブジェクトの 66 %）がアップ状態になるまで、追跡リストがアップ状態になりません。

手順の概要

1. **configure terminal**
2. **track** *track-number* **list threshold percentage**
3. **threshold percentage up** *up-value* **down** *down-value*
4. **object** *object-number*
5. （任意）**show track**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**track** *track-number* **list threshold percentage**
	
	Example:
	`switch(config)# track 1 list threshold percentage`
	`switch(config-track#`
		トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。トラッキング対象リストのステートが設定されたしきい値パーセントに基づいて決まることを指定します。
		
		track-number の範囲は 1 ～ 500 です。

ステップ 3	**threshold percentage up** *up-value* **down** *down-value* **Example:** `switch(config-track)# threshold percentage up 70 down 30`	トラッキング対象リストのしきい値パーセントを設定します。指定できる範囲は 0 ～ 100% です。
ステップ 4	**object** *object-id* **Example:** `switch(config-track)# object 10`	トラッキング リストにトラッキング対象オブジェクトを追加します。*object-id* の範囲は 1 ～ 500 です。

	コマンド	目的
ステップ 5	**show track** **Example:** switch(config-track)# show track	（任意）オブジェクト トラッキング情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、アップしきい値が 70 % でダウンしきい値が 30 % の追跡リストを設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold percentage
switch(config-track)# threshold percentage up 70 down 30
switch(config-track)# object 10
switch(config-track)# object 20
switch(config-track)# object 30
```

重みしきい値を使用したオブジェクト トラッキング リストの設定

重みしきい値を含むオブジェクト トラッキング リストを設定できます。トラッキング対象リストには 1 つまたは複数のオブジェクトが含まれます。トラッキング リストがアップ ステートになるには、アップ オブジェクトの重み値の合計がトラッキング リストに設定されたアップ重みしきい値を超えている必要があります。たとえば、トラッキング対象リストに重み値がデフォルトの 10 である 3 つのオブジェクトがあり、アップしきい値を 15 に設定した場合、トラッキング リストがアップ状態になるには、2 つのオブジェクトがアップ状態になる（重み値の合計が 20 になる）必要があります。

手順の概要

1. **configure terminal**
2. **track** *track-number* **list threshold weight**
3. **threshold weight up** *up-value* **down** *down-value*
4. **object** *object-number* **weight** *value*
5. （任意）**show track**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *track-number* **list threshold weight** **Example:** switch(config)# track 1 list threshold weight switch(config-track#	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。トラッキング対象リストのステートが設定されたしきい値重みに基づいて決まることを指定します。 *track-number* の範囲は 1 ～ 500 です。
ステップ 3	**threshold weight up** *up-value* **down** *down-value* **Example:** switch(config-track)# threshold weight up 30 down 10	トラッキング対象リストのしきい値重みを設定します。指定できる範囲は 1 ～ 255 です。
ステップ 4	**object** *object-id* **weight** *value* **Example:** switch(config-track)# object 10 weight 15	トラッキング リストにトラッキング対象オブジェクトを追加します。*object-id* の範囲は 1 ～ 500 です。*value* の範囲は 1 ～ 255 です。デフォルトの重み値は 10 です。
ステップ 5	**show track** **Example:** switch(config-track)# show track	（任意）オブジェクト トラッキング情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、トラッキング リストのアップ重みしきい値を 30、ダウンしきい値を 10 にそれぞれ設定する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
```

この例では、オブジェクト 10 とオブジェクト 20 がアップの場合にトラッキング リストがアップになり、3 つのオブジェクトがすべてダウンの場合にトラッキング リストがダウンになります。

オブジェクト トラッキング遅延の設定

トラッキング対象オブジェクトまたはオブジェクト トラッキング リストに対して、オブジェクトまたはリストがステートの変化を開始したときに適用する遅延を設定できます。トラッキング対象オブジェクトまたはトラッキング リストは、ステートの変化が発生したときに遅延タイマーを開始しますが、遅延タイマーが切れるまでステートの変化を認識しません。遅延タイマーが切れると、Cisco NX-OS

は再びオブジェクトのステートを確認し、オブジェクトまたはリストが現在も変更されたステートのままだった場合にだけステートの変化を記録します。オブジェクト トラッキングは遅延タイマーが切れる前の中間的なステートの変化を無視します。

たとえば、インターフェイス ライン プロトコルのトラッキング対象オブジェクトがアップ ステートであり、ダウン遅延が 20 秒に設定されている場合は、ライン プロトコルがダウンになると遅延タイマーが開始します。20 秒後にライン プロトコルがダウンになっていなければ、このオブジェクトはダウン ステートになりません。

トラッキング対象オブジェクトまたはトラッキング リストには、独立したアップ遅延とダウン遅延を設定できます。遅延を削除すると、オブジェクト トラッキングからアップ遅延とダウン遅延の両方が削除されます。

遅延は任意の時点で変更できます。オブジェクトまたはリストがトリガーされたイベントから遅延タイマーをすでにカウントしている場合は、次のようにして新しい遅延が計算されます。

- 新しい設定値が古い設定値より小さい場合は、新しい値でタイマーが開始します。
- 新しい設定値が古い設定値より大きい場合は、新しい設定値から現在のタイマーのカウントダウンを引き、古い設定値を引いたものがタイマーになります。

手順の概要

1. **configure terminal**
2. **track** *object-id* {*parameters*}
3. **track** *track-number* **list** {*parameters*}
4. **delay** {***up*** *up-time* [***down*** *down-time*] | ***down*** *down-time* [***up*** *up-time*]}
5. （任意）**show track**
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-id* {*parameters*} **Example:** switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。*object-id* の範囲は 1 ～ 500 です。IP のプレフィクス フォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。
ステップ 3	**track** *track-number* **list** {*parameters*} **Example:** switch(config)# track 1 list threshold weight switch(config-track#	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。トラッキング対象リストのステートが設定されたしきい値重みに基づいて決まることを指定します。 *track-number* の範囲は 1 ～ 500 です。

	コマンド	目的
ステップ 4	**delay** {**up** *up-time* [**down** *down-time*] | **down** *down-time* [**up** *up-time*]} **Example:** switch(config-track)# delay up 20 down 30	オブジェクトの遅延タイマーを設定します。指定できる範囲は 0 ～ 180 秒です。
ステップ 5	**show track** **Example:** switch(config-track)# show track 3	（任意）オブジェクト トラッキング情報を表示します。
ステップ 6	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、ルートのオブジェクト トラッキングを設定し、遅延タイマーを使用する例を示します。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# delay up 20 down 30
switch(config-track)# copy running-config startup-config
```

次に、トラッキング リストのアップ重みしきい値を 30、ダウンしきい値を 10 にそれぞれ設定し、遅延タイマーを使用する例を示します。

```
switch# configure terminal
switch(config)# track 1 list threshold weight
switch(config-track)# threshold weight up 30 down 10
switch(config-track)# object 10 weight 15
switch(config-track)# object 20 weight 15
switch(config-track)# object 30
switch(config-track)# delay up 20 down 30
```

次に、インターフェイスがシャットダウンする前後の show track コマンドの出力に表示された遅延タイマーの例を示します。

```
switch(config-track)# show track
Track 1
  Interface loopback1 Line Protocol
  Line Protocol is UP
  1 changes, last change 00:00:13
  Delay down 10 secs

switch(config-track)# interface loopback 1
switch(config-if)# shutdown
switch(config-if)# show track
Track 1
  Interface loopback1 Line Protocol
  Line Protocol is delayed DOWN (8 secs remaining)<------- delay timer counting down
  1 changes, last change 00:00:22
  Delay down 10 secs
```

非デフォルト VRF のオブジェクト トラッキング設定

特定の VRF でオブジェクトをトラッキングするように Cisco NX-OS を設定できます。

手順の概要

1. **configure terminal**
2. **track** *object-id* **ip route** *prefix/length* **reachability**
3. **vrf member** *vrf-name*
4. （任意）**show track** [*object-id*]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**track** *object-id* **ip route** *prefix/length* **reachability** **Example:** switch(config)# track 2 ip route 192.0.2.0/8 reachability switch(config-track)#	ルートのトラッキング対象オブジェクトを作成し、トラッキング コンフィギュレーション モードを開始します。*object-id* の範囲は 1 ～ 500 です。IP のプレフィクス フォーマットは A.B.C.D/length です。length の範囲は 1 ～ 32 です。
ステップ 3	**vrf member** *vrf-name* **Example:** switch(config-track)# vrf member Red	設定されたオブジェクトのトラッキングに使用する VRF を設定します。
ステップ 4	**show track** [*object-id*] **Example:** switch(config-track)# show track 3	（任意）オブジェクト トラッキング情報を表示します。
ステップ 5	**copy running-config startup-config** **Example:** switch(config-track)# copy running-config startup-config	（任意）この設定の変更を保存します。

ルートのオブジェクト トラッキングを設定し、VRF Red を使用して、そのオブジェクトの到達可能性情報を調べる例を示します。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)# copy running-config startup-config
```

トラッキング対象オブジェクト 2 を変更し、VRF Red の代わりに VRF Blue を使用して、そのオブジェクトの到達可能性情報を調べる例を示します。

```
switch# configure terminal
switch(config)# track 2
```

```
switch(config-track)# vrf member Blue
switch(config-track)# copy running-config startup-config
```

オブジェクト トラッキングの設定確認

オブジェクト トラッキングの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show track [*object-id*] [**brief**]	1 つまたは複数のオブジェクトについて、オブジェクト トラッキング情報を表示します。
show track [*object-id*] **interface** [**brief**]	インターフェイスベースのオブジェクト トラッキング情報を表示します。
show track [*object-id*] **ip route** [**brief**]	IPv4 ルートベースのオブジェクト トラッキング情報を表示します。

オブジェクト トラッキングの設定例

次に、ルート到達可能性のオブジェクト トラッキングを設定し、VRF Red を使用してそのルートの到達可能性情報を調べる例を示します。

```
switch# configure terminal
switch(config)# track 2 ip route 209.165.201.0/8 reachability
switch(config-track)# vrf member Red
switch(config-track)# copy running-config startup-config
```

関連資料

オブジェクト トラッキングの関連情報については、次の項目を参照してください。

- 第 9 章「レイヤ 3 仮想化の設定」
- 第 12 章「HSRP の設定」

その他の関連資料

オブジェクト トラッキングの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.14-15）
- 「標準」（P.14-15）

関連資料

関連項目	マニュアル名
オブジェクト トラッキング CLI コマンド	*『Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x』*

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

オブジェクト トラッキング機能の履歴

表 14-2 は、この機能のリリースの履歴です。

表 14-2　オブジェクト トラッキング機能の履歴

機能名	リリース	機能情報
オブジェクト トラッキング	5.0(3)N1(1)	この機能が導入されました。

APPENDIX A

Cisco NX-OS Unicast Features Release 5.0(3)N1(1) がサポートする IETF RFC

この付録は、Cisco NX-OS Release 5.0(3)N1(1) がサポートする IETF RFC の一覧です。

BGP の RFC

RFC	タイトル
RFC 1997	*『BGP Communities Attribute』*
RFC 2385	*『Protection of BGP Sessions via the TCP MD5 Signature Option』*
RFC 2439	*『BGP Route Flap Damping』*
RFC 2519	*『A Framework for Inter-Domain Route Aggregation』*
RFC 2858	*『Multiprotocol Extensions for BGP-4』*
RFC 3065	*『Autonomous System Confederations for BGP』*
RFC 3392	*『Capabilities Advertisement with BGP-4』*
RFC 4271	*『A Border Gateway Protocol 4 (BGP-4)』*
RFC 4273	*『Definitions of Managed Objects for BGP-4』*
RFC 4456	*『BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)』*
RFC 4486	*『Subcodes for BGP Cease Notification Message』*
RFC 4893	*『BGP Support for Four-octet AS Number Space』*
RFC 5004	*『Avoid BGP Best Path Transitions from One External to Another』*
draft-ietf-idr-bgp4-mib-15.txt	*『BGP4-MIB』*

First-Hop Redundancy Protocol の RFC

RFC	タイトル
RFC 2281	『Hot Standby Redundancy Protocol』
RFC 3768	『Virtual Router Redundancy Protocol』

IP サービスに関する RFC の参考資料

RFC	タイトル
RFC 786	『UDP』
RFC 791	『IP』
RFC 792	『ICMP』
RFC 793	『TCP』
RFC 826	『ARP』
RFC 1027	『Proxy ARP』
RFC 1591	『DNS Client』
RFC 1812	『IPv4 routers』

OSPF の RFC

RFC	タイトル
RFC 2328	『OSPF Version 2』
RFC 3101	『The OSPF Not-So-Stubby Area (NSSA) Option』
RFC 2370	『The OSPF Opaque LSA Option』
RFC 3137	『OSPF Stub Router Advertisement』

RIP の RFC

RFC	タイトル
RFC 2453	『RIP Version 2』
RFC 2082	『RIP-2 MD5 Authentication』

GLOSSARY

A

ABR エリア境界ルータを参照してください。

ARP Address Resolution Protocol（アドレス解決プロトコル）。ARP は既知の IPv4 アドレスに対応する MAC アドレスを検出します。

AS 自律システムを参照してください。

ASBR 自律システム境界ルータを参照してください。

AVF Active Virtual Forwarder（アクティブ バーチャル フォワーダ）。特定のバーチャル MAC アドレスにトラフィックを転送するために選定された、GLBP グループ内のゲートウェイ。

AVG Active Virtual Gateway（アクティブ バーチャル ゲートウェイ）。アクティブ バーチャル ゲートウェイとして選択され、プロトコルの動作を担当する、GLBP グループ内の 1 つのバーチャル ゲートウェイ。

B

BDR Backup Designated Router（バックアップ指定ルータ）。マルチアクセス OSPF ネットワークにおいて、指定ルータで障害が発生した場合に、バックアップとして動作するように選定されたルータ。すべてのネイバーは、指定ルータと同様、バックアップ指定ルータ（BDR）とも隣接関係を形成します。

BGP Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。BGP はドメイン間または外部ゲートウェイ プロトコルです。

BGP ピア ローカル BGP スピーカとネイバー関係が確立されている、リモート BGP スピーカ。

BGP スピーカ BGP 対応ルータ。

D

DHCP Dynamic Host Control Protocol（動的ホスト制御プロトコル）。

DNS クライアント Domain Name System（ドメイン ネーム システム）クライアント。DNS サーバと通信し、ホスト名を IP アドレスに変換します。

DR Designated Router（指定ルータ）。マルチアクセス OSPF ネットワークにおいて、すべての隣接ネイバーに代わって LSA を送信するように選定されたルータ。すべてのネイバーは、指定ルータおよびバックアップ指定ルータとだけ隣接関係を確立します。

DUAL Diffusing Update Algorithm（拡散更新アルゴリズム）。宛先への最適ルートを選択するための EIGRP アルゴリズム。

E

eBGP 外部 BGP（ボーダー ゲートウェイ プロトコル）。外部システム間で動作します。

EIGRP Enhanced Interior Gateway Protocol。拡散更新アルゴリズムを使用して高速コンバージェンスを実現し、帯域幅の使用率を最小限に抑える、シスコのルーティング プロトコルです。

F

FIB Fowarding Information Base（転送情報ベース）。パケットごとにレイヤ 3 フォワーディングを決定するために使用される、各モジュール上のフォワーディング テーブル。

H

hello 間隔 OSPF または EIGRP ルータが hello パケットを送信する、設定可能な間隔。

hello パケット OSPF または IS-IS がネイバー検出のために使用する、特殊なメッセージ。確立されたネイバー間のキープ アライブ メッセージとしても機能します。

I

iBGP 内部ボーダー ゲートウェイ プロトコル（BGP）。自律システム内で動作します。

ICMP

IETF RFC インターネット技術特別調査委員会コメント要求。

IGP Interior gateway protocol。同じ自律システム内のルータ間で使用されます。

IP トンネル

IPv4 インターネット プロトコル バージョン 4。

L

LSA Link-state Advertisement（リンクステート アドバタイズメント）。リンクの動作状態、リンク コスト、およびその他の OSPF ネイバー情報を共有するための OSPF メッセージ。

M

MD5 認証ダイジェスト 認証キーおよび元のメッセージに基づいて計算される、暗号構築物。メッセージとともに宛先に送信されます。宛先は送信側の正統性を判別し、送信中にメッセージが改ざんされていない保証を得られます。

MTU Maximum Transmission Unit（最大伝送ユニット）。ネットワーク リンクで分割しないで送信できる、最大パケット サイズ。

N

NSSA Not-So-Stubby-Area。OSPF エリアにおいて、AS External LSA を制限します。

O

OSPF Open Shortest Path First。IETF リンクステート プロトコル。OSPFv2 は IPv4 をサポートしています。

R

Reliable Transport Protocol すべてのネイバーに EIGRP パケットを保証付きで順序正しく配信する役目を担います。

RIB Routing Information Base（ルーティング情報ベース）。直接接続ルート、スタティック ルート、およびダイナミック ユニキャスト ルーティング プロトコルから学習したルートからなる、ルーティング テーブルを維持します。

S

SPF アルゴリズム 最短パス優先アルゴリズム。ネットワーク経由で特定の宛先までの最短ルートを判別するために、OSPF で使用されるダイクストラ アルゴリズム。

SVI スイッチ仮想インターフェイス。

U

UFIB ユニキャスト IPv4 転送情報ベース。

URIB ユニキャスト IPv4 ルーティング情報ベース。すべてのルーティング プロトコルから情報を集め、各モジュールの転送情報ベースをアップデートする、ユニキャスト ルーティング テーブル。

V

VRF Virtual Routing and Forwarding（仮想ルーティングおよびフォワーディング）。システム内部で別個の独立したレイヤ 3 エンティティを作成するための方法。

VRRP Virtual Router Redundancy Protocol（仮想ルータ冗長プロトコル）。

あ

アドレス ファミリ ルーティング プロトコルがサポートする特定のネットワーク アドレッシング タイプ。IPv4 ユニキャスト、IPv4 マルチキャストなど。

アドミニストレーティブ ディスタンス ルーティング情報源の信頼性に関する格付け。通常、値が大きいほど、信頼性の格付けが下がります。

い

インスタンス 独立した設定可能なエンティティ。通常はプロトコル。

え

エリア OSPF ドメイン内の独立したサブドメインを形成する、ルータおよびリンクからなる論理区分。LSA フラッディングはエリア内に封じ込められます。

エリア境界ルータ ある OSPF エリアを別の OSPF エリアに接続するルータ。

か

拡散更新アルゴリズム DUAL を参照してください。

仮想化 物理エンティティを複数の独立した論理エンティティとして動作させる 1 つの方法。

き

キープアライブ ルーティング ペア間の通信を確認して維持するために、ピア間で送信される特殊なメッセージ。

け

ゲートウェイ LAN からの Layer 3 トラフィックをその他のネットワークに転送するスイッチまたはルータ。

こ

コンバージェンス 収束を参照してください。

さ

再配布 あるルーティング プロトコルが別のルーティング プロトコルからルート情報を受け入れ、ローカル自律システムでそれをアドバタイズします。

し

指定ルータ DR を参照してください。

収束 ネットワーク内のすべてのルータが同じルーティング情報を得るポイント。

自律システム 単一のテクニカル アドミニストレーション エンティティによって制御されるネットワーク。

自律システム境界ルータ OSPF 自律システムを外部の自律システムに接続するルータ。

信頼性 各ネットワーク リンクに頼れるかどうか（通常は、ビット誤り率で表します）。

す

スプリット ホライズン ルータが自身のルート アップデートを見ないように、ルートの学習元になったインターフェイスには、学習したルートをアドバタイズしません。

スタティック ルート 手動で設定されたルート。

スタブ エリア AS External（type 5）LSA を認めない OSPF エリア。

スタブ ルータ メイン ネットワークへの直接接続がなく、既知のリモート ルータを使用してメイン ネットワークにルーティングされるルータ。

そ

属性 BGP UPDATE メッセージで送信される、ルートのプロパティ。これらの属性には、アドバタイズされた宛先へのパスとともに、ベスト パス選択プロセスを変更する、設定可能なオプションがあります。

た

帯域幅 リンクの使用可能なトラフィック容量。

ち

遅延 システムから宛先にインターネットワークを介してパケットを転送するために必要な時間。

つ

通信コスト リンクを介してルーティングする運用コストの算定基準。

て

デッド間隔 その範囲内で OSPF ルータが OSPF ネイバーから hello パケットを受信しなければならない時間。デッド間隔は通常、hello 間隔の倍数です。hello パケットを受信しなかった場合、ネイバーの隣接関係は削除されます。

デフォルト ゲートウェイ あらゆるルーティング不能パケットの送信先となるルータ。ラスト リゾート ルータともいいます。

ディスタンス ベクトル 距離（宛先までのホップ数など）および方向（ネクストホップ ルータなど）によってルートを定義し、さらに直接接続されたネイバー ルータにブロードキャストします。

ね

ネットワーク層到達可能性情報 BGP network layer reachability information（NRLI）。アドバタイズ側 BGP ピアから到達可能な、ネットワーク IP アドレスおよびネットワークに対応するネットワーク マスクのリストが含まれます。

ネクスト ホップ 宛先アドレスまでの間で、パケットの次の送信先になるルータ。

は

パス長 送信元から宛先までのルーティングにおいて、パケットが経験するすべてのリンク コストおよびホップ カウントの合計。

バックアップ指定ルータ BDR を参照してください。

ふ

フィジブル ディスタンス EIGRP で計算された、ネットワークの宛先までの最短距離。フィジブル ディスタンスは、ネイバーがアドバタイズした距離に、そのネイバーへのリンク コストを加えた合計です。

フィジブル サクセサ 現在のフィジブル ディスタンスより短い宛先までの距離をアドバタイズした、EIGRP のネイバー。

負荷 ルータなどのネットワーク リソースが使用中になっている程度。

ほ

ホールド タイム BGP において、UPDATE または KEEPALIVE メッセージの間隔として許容される最大時間限度。この時間を超えると、BGP ピア間の TCP 接続が終了します。

EIGRP では、EIGRP hello メッセージの間隔として許容される最大時間。この時間を超えると、ネイバーが到達不能として宣言されます。

ポイズン リバースを指定したスプリット ホライズン ルータが自身のルート アップデートを見ないように、インターフェイスから学習したルートを到達不能として設定し、ルートの学習元になったインターフェイスには、学習したルートをアドバタイズしません。

ホップ カウント ルート上で経由できるルータの数。RIP で使用されます。

め

メッセージ ダイジェスト 共有パスワードを使用するメッセージに適用される、一方向ハッシュ。メッセージを認証し、メッセージが送信中に変更されていないことを保証するために、メッセージに付加されます。

メトリック パス帯域幅など、宛先への最適パスを決定するためにルーティング アルゴリズムが使用する、標準の測定単位。

り

リンク コスト OSPF インターフェイス上で設定された、最短パス優先計算に含まれる任意の値。

リンクステート 隣接ルータとのリンク、リンク コストに関する情報の共有。

リンクステート アドバタイズメント LSA を参照してください。

リンクステート データベース 受信したすべての LSA に関する OSPF データベース。OSPF ではこのデータベースを使用して、ネットワーク上の各宛先に最適なパスを計算します。

リンクステート リフレッシュ すべての OSPF ルータが同じ情報を持っていることを保証するために、OSPF が LSA をネットワークにフラッディングする時間。

隣接関係 コンフィギュレーションに互換性があり、リンクステート データベースが同期している 2 つの OSPF ルータ。

る

ルーティング情報ベース RIB を参照してください。

ルート マップ 一致基準に基づいてルートまたはパケットをマッピングし、任意で設定基準に基づいてルートまたはパケットを変更するために使用される構築物。ルート再配布に使用されます。

ルート集約 ルート テーブル内の関連した一連の固有ルートを汎用性の高いルートに置き換えるプロセス。

ルータ ID ルーティング プロトコルで使用される一意の識別情報。手動で設定しなかった場合は、ルーティング プロトコルがシステムに設定されている最大の IP アドレスを選択します。

ろ

ロード バランシング 所定の宛先に複数のパスを使用してネットワーク トラフィックを配信すること。

INDEX

A

B

D

E

F

G

H

I

M

N

O

R

U

V

あ

い

お

か

こ

さ

し

す

た

ち

つ

て

と

な

ね

は

ひ

ふ

ほ

ま

ら

り

る

れ

ろ