# Cisco DCNM Unicast Routing コンフィギュレーション ガイド Release 4.0

October 2008

Text Part Number: OL-15806-01-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、米国シスコシステムズ発行ドキュメントの参考和訳です。**
**米国サイト掲載ドキュメントとの差異が生じる場合があるため、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 DCNM Unicast Routing コンフィギュレーション ガイド Release 4.0*

# CONTENTS

# はじめに

このマニュアルでは、Cisco DCNM 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。

## 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。

## マニュアルの構成

このマニュアルは、次の章で構成されています。

| 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「IPv6 の設定」 | IPv6 の設定および管理方法について説明します。 |
| 第 4 章「GLBP の設定」 | GLBP を設定する手順について説明します。 |
| 第 5 章「オブジェクト トラッキングの設定」 | オブジェクト追跡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 4.x がサポートする IETF RFC」 | Cisco NX-OS でサポートされる IETF RFC の一覧です。 |

## 表記法

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*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

**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 DCNM のマニュアルについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Cisco DCNM のマニュアル セットには、次のマニュアルが含まれます。

## リリース ノート

『*Cisco DCNM Release Notes, Release 4.0*』

## DCNM コンフィギュレーション ガイド

『*Cisco DCNM Getting Started with Virtual Device Contexts, Release 4.0*』

『*Cisco DCNM Fundamentals Configuration Guide, Release 4.0*』

『*Cisco DCNM Interfaces Configuration Guide, Release 4.0*』

『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 4.0*』

『*Cisco DCNM Web Services API Guide, Release 4.0*』

『*Cisco DCNM Security Configuration Guide, Release 4.0*』

『*Cisco DCNM Unicast Routing Configuration Guide, Release 4.0*』

『*Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0*』

# マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、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

## シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

## Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

## その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

  http://www.cisco.com/go/services

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

CHAPTER 1

# 概要

Cisco Datacenter Network Manager（DCNM）は、IP アドレス指定、オブジェクト追跡、および Gateway Load Balancing Protocol（GLBP）をサポートします。

ここでは、次の内容を説明します。



Cisco NX-OS は、FIB を分割して、複数のアドレス ファミリをサポートします。FIB TCAM は 128K の物理エントリで、デフォルトで次のセクションのように分割されます。

- 56K IPv4 ユニキャスト ルータ（56K 物理エントリ）
- 32K IPv4 マルチキャスト ルータまたは IPv6 ユニキャスト ルータ（64K 物理エントリ）
- 2K IPv6 マルチキャスト ルータ（8K 物理エントリ）

**（注）** FIB のデフォルト セクションを変更することはできません。

**（注）** すべての IPv4 インターネット ルート テーブルには 256K 以上のルートがあり、Cisco NX-OS FIB エントリ最大数を超えます。

## IPv4 と IPv6

レイヤ 3 は、IPv4 プロトコルまたは IPv6 プロトコルを使用します。IPv6 は新しい IP プロトコルで、世界中で広く展開され、使用されているインターネット プロトコルである IPv4 に代わるものとして設計されました。IPv6 では、ネットワーク アドレス ビット数が 32 ビット（IPv4 の場合）から 128 ビットに増やされています。詳細については、第 2 章「IPv4 の設定」または第 3 章「IPv6 の設定」を参照してください。

# First-Hop Redundancy Protocol（FHRP）

FHRP を使用すると、ホストで冗長接続が可能となります。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。Gateway Load Balancing Protocol（GLBP）の詳細については、第 4 章「GLBP の設定」を参照してください。

# オブジェクト追跡

オブジェクト追跡を使用すると、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の向上し、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 5 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。

CHAPTER 2

# IPv4 の設定

この章では、デバイス上で Internet Protocol version 4（IPv4）を設定する方法について説明します。

ここでは、次の内容を説明します。

# IPv4 について

デバイス上で IP を設定し、ネットワーク インターフェイスに IP アドレスを割り当てることができます。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、デバイス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。デバイスが生成したパケットは、つねにプライマリ 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 デバイスは、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 アドレスには、ネットワーク アドレスとホスト アドレスが含まれます。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、スーパーバイザ モジュールで終端する IPv4 パケットを処理し、IPv4 パケットを転送する役割を果たしています。この役割には、IPv4 ユニキャスト / マルチキャスト ルート ルックアップ、RPF チェック、およびソフトウェア アクセス コントロール リスト / ポリシーベース ルーティング（ACL/PBR）転送が含まれます。また、IP 機能は、ネットワーク インターフェイス 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、および 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。



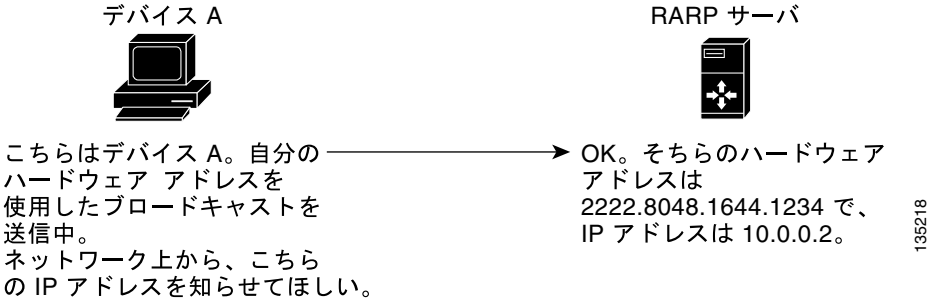
## 複数の IPv4 アドレス

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。もっと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、同時に複数のアクティブなインターフェイス上に表示することはできません。

**（注）** ネットワーク セグメント上のいずれかのデバイスがセカンダリ 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デバイスも、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。

**図 2-1　Reverse ARP**




## 仮想化サポート

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。VRF は Virtual Device Contexts（VDC; 仮想化デバイス コンテキスト）内にあります。特に VDC および VRF を設定しないかぎり、デフォルトで、Cisco NX-OS はユーザにデフォルト VDC およびデフォルト VRF を使用させます。詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』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 |
|---|---|
| DCNM | IP 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ない機能はいずれも、Cisco DCNM にバンドルされており、無償で提供されます。DCNM ライセンス方式の詳細については、『*Cisco DCNM Licensing Guide*』を参照してください。 |
| NX-OS | IP 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、Cisco NX-OS システム イメージにバンドルされて提供されます。追加料金は発生しません。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。

- レイヤ 3 インターフェイス上でのみ設定可能です。

# 注意事項および制約事項

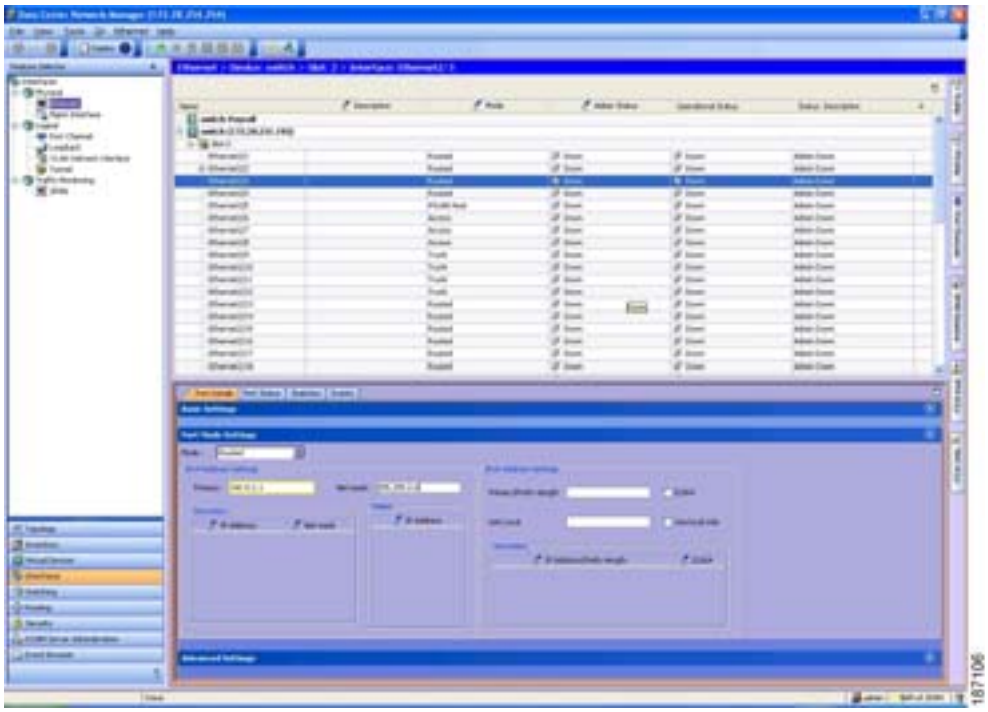
IPv4 には、次の注意事項、および制約、制限事項があります。

- 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のみ設定できます。

# IPv4 の設定

インターフェイス機能選択により、レイヤ 3 インターフェイスに IP アドレスを指定することができます。図 2-2 にレイヤ 3 インターフェイスを示します。

**図 2-2　レイヤ 3 インターフェイスの設定**




Data Center Network Manager 機能の詳細については、『*Cisco Data Center Network Manager Fundamentals Guide*』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。

- IPv4 アドレス指定の設定（p.2-5）
- 複数の IP アドレスの設定（p.2-6）

# 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。

## 詳細な手順

ルーテッド インターフェイスに IPv4 アドレスを設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインから、**Interfaces > Physical > Ethernet** の順に選択します。

Summary ペインに使用できるデバイスが表示されます（図 2-2 を参照）。

**ステップ 2**　Summary ペインでデバイスをダブルクリックして、スロットの一覧を表示します。

**ステップ 3**　スロットをダブルクリックして、インターフェイスの一覧を表示します。

**ステップ 4**　ルーテッド インターフェイスとして設定したいインターフェイスをクリックします。

Summary ペインのインターフェイスが強調表示され、Details ペインにタブが表示されます。

**ステップ 5**　Details ペインで、**Port Details** タブをクリックします。

Port Details タブが表示されます。

**ステップ 6**　Port Details タブで、**Port Mode Settings** セクションを展開表示します。

ポート モードが表示されます。

**ステップ 7**　Mode ドロップダウン リストから、**Routed** を選択します。

Details ペインに IP アドレス情報が表示され、Cisco NX-OS はレイヤ 2 設定を削除します。

**ステップ 8**　（任意）IPv4 Address Settings の Primary フィールドから、このルーテッド インターフェイスに IPv4 アドレスを設定します。

**ステップ 9**　（任意）Net マスク フィールドからネットワーク マスクを使用して、この IPv4 アドレスをドット付き 10 進数で表記します。

**ステップ 10**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# 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のみ追加できます。

## 詳細な手順

IPv4 セカンダリ アドレスまたはヘルパー アドレスをルーテッド インターフェイスに設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインから、**Interfaces > Physical > Ethernet** の順に選択します。

Summary 画面に使用できるデバイスが表示されます（図 2-2 を参照）。

**ステップ 2**　Summary ペインでデバイスをダブルクリックして、スロットの一覧を表示します。

**ステップ 3**　スロットをダブルクリックして、インターフェイスの一覧を表示します。

**ステップ 4**　ルーテッド インターフェイスとして設定したいインターフェイスをクリックします。

Summary ペインのインターフェイスが強調表示され、Details ペインにタブが表示されます。

**ステップ 5**　Details ペインで、**Port Details** タブをクリックします。

Port Details タブが表示されます。

**ステップ 6**　Port Details タブで、**Port Mode Settings** セクションを展開表示します。

ポート モードが表示されます。

**ステップ 7**　（任意）IPv4 Address Settings セクションの Secondary エリアで、**Add Secondary IP** 右クリックして選択し、セカンダリ IP アドレスを追加します。

**ステップ 8**　セカンダリ エリアから、IP アドレス フィールドに IPv4 アドレスを入力します。

**ステップ 9**　ネット マスク フィールドからネットワーク マスクを入力して、IPv4 アドレスをドット付き 10 進数で表記します。

**ステップ 10**　（任意）IPv4 Address Settings セクションの Helper エリアで、**Add Helper IP** を右クリックして選択し、ヘルパー IP アドレスを追加します。

**ステップ 11**　Helper エリアから、IP アドレス フィールドに IPv4 アドレスを入力します。

**ステップ 12**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# IP フィールドの説明

IP アドレス フィールドの詳細については、『*Cisco DCNM Interfaces Configuration Guide, Release 4.0*』の 「Basic Parameters」の章を参照してください。

# 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.2-7）
- 規格（p.2-7）


## 関連資料

| 関連項目 | マニュアル名 |
|---|---|
| IP CLI コマンド | 『*Cisco NX-OS Unicast Routing Command Reference, Release 4.0*』 |

## 規格

| 規格 | タイトル |
|---|---|
| この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。 | — |

CHAPTER 3

# IPv6 の設定

この章では、デバイス上で Internet Protocol version 6（IPv6）を設定する方法について説明します。

ここでは、次の内容を説明します。

# IPv6 について

IPv6 は、IPv4 の後継として設計されており、ネットワーク アドレス ビット数が 32 ビット（IPv4 の場合）から 128 ビットに増やされています。IPv6 は IPv4 に基づいていますが、アドレス空間が大幅に拡大されており、メイン ヘッダーと拡張ヘッダーの簡素化など、その他の機能強化が含まれています。

拡大された IPv6 アドレス空間により、ネットワークのスケーラビリティが可能となり、グローバルな到達可能性が提供されます。簡素化された IPv6 パケット ヘッダー フォーマットにより、パケットの処理効率が向上しています。柔軟性の高い IPv6 アドレス空間により、プライベート アドレスの必要性と、プライベート（グローバルに一意ではない）アドレスを限られた数のパブリック アドレスに変換する Network Address Translation（NAT; ネットワーク アドレス変換）の使用が削減されます。IPv6 を使用すると、ネットワークの境界にある境界ルータによる特別な処理を必要としない新しいアプリケーション プロトコルがイネーブルになります。

プレフィクス集約、簡易ネットワーク再番号割り当て、IPv6 サイト マルチホーミング機能などの IPv6 機能により、さらに効率的にルーティングが行われます。IPv6 は、Routing Information Protocol（RIP）、Integrated Intermediate System-to-Intermediate System（IS-IS）、IPv6 向け OSPF（Open Shortest Path First）、マルチプロトコル Border Gateway Protocol（BGP）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。

## IPv6 アドレス形式

IPv6 アドレスは、128 ビットまたは 16 バイトです。アドレスは 8 分割され、16 ビットの 16 進数ブロックにコロン（:）で区切られて表記されます（例：x:x:x:x:x:x:x:x）。IPv6 アドレスの例は、次のとおりです。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:3210
2001:0DB8:0:0:8:800:200C:417A
```

IPv6 アドレスの中には、連続するゼロが含まれます。2 つのコロン（::）を IPv6 アドレスの冒頭、中間、末尾に使用して、連続するゼロの代わりとすることもできます。表 3-1 に、省略した IPv6 アドレス形式を示します。

**（注）** IPv6 アドレスでは、アドレス中でもっとも長く連続するゼロの代わりに、2 つのコロン（::）を 1 度だけ使用できます。

連続する 16 ビット値がゼロで示されている場合は、2 つのコロンを IPv6 アドレスの一部として使用できます。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

IPv6 アドレス中の 16 進数の文字の大文字と小文字は区別されません。

**表 3-1　省略した IPv6 アドレス形式**

| IPv6 アドレス タイプ | 元のフォーマット | 省略されたフォーマット |
|---|---|---|
| ユニキャスト | 2001:0:0:0:0DB8:800:200C:417A | 2001::0DB8:800:200C:417A |
| マルチキャスト | FF01:0:0:0:0:0:0:101 | FF01::101 |
| ループバック | 0:0:0:0:0:0:0:1 | ::1 |
| 未指定 | 0:0:0:0:0:0:0:0 | :: |

ノードは、表 3-1 にあるループバック アドレスを使用して、IPv6 パケットを自分宛てに送信できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレスと同じです。詳細については、第 1 章「概要」を参照してください。

**（注）** IPv6 ループバック アドレスは、物理インターフェイスには割り当てられません。送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットは、そのパケットを作成したノードの外には転送できません。IPv6 ルータは、送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットを転送しません。

**（注）** IPv6 未指定アドレスは、インターフェイスには割り当てられません。未指定 IPv6 アドレスは、IPv6 パケット内の宛先アドレスまたは IPv6 ルーティング ヘッダーとして使用しないでください。

IPv6 プレフィクスは、RFC 2373 で規定された形式です。この形式では、IPv6 アドレスが、コロンに囲まれた 16 ビット値を使用した 16 進数で指定されています。プレフィクス長は、プレフィクス（アドレスのネットワーク部）を構成する、アドレスの高位隣接ビットの数を示す 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィクスです。

# IPv6 ユニキャスト アドレス

IPv6 ユニキャスト アドレスは、単一ノード上の単一インターフェイスの ID です。ユニキャスト アドレス宛てに送信されたパケットは、そのアドレスを持つインターフェイスに配信されます。ここでは、次の内容について説明します。

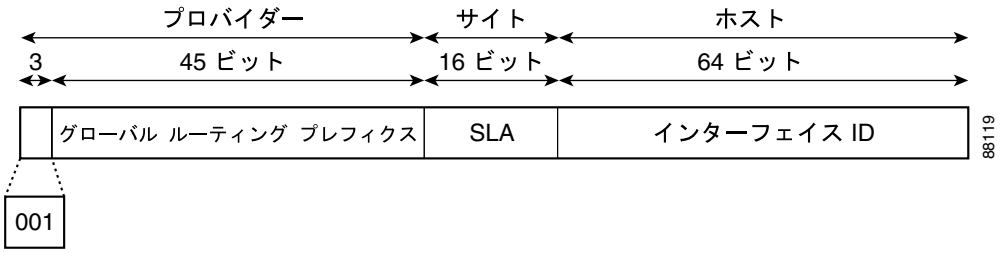


## 集約可能グローバル アドレス

集約可能グローバル アドレスは、集約可能なグローバル ユニキャスト プレフィクスによる IPv6 アドレスです。集約可能なグローバル ユニキャスト アドレスの構造により、グローバル ルーティング テーブル内のルーティング テーブル エントリ数を制限するルーティング プレフィクスの厳密な集約が可能となります。集約可能なグローバル アドレスは、組織間を上に向かって、最終的に Internet service provider（ISP; インターネット サービス プロバイダー）まで集約されるリンクで使用されます。

集約可能なグローバル IPv6 アドレスは、グローバル ルーティング プレフィクス、サブネット ID、およびインターフェイス ID により定義されます。バイナリ 000 で始まるアドレスを除き、グローバル ユニキャスト アドレスはすべて 64 ビット インターフェイス ID を持ちます。IDIPv6 グローバル ユニキャスト アドレスの割り当てでは、バイナリ値 001 で始まる範囲内のアドレスを使用します（2000::/3）。図 3-1 に、集約可能なグローバル アドレスの構成を示します。

**図 3-1　集約可能グローバル アドレスのフォーマット**




2000::/3 (001) ～ E000::/3 (111) のプレフィクスを持つアドレスには、Extended Universal Identifier（EUI）-64 フォーマットの 64 ビット インターフェイス ID が必要です。Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）は、2000::/16 の範囲の IPv6 アドレス空間を地域レジストリに割り当てます。

集約可能なグローバル アドレスは、48 ビット グローバル ルーティング プレフィクスと、16 ビット サブネット ID または Site-Level Aggregator（SLA）で構成されます。IPv6 集約可能なグローバル ユニキャスト アドレス フォーマット文書（RFC 2374）では、グローバル ルーティング プレフィクスには、Top-Level Aggregator（TLA）および Next-Level Aggregator（NLA）という他の 2 つの階層構造のフィールドが含まれるとされていました。TLS フィールドおよび NLA フィールドはポリシーベースであるため、IETF は、これらのフィールドを RFC から削除することを決定しました。この変更以前に展開された既存の IPv6 ネットワークの中には、依然として、古いアーキテクチャ上のネットワークを使用しているものもあります。

個々の組織では、16 ビット サブネット フィールドであるサブネット ID を使用して、ローカル アドレス指定階層構造を作成したり、サブネットを識別したりできます。サブネット ID は、IPv4 でのサブネットに似ていますが、IPv6 サブネット ID を持つ組織では 65,535 のサブネットをサポートできるという点で異なります。

インターフェイス ID で、リンク上のインターフェイスが識別されます。インターフェイス ID は、リンク上では一意です。多くの場合、インターフェイス ID は、インターフェイスのリンクレイヤ アドレスと同じか、リンクレイヤ アドレスに基づいています。集約可能なグローバル ユニキャスト アドレス タイプおよびその他の IPv6 アドレス タイプで使用されるインターフェイス ID は、長さが 64 ビットの変更済み EUI-64 フォーマットです。

インターフェイス ID は、次のいずれかに該当する変更済みの EUI-64 フォーマットです。

- すべての IEEE 802 インターフェイス タイプ（イーサネット、および Fiber Distributed Data インターフェイスなど）の場合は、最初の 3 オクテット（24 ビット）がそのインターフェイスの 48 ビット リンクレイヤ アドレス（MAC アドレス）の Organizationally Unique Identifier（OUI）、4 番めと 5 番めのオクテット（16 ビット）が FFFE の固定 16 進数値、そして、最後の 3 オクテット（24 ビット）が MAC アドレスの最後の 3 オクテットです。最初のオクテットの 7 番めのビットである Universal/Local（U/L）ビットの値は 0 または 1 です。0 はローカルな管理 ID、1 はグローバルに一意な IPv6 インターフェイス ID です。
- その他のすべてのインターフェイス タイプ（シリアル、ループバック、ATM、フレームリレー、トンネル インターフェイス タイプなど。ただし、IPv6 オーバーレイ トンネルで使用されるトンネル インターフェイスを除く）の場合、インターフェイス ID は IEEE 802 インターフェイス タイプのインターフェイス ID に似ていますが、ルータの MAC アドレス プールからの最初の MAC アドレスが ID として使用される点が異なります（インターフェイスが MAC アドレスを持たないため）。
- IPv6 オーバーレイ トンネルで使用されるトンネル インターフェイス タイプの場合、インターフェイス ID は、ID の高位 32 ビットがすべてのゼロであるトンネル インターフェイスに割り当てられた IPv4 アドレスです。

**（注）** PPP（ポイントツーポイント プロトコル）を使用するインターフェイスの場合は、接続の両端のインターフェイスが同じ MAC アドレスを持つため、接続の両端のインターフェイス ID が、両方の ID が一意となるまでネゴシエートされます（ランダムに選択され、必要に応じて再構築されます）。ルータの最初の MAC アドレスが、PPP を使用するインターフェイスの ID として使用されます。

ルータに IEEE 802 インターフェイス タイプがない場合は、ルータのインターフェイスでリンクローカル IPv6 アドレスが次のシーケンスで生成されます。

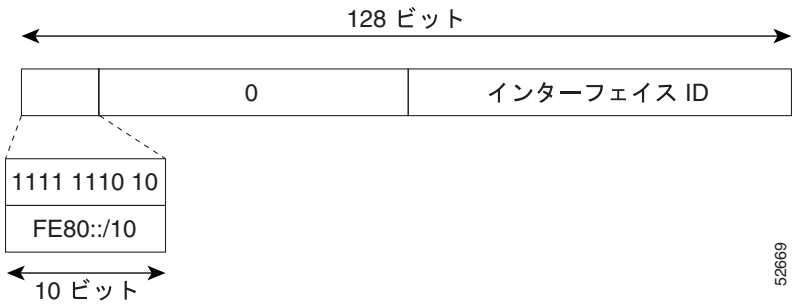
1. ルータに MAC アドレス（ルータ内の MAC アドレス プールの）が照会されます。
2. 使用可能な MAC アドレスがルータにない場合は、ルータのシリアル番号を使用して、リンクローカル アドレスが作成されます。
3. リンク ローカル アドレスの作成にルータのシリアル番号を使用できない場合、ルータは MD5 ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

## リンク ローカル アドレス

リンク ローカル アドレスは、リンク ローカル プレフィクス FE80::/10（1111 1110 10）と、変更済み EUI-64 フォーマットのインターフェイス ID を使用するどのインターフェイスでも自動設定が可能な IPv6 ユニキャスト アドレスです。リンク ローカル アドレスは NDP およびステートレス自動設定処理で使用されます。ローカル リンク上のノードは、リンク ローカル アドレスを使用して通信でき、通信するためにはグローバルに一意のアドレスを必要としません。図 3-2 に、リンク ローカル アドレスの構成を示します。

IPv6 ルータは、送信元または宛先がリンク ローカル アドレスであるパケットを他のリンクに転送できません。

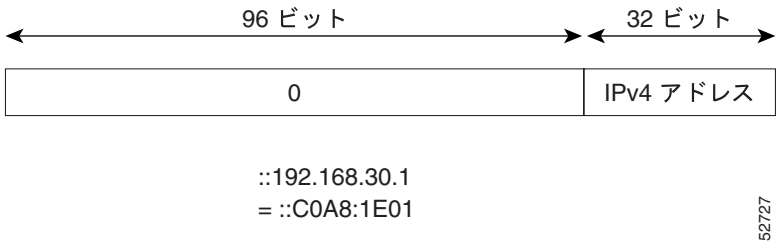
**図 3-2　リンク ローカル アドレス形式**




## IPv4 互換の IPv6 アドレス

IPv4 互換 IPv6 アドレスとは、アドレスの高位 96 ビットがゼロであり、アドレスの低位 32 ビットが IPv4 アドレスである IPv6 ユニキャスト アドレスです。IPv4 互換 IPv6 アドレスのフォーマットは 0:0:0:0:0:0:A.B.C.D または ::A.B.C.D です。IPv4 互換 IPv6 アドレスの 128 ビット全体はノードの IPv6 アドレスとして使用され、低位 32 ビットに埋め込まれた IPv4 アドレスはノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 および IPv6 の両プロトコル スタックをサポートするノードに割り当てられ、自動トンネルで使用されます。図 3-3 に、IPv4 互換 IPv6 アドレスおよび一部容認可能なアドレス形式の構成を示します。

**図 3-3　IPv4 互換 IPv6 アドレス形式**



## ユニーク ローカル アドレス

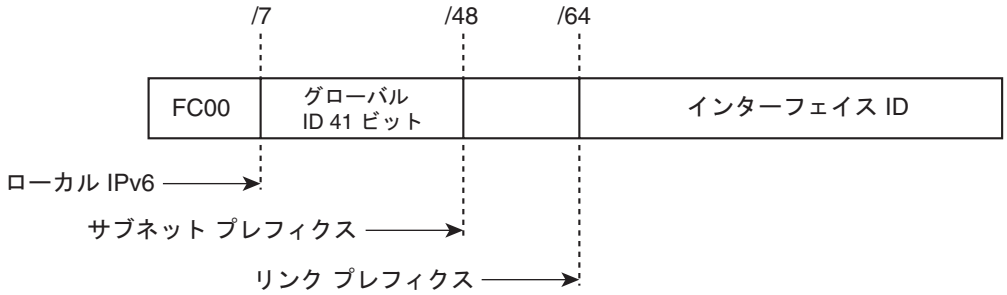
ユニーク ローカル アドレスは、グローバルに一意であり、ローカルでの通信のための IPv6 ユニキャスト アドレスです。グローバルなインターネット上でのルーティングには対応しておらず、サイトなどの限られたエリア内でのみルーティング可能です。限られた複数のサイト間もルーティングできる場合もあります。アプリケーションは、ユニーク ローカル アドレスをグローバルなスコープのアドレスとして扱う場合があります。

ユニーク ローカル アドレスには次の特徴があります。

- グローバルに一意のプレフィクスを持っている（一意である可能性が大）
- 周知のプレフィクスを持つため、サイトの境界でフィルタリングが容易
- アドレスの競合が発生せず、これらのプレフィクスを使用するインターフェイスの再番号割り当ても必要とせずに、サイトを結合したり、プライベートに相互接続したりできる
- ISP に依存せず、永久的または断続的なインターネット接続を使用することなく、サイト内での通信に使用できる
- ルーティングや Domain Name Server（DNS; ドメイン ネーム サーバ）により、誤ってサイト外に漏れても、他のどのアドレスとも競合しない

図 3-4 は、ユニーク ローカル アドレスの構造を示します。

**図 3-4　ユニーク ローカル アドレスの構造**




- プレフィクス — ローカル IPv6 ユニキャスト アドレスを認識する FC00::/7 プレフィクス
- グローバル ID — グローバルに一意なプレフィクスを作成する 41 ビットのグローバル識別子
- サブネット ID — 6 ビットのサブネット ID は、サイト内サブネットの識別子
- インターフェイス ID — 64 ビット ID

232389

## サイトローカル アドレス

RFC 3879 によりサイトローカル アドレスの使用が廃止されたため、プライベート IPv6 アドレスの設定時には、RFC 4193 で推奨されるユニーク ローカル アドレス（UCA）を使用する必要があります。

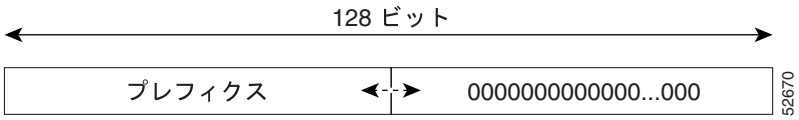
## IPv6 エニーキャスト アドレス

エニーキャスト アドレスとは、異なるノードに属するインターフェイス一式に割り当てられたアドレスです。エニーキャスト アドレスに送信されたパケットは、ルーティング プロトコルの定義に従って、そのエニーキャスト アドレスが示す最寄りのインターフェイスに配信されます。エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。ユニキャスト アドレスを複数のインターフェイスに割り当てると、ユニキャスト アドレスがエニーキャスト アドレスとなります。エニーキャスト アドレスが割り当てられたノードは、アドレスがエニーキャスト アドレスであることを認識できるよう、設定する必要があります。

**（注）** エニーキャスト アドレスを使用できるのは、ルータのみです。ホストはエニーキャスト アドレスを使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスには使用できません。

図 3-5 は、サブネット ルータ エニーキャスト アドレスのフォーマットを示します。アドレスには、連続するゼロに連結されたプリフィクス（インターフェイス ID）があります。サブネット ルータ エニーキャスト アドレスを使用すると、サブネット ルータ エニーキャスト アドレスのプレフィクスが表すリンク上のルータに到達できます。

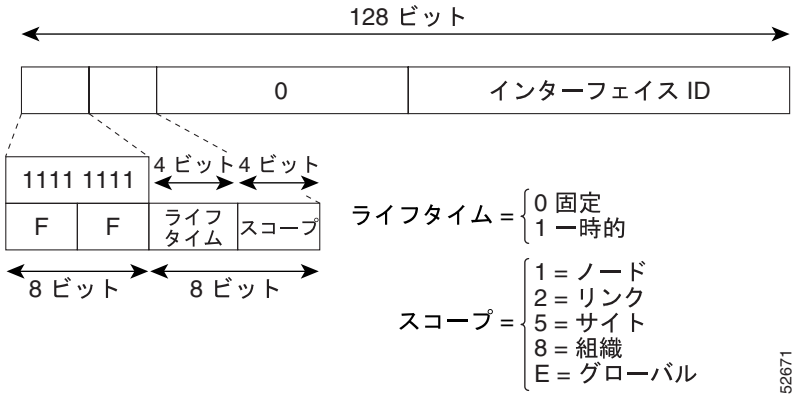
**図 3-5　サブネット ルータ エニーキャスト アドレスのフォーマット**



# IPv6 マルチキャスト アドレス

IPv6 マルチキャスト アドレスとは、FF00::/8（1111 1111）というプレフィクスを持つ IPv6 アドレスです。IPv6 マルチキャスト アドレスは、異なるノードに属するインターフェイス一式の ID です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。プレフィクスに続く 2 番めのオクテットで、マルチキャスト アドレスのライフタイムとスコープが定義されます。固定マルチキャスト アドレスは 0 と同等のライフタイム パラメータを持ち、一時マルチキャスト アドレスは 1 と同等のライフタイム パラメータを持ちます。ノード、リンク、サイト、または組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータはそれぞれ、1、2、5、8、または E です。たとえば、FF02::/16 というプレフィクスを持つマルチキャスト アドレスは、リンク スコープを持つ永久マルチキャスト アドレスです。図 3-6 に、IPv6 マルチキャスト アドレスのフォーマットを示します。

**図 3-6　IPv6 マルチキャスト アドレス形式**



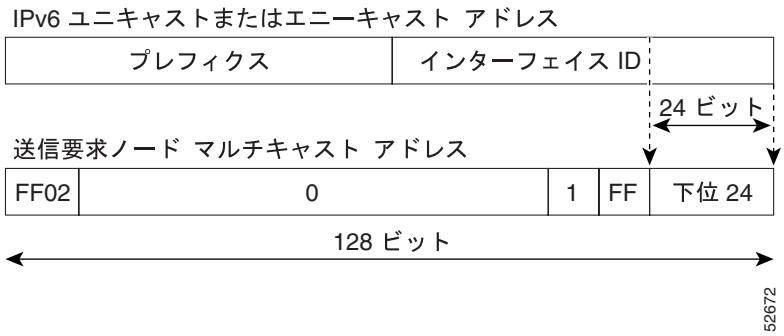

IPv6 ノード（ホストとルータ）は、（受信パケットの宛先となる）次のマルチキャスト グループに加入する必要があります。

- 全ノード マルチキャスト グループ FF02:0:0:0:0:0:0:1（スコープはリンク ローカル）
- 割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00:0000/104

IPv6 ルータは、全ルータ マルチキャスト グループ FF02:0:0:0:0:0:0:2（スコープはリンク ローカル）にも加入する必要があります。

送信要求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスまたは IPv6 エニーキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているユニキャスト アドレスおよびエニーキャスト アドレスごとに、関連付けられた送信要求ノード マルチキャスト グループに加入する必要があります。IPv6 送信要求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレス または IPv6 エニーキャスト アドレスの低位 24 ビットに連結されたプレフィクス FF02:0:0:0:0:1:FF00:0000/104 があります（図 3-7 を参照）。たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する送信要求ノード マルチキャスト アドレスは FF02::1:FF0E:8C6C です。送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

**図 3-7　IPv6 送信要求ノード マルチキャスト アドレス形式**

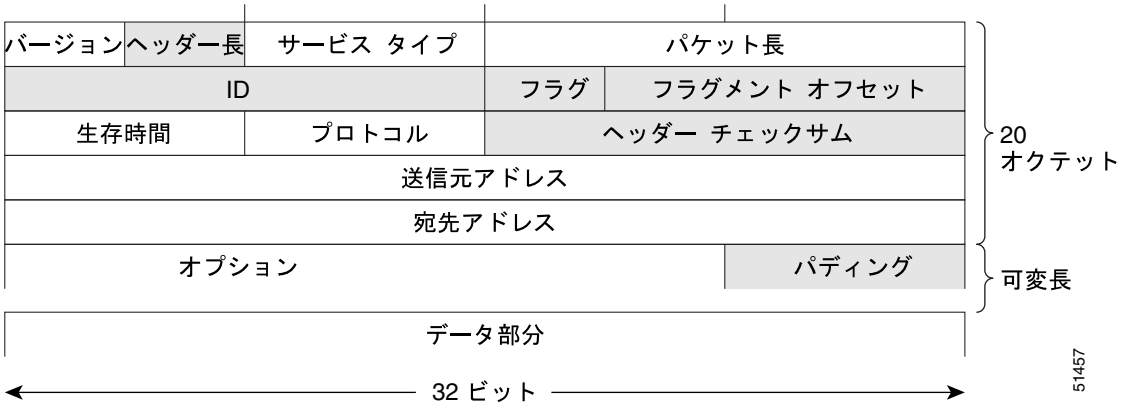



(注)　IPv6 にはブロードキャスト アドレスはありません。IPv6 マルチキャスト アドレスがブロードキャスト アドレスの代わりに使用されます。

## IPv4 パケット ヘッダー

基本 IPv4 パケット ヘッダーには、合計サイズが 20 オクテット（160 ビット）の 12 のフィールドがあります（図 3-8 を参照）。この 12 このフィールドのあとにはオプション フィールドが、さらにそのあとに、通常はトランスポート レイヤ パケットであるデータ部分が続く場合があります。オプション フィールドの可変長部分は、IPv4 パケット ヘッダーの合計サイズに加算されます。IPv4 パケット ヘッダーのグレーの部分のフィールドは、IPv6 パケット ヘッダーに含まれません。

**図 3-8　IPv4 パケット ヘッダーのフォーマット**



# 簡易 IPv4 パケット ヘッダー

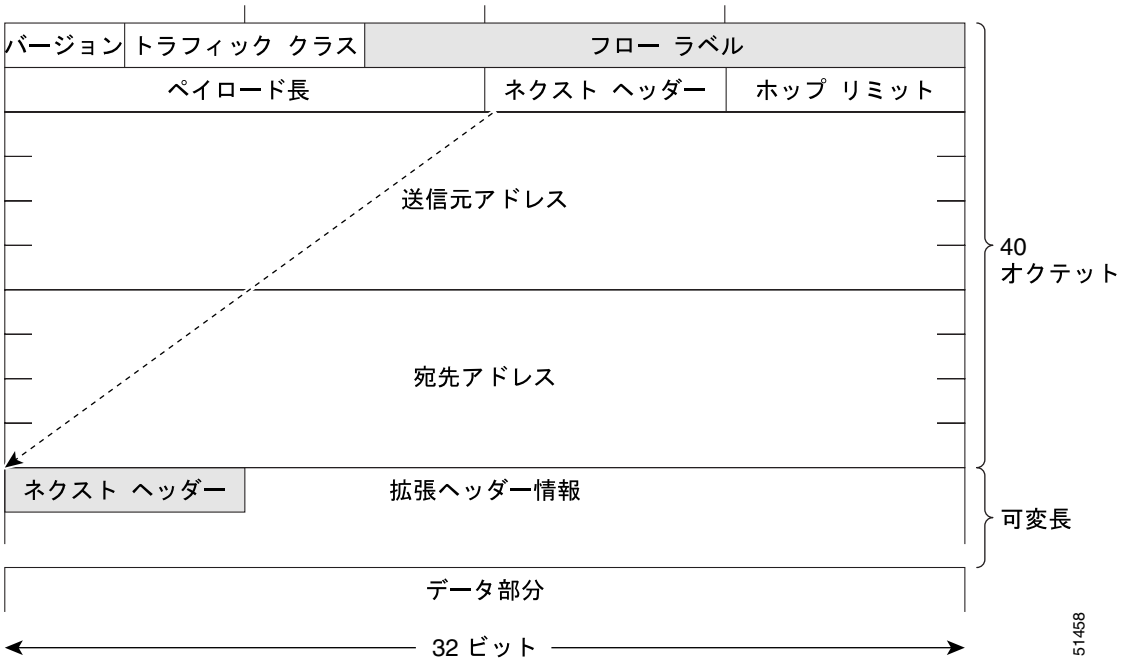
基本 IPv6 パケット ヘッダーには、合計サイズが 40 オクテット（320 ビット）の 8 つのフィールドがあります（図 3-9 を参照）。フラグメンテーションはパケットの送信元により処理され、データリンク レイヤのチェックサムとトランスポート レイヤが使用されます。User Datagram Protocol（UDP）チェックサムにより、内部パケットと基本 IPv6 パケット ヘッダーの整合性がチェックされ、オプション フィールドが 64 ビットに揃えられるため、IPv6 パケットの処理が容易になります。

表 3-2 は、基本 IPv6 パケット ヘッダーのフィールドの一覧です。

**表 3-2　基本 IPv6 パケット ヘッダーのフィールド**

| フィールド | 説明 |
|---|---|
| バージョン | IPv4 パケット ヘッダーのバージョン フィールドに該当しますが、IPv4 で示される数字 4 の代わりに、IPv6 では数字 6 が示されます。 |
| トラフィック クラス | IPv4 パケット ヘッダーのサービス タイプ フィールドに該当します。トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。 |
| フロー ラベル | IPv6 パケット ヘッダーの新規フィールドです。フロー ラベル フィールドは、ネットワーク レイヤでパケットを差別化する特定のフローのタグを、パケットに付けます。 |
| ペイロード長 | IPv4 パケット ヘッダーのパケット長フィールドに該当します。ペイロード長フィールドは、パケットのデータ部分の長さの合計を示します。 |
| 次ヘッダー | IPv4 パケット ヘッダーのプロトコル フィールドに該当します。次ヘッダー フィールドの値により、基本 IPv6 ヘッダーの後に続く情報のタイプが決まります。基本 IPv6 ヘッダーの後に続く情報のタイプは、図 3-9 に示すように、TCP パケット、UDP パケット、または拡張ヘッダーなどのトランスポート レイヤ パケットです。 |
| ホップ リミット | IPv4 パケット ヘッダーの生存時間フィールドに該当します。ホップ リミット フィールドは、IPv6 パケットが無効になる前に通過できるルータの最大数を指定します。各ルータを通過するたびに、この値が 1 ずつ減少します。IPv6 ヘッダーにはチェックサムがないため、ルータは、値が減少するたびにチェックサムを再計算する必要がなく、処理リソースの節約となります。 |
| 送信元アドレス | IPv4 パケット ヘッダーの送信元アドレス フィールドに該当しますが、IPv4 の 32 ビット送信元アドレスの代わりに、IPv6 では 128 ビット送信元アドレスが含まれます。 |
| 宛先アドレス | IPv4 パケット ヘッダーの宛先アドレス フィールドに該当しますが、IPv4 の 32 ビット宛先アドレスの代わりに、IPv6 では 128 ビット宛先アドレスが含まれます。 |

**図 3-9　IPv6 パケット ヘッダーのフォーマット**




任意に使用できる拡張ヘッダーおよびパケットのデータ部分は、基本 IPv6 パケット ヘッダーの 8 つのフィールドのあとに続きます。拡張ヘッダーがある場合は、各拡張ヘッダーが 64 ビットに揃えられます。IPv6 パケットの拡張ヘッダーの数は決められていません。各拡張ヘッダーは、前のヘッダーの次ヘッダー フィールドに示されます。通常は、最後の拡張ヘッダーに、TCP または UDP などのトランスポート レイヤ プロトコルの次ヘッダー フィールドがあります。図 3-10 に、IPv6 拡張ヘッダーのフォーマットを示します。

**図 3-10　IPv6 拡張ヘッダーのフォーマット**

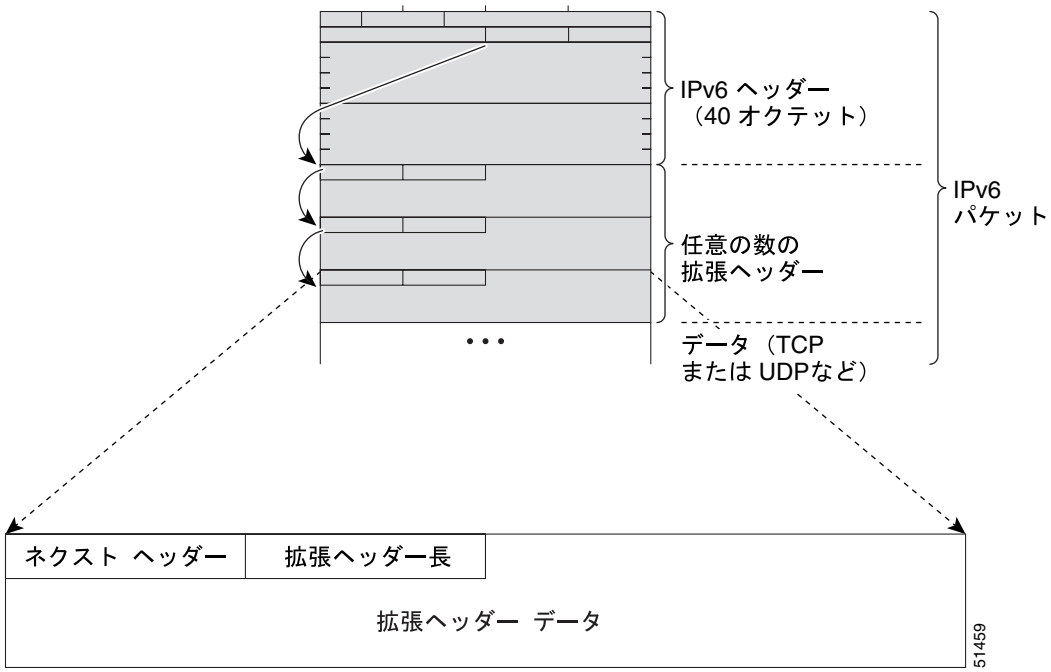


表 3-3 は、拡張ヘッダーのタイプとその次ヘッダー フィールドの値の一覧です。

**表 3-3　IPv6 拡張ヘッダーのタイプ**

| ヘッダーのタイプ | 次ヘッダーの値 | 説明 |
|---|---|---|
| ホップバイホップ オプション ヘッダー | 0 | パケットのパス上のすべてのホップで処理されるヘッダー。存在する場合、ホップバイホップ オプション ヘッダーは、常に基本 IPv6 パケット ヘッダーの直後に続きます。 |
| 宛先オプション ヘッダー | 6 | 任意のホップバイホップ オプション ヘッダーの後に続くことのあるヘッダー。このヘッダーは、最終の宛先、およびルーティング ヘッダーで指定された各通過アドレスで処理されます。また、宛先オプション ヘッダーは、任意の Encapsulating Security Payload（ESP）ヘッダーの後に続く場合もあります。この場合の宛先オプション ヘッダーは、最終の宛先でのみ処理されます。 |
| ルーティング ヘッダー | 43 | 送信元のルーティングに使用されるヘッダー |
| フラグメント ヘッダー | 44 | 送信元が、送信元と宛先の間のパスの Maximum Transmission Unit（MTU; 最大伝送ユニット）より大きいパケットをフラグメント化するときに使用されるヘッダー。フラグメント ヘッダーは、フラグメント化された各パケットで使用されます。 |
| 上位層ヘッダー | 6（TCP の場合）<br>17（UDP の場合） | データ転送のためにパケット内で使用されるヘッダー。おもな転送プロトコルは TCP と UDP の 2 つです。 |

## IPv6 の DNS

IPv6 は、DNS 名前 / アドレスおよびアドレス / 名前のルックアップ処理でサポートされる DNS レコード タイプをサポートしています。DNS レコード タイプは IPv6 アドレスをサポートしています。

**（注）** IPv6 は、IPv6 アドレスから DNS 名への逆マッピングもサポートしています。

**表 3-4　IPv6 DNS レコード タイプ**

| レコード タイプ | 説明 | フォーマット |
|---|---|---|
| AAAA | ホスト名を IPv6 アドレスにマッピングします（IPv4 の A レコードに該当） | www.abc.test AAAA 3FFE:YYYY:C18:1::2 |
| PTR | IPv6 アドレスをホスト名にマッピングします（IPv4 の PTR レコードに該当） | 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e.f.f.3.ip6.int PTR www.abc.test |

## IPv6 のパス MTU 探索

IPv4 の場合と同様に、ホストがダイナミックに、データ パス上のすべてのリンクの MTU サイズの差を検出し、それに合わせて調整できるよう、IPv6 でパス MTU 探索を使用できます。ただし、IPv6 では、データ パス上のリンクのパス MTU が小さすぎてパケットを処理できない場合は、パケットの送信元によりフラグメンテーションが処理されます。IPv6 ホストにパケットのフラグメンテーションを処理させると、IPv6 ルータの処理リソースが節約され、IPv6 ネットワークの効率が向上します。

(注)　IPv6 では、最小リンク MTU は 1280 オクテットです。IPv6 リンクには、1500 オクテットの MTU 値の使用をお勧めします。

## CDP IPv6 アドレスのサポート

隣接情報機能向け CDP IPv6 アドレス サポートを使用して、2 台のシスコ デバイス間で IPv6 アドレス指定情報を転送できます。IPv6 アドレス向け CDP サポートは、ネットワーク管理製品およびトラブルシューティング ツールに IPv6 情報を提供します。

## IPv6 の ICMP

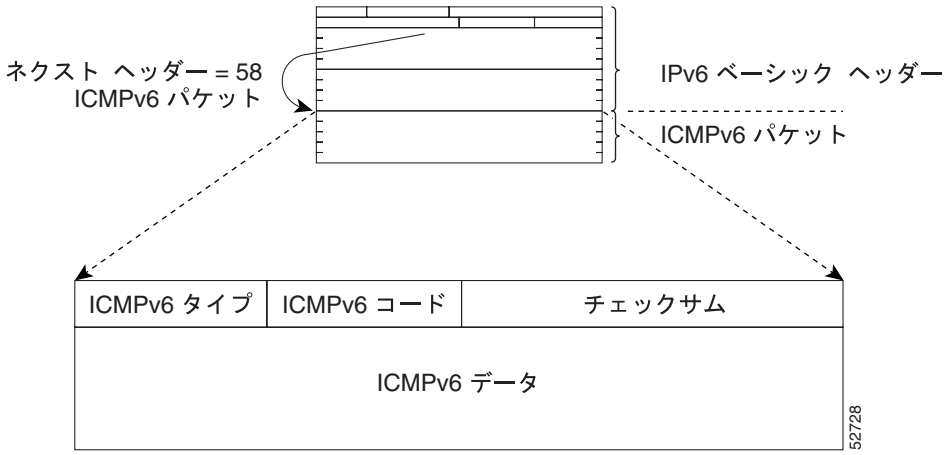
IPv6 で ICMP を使用して、ネットワークの状態に関する情報を提供できます。IPv6 で使用できるバージョンである ICMPv6 は、パケットが正しく処理されない場合にエラーを報告し、ネットワークの状態に関する情報メッセージを送信します。たとえば、パケットが大きすぎて別のネットワークに送信できないために、ルータがパケットを転送できない場合は、ルータにより、送信元のホストに ICMPv6 メッセージが送信されます。さらに、IPv6 の ICMP パケットは IPv6 近隣探索およびパス MTU 探索に使用されます。パス MTU 探索処理により、パケットが確実に、特定のルートでサポートされる最大のサイズで送信されます。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの 58 という値は、IPv6 ICMP パケットであることを示します。ICMP パケットはすべて拡張ヘッダーから始まる、IPv6 パケット情報の最後の断片です。IPv6 ICMP パケットでは、ICMPv6 タイプ フィールドと ICMPv6 コード フィールドに、ICMP メッセージ タイプなどの IPv6 ICMP パケット情報が示されます。チェックサム フィールドの値は送信側で計算され、受信側により、ICMP パケット内および IPv6 疑似ヘッダー内のフィールドでチェックされます。

(注)　IPv6 ヘッダーには、チェックサムはありません。ただし、チェックサムは、パケットの誤配信を判定するために、トランスポート レイヤで重要です。計算に IP アドレスが含まれるすべてのチェックサム計算は、新しい 128 ビット アドレスを処理できるよう、IPv6 用に変更する必要があります。チェックサムは、疑似ヘッダーを使用して生成されます。

ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。図 3-11 に、IPv6 ICMP パケット ヘッダー フォーマットを示します。

**図 3-11　IPv6 ICMP パケット ヘッダーのフォーマット**



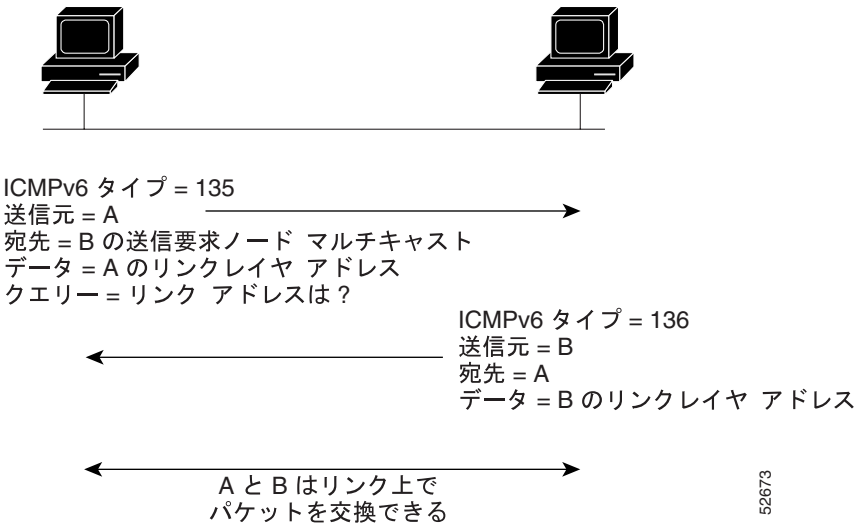

## IPv6 近隣探索

IPv6 NDP を使用して、隣接ルータが到達可能かどうかを判定できます。IPv6 ノードは、近隣探索を使用して、同じネットワーク上のノードのアドレス（ローカル リンク）を決定します。そして、ノード自身からのパケットを転送できる隣接ルータを見つけ、その隣接ルータが到達可能かどうかを確認し、リンクレイヤ アドレスの変更を検出します。NDP は ICMP メッセージを使用して、パケットが到達不可能な隣接ルータに送信されたかどうかを検出します。

## IPv6 ネイバー送信要求メッセージ

ノードは、同じローカル リンク上の別のノードのリンクレイヤ アドレスを決定するときに、ICMP パケット ヘッダーのタイプ フィールドの値が 135 であるネイバー送信要求メッセージをローカル リンクで送信します（図 3-12 を参照）。送信元アドレスは、ネイバー送信要求メッセージを送信するノードの IPv6 アドレスです。宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノード マルチキャスト アドレスです。ネイバー送信要求メッセージには、送信元ノードのリンクレイヤ アドレスも含まれます。

**図 3-12　IPv6 近隣探索 — ネイバー送信要求メッセージ**



ネイバー送信要求メッセージを受信したあとに、宛先ノードは返信として、ICMP パケット ヘッダーのタイプ フィールドの値が 136 のネイバー アドバタイズメント メッセージをローカル リンクで送信します。送信元アドレスは、ノードの IPv6 アドレス（ネイバー アドバタイズメント メッセージを送信するノード インターフェイスの IPv6 アドレス）です。宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。データ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンクレイヤ アドレスが含まれます。

送信元ノードがネイバー アドバタイズメント メッセージを受信すると、送信元ノードと宛先ノードは通信できるようになります。

ネイバー送信要求メッセージにより、ノードがネイバーのリンクレイヤ アドレスを認識したあとに、ネイバーの到達可能性が確認できます。ノードは、ネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスを、ネイバーのユニキャスト アドレスとして使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンクレイヤ アドレスが変更されたときにも送信されます。変更があったときのネイバー アドバタイズメント メッセージの宛先アドレスは、全ノード マルチキャスト アドレスです。

ネイバー到達不能検出により、ネイバーの障害またはネイバーへの転送パスの障害が特定されます。また、この検出は、ホストと近隣ノード（ホストまたはルータ）の間のすべてのパスで使用されます。ネイバー到達不能検出は、ユニキャスト パケットのみが送信されるネイバーに対してのみ実行され、マルチキャスト パケットが送信されるネイバーに対しては実行されません。

ネイバーは、そのノードから受諾の確認応答（以前にそのノードに送信されたパケットが受信され、処理されたことを示す）が返されると、到達可能とみなされます。受諾の確認応答（TCP などの上位層プロトコルからの）は、接続が順調に進んでいる（宛先に到達しつつある）ことを示します。パケットがピアに到達している場合は、送信元ノードのネクストホップ ネイバーにも到達しています。順調に進んでいることで、ネクストホップ ネイバーが到達可能であることも確認されます。

ローカル リンクにない宛先の場合は、順調に進んでいることで、ファーストホップ ルータが到達可能であることがわかります。上位層プロトコルからの確認応答がない場合、ノードは、ユニキャスト ネイバー送信要求メッセージを使用してネイバーを探し、宛先へのパスがまだ機能しているかどうかを確認します。ネイバーから返信された送信要求ネイバー アドバタイズメント メッセージは、宛先へのパスがまだ機能しているという確認応答です（1 という値が設定された送信要求フラグを持つネイバー アドバタイズメント メッセージは、ネイバー送信要求メッセージへの返信としてのみ送信されます）。非送信要求メッセージが返信された場合は、送信元ノードから宛先ノードまでの片道のパスのみが確認されています。送信要求ネイバー アドバタイズメント メッセージは、往復のパスがいずれも機能していることを示します。

**（注）** 0 という値が設定された送信要求フラグを持つネイバー アドバタイズメント メッセージは、宛先へのパスがまだ機能していることを示す確認応答とはみなされません。

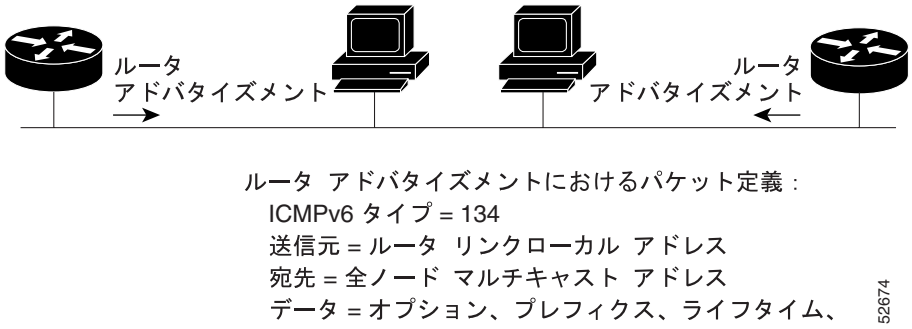
ネイバー送信要求メッセージは、ユニキャスト IPv6 アドレスをインターフェイスに割り当てる前にそのアドレスが一意であることを確認するために、ステートレス自動設定処理でも使用されます。新規のリンク ローカル IPv6 アドレスに対しては、インターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（新規アドレスは、重複アドレス検出の実行中は一時的なアドレスのままです）。ノードは、未指定の送信元アドレスと一時的なリンク ローカル アドレスがメッセージ本文に含まれるネイバー送信要求メッセージを送信します。そのアドレスがすでに他のノードによって使用されている場合、ノードは、一時的リンク ローカル アドレスを含むネイバー アドバタイズメント メッセージを返信します。他のノードが同時に、同じアドレスが一意であることを確認している場合は、そのノードも、ネイバー送信要求メッセージを返信します。ネイバー送信要求メッセージの返信としてのネイバー アドバタイズメント メッセージも、同じ一時的アドレスを確認中の他のノードからのネイバー送信要求メッセージも受信しない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンク ローカル アドレスが一意であると判断し、そのアドレスをインターフェイスに割り当てます。

# IPv6 ルータ アドバタイズメント メッセージ

ルータ アドバタイズメント（RA）メッセージは、ICMP パケット ヘッダーのタイプ フィールドの値が 134 であり、IPv6 ルータの設定済みの各インターフェイスへと定期的に送信されます。ステートレス自動設定が正しく機能するには、RA メッセージでアドバタイズされたプレフィクス長が常に 64 ビットである必要があります。

RA メッセージは、全ノード マルチキャスト アドレスに送信されます（図 3-13 を参照）。

**図 3-13　IPv6 近隣探索 — RA メッセージ**




RA メッセージには通常、次の情報が含まれます。

- ローカル リンク上のノードが、その IPv6 アドレスの自動設定に使用できる 1 つ以上のオンリンク IPv6 プレフィクス
- アドバタイズメントに含まれる各プレフィクスのライフタイム情報
- 完成可能な自動設定のタイプ（ステートレスまたはステートフル）を示すフラグ一式
- デフォルト ルータ情報（アドバタイズメントを送信しているルータをデフォルトとして使用する必要があるかどうか、および、その場合は、ルータがデフォルト ルータとして使用される秒単位の時間）
- ホストが発信するパケットで使用する必要のあるホップ リミットと MTU などの、ホストの詳細情報

RA は、ルータ送信要求メッセージの返信としても送信されます。ルータ送信要求メッセージは、ICMP パケット ヘッダーのタイプ フィールドの値が 133 であり、システム起動時にホストにより送信されます。これにより、ホストは、次回の定期 RA メッセージを待つことなく、ただちに自動設定できます。送信元アドレスは通常、未指定 IPv6 アドレス（0:0:0:0:0:0:0:0）です。ホストでユニキャスト アドレスが設定されている場合は、ルータ送信要求メッセージを送信するインターフェイスのユニキャスト アドレスが、メッセージで送信元アドレスとして使用されます。宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。RA がルータ送信要求の返信として送信されるときの RA メッセージの宛先アドレスは、ルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次の RA メッセージ パラメータを設定できます。

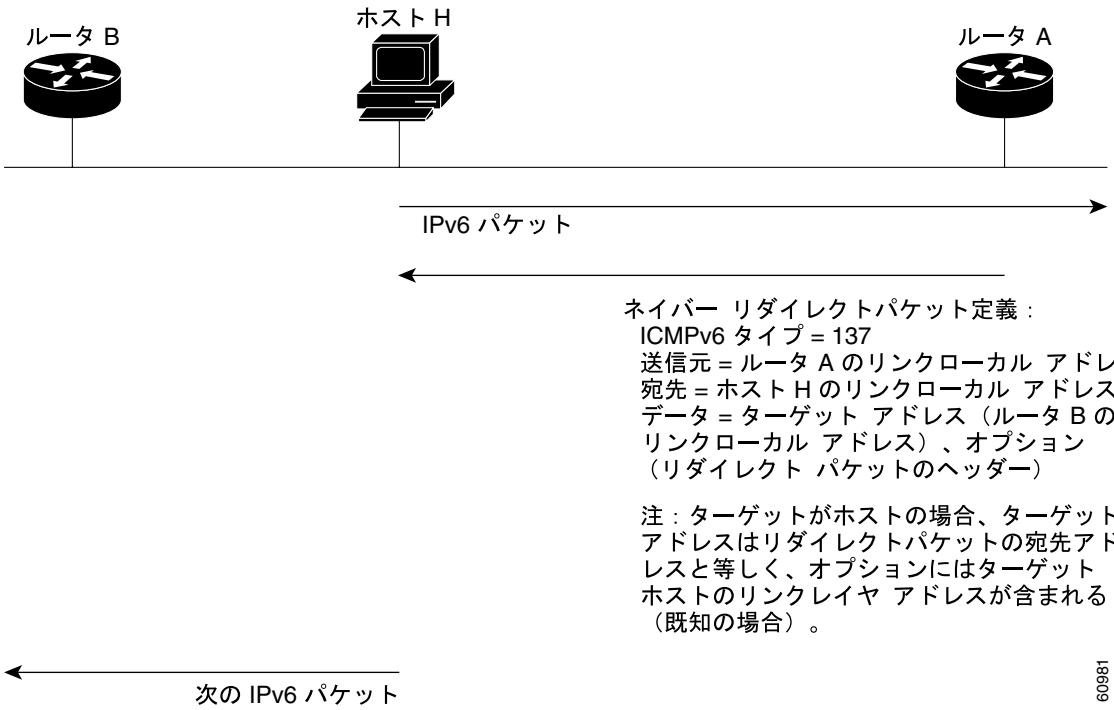
- RA メッセージが定期的に送信される時間の間隔
- デフォルト ルータ（リンクのすべてのノードが使用する）としてのルータの実用性を示すルータのライフタイム値
- リンクで使用されているネットワーク プレフィクス
- （リンクで）ネイバー送信要求メッセージが再送される時間の間隔
- ネイバーが到達可能である（リンク上のすべてのノードが使用できる）とノードが判断するまでの時間

設定されたパラメータは、各インターフェイス固有のパラメータです。RA メッセージ（デフォルト値を含む）の送信は、自動的にイーサネット インターフェイス上でイネーブルになります。他のインターフェイス タイプの場合は、**no ipv6 nd suppress-ra** コマンドを入力して RA メッセージを送信する必要があります。個々のインターフェイスでは、**ipv6 nd suppress-ra** コマンドを入力して、RA メッセージ機能をディセーブルにできます。

## IPv6 ネイバー リダイレクト メッセージ

ルータは、ネイバー リダイレクト メッセージを送信して、パス上の宛先へのより適切なファーストホップ ノードをホストに通知します（図 3-14 を参照）。IPv6 ネイバー リダイレクト メッセージは、ICMP パケット ヘッダーのタイプ フィールドの値が 137 となっています。

**図 3-14　IPv6 近隣探索 — ネイバー リダイレクト メッセージ**




**（注）** リダイレクト メッセージの目的のアドレス（最終の宛先）により、確実に隣接ルータのリンク ローカル アドレスが特定されるよう、ルータは、その各隣接ルータのリンク ローカル アドレスを決定可能である必要があります。スタティック ルーティングの場合は、ルータのリンク ローカル アドレスを使用して、ネクストホップ ルータのアドレスを指定する必要があります。ダイナミック ルーティングの場合は、隣接ルータのリンク ローカル アドレスを交換するように、すべての IPv6 ルーティング プロトコルを設定する必要があります。

パケットの転送後に、次の条件を満たす場合は、ルータがパケットの送信元にリダイレクト メッセージを送信します。

- パケットの宛先アドレスがマルチキャスト アドレスではない。
- パケットがルータ宛てではなかった。

- パケットが、パケットを受信したインターフェイスから、まもなく送信される。
- ルータが、パケットにより適したファーストホップ ノードはパケットの送信元と同じリンク上にあると決定した。
- パケットの送信元アドレスが、同じリンク上のネイバーのグローバル IPv6 アドレス、またはリンク ローカル アドレスである。

### 仮想化サポート

IPv6 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。VRF は Virtual Device Contexts（VDC; 仮想化デバイス コンテキスト）内にあります。デフォルトでは、特に別の VDC および VRF を設定しない限り、Cisco NX-OS によりデフォルト VDC およびデフォルト VRF が使用されます。詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

## IPv6 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 |
|---|---|
| DCNM | IPv6 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ない機能はいずれも、Cisco DCNM にバンドルされており、無償で提供されます。DCNM ライセンス方式の詳細については、『*Cisco DCNM Licensing Guide*』を参照してください。 |
| NX-OS | IPv6 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、Cisco NX-OS システム イメージにバンドルされて提供されます。追加料金は発生しません。NX-OS ライセンス方式の詳細説明については、『*Cisco NX-OS Licensing Guide*』を参照してください。 |

## IPv6 の前提条件

IPv6 には、次の前提条件があります。

- IPv6 アドレス指定、IPv6 ヘッダー情報、ICMPv6、IPv6 NDP など、IPv6 の基礎に関する詳しい知識が必要です。
- デバイスをデュアルスタック デバイス（IPv4/IPv6）にする場合は、必ずメモリ / 処理の注意事項に従ってください。

## IPv6 の注意事項および制約事項

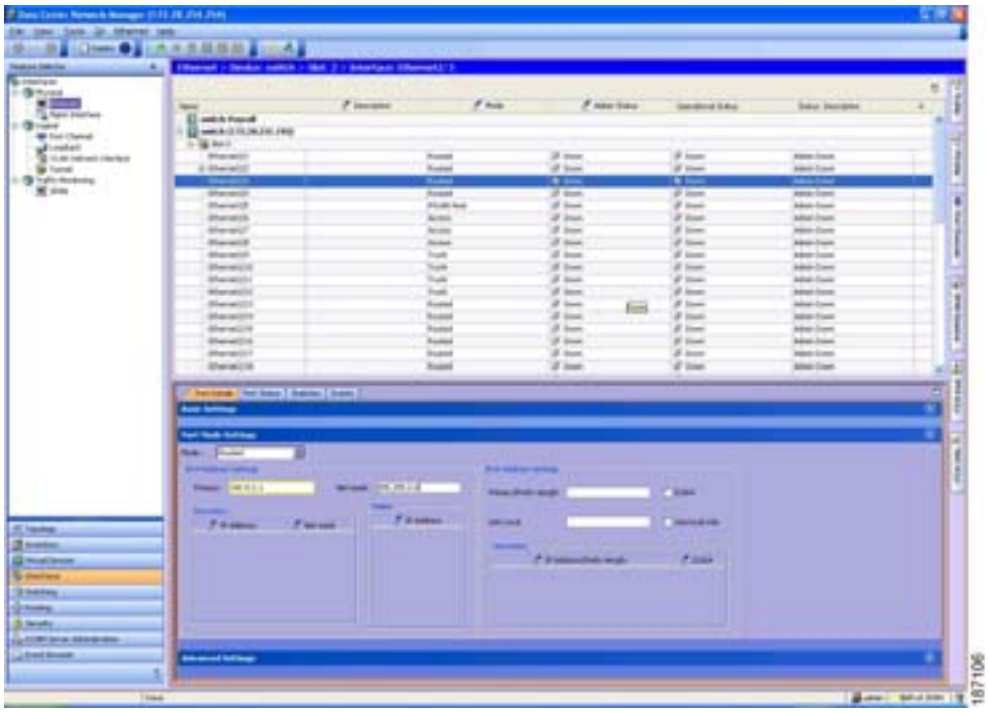
IPv6 には、次の注意事項、および制約、制限事項があります。

- スイッチは、IPv6 フレームを転送する前にレイヤ 3 パケット情報を確認しないため、IPv6 パケットは、レイヤ 2 LAN スイッチに対して透過的です。IPv6 ホストは、レイヤ 2 LAN スイッチに直接接続できます。
- インターフェイスの同じプレフィクス内に複数の IPv6 グローバル アドレスを設定できます。ただし、インターフェイス上の複数の IPv6 リンク ローカル アドレスはサポートされていません。
- RFC 3879 によりサイトローカル アドレスの使用が廃止されたため、RFC 4193 のユニーク ローカル アドレス（UCA）の推奨に従って、プライベート IPv6 アドレスを設定する必要があります。

# IPv6 の設定

Interfaces 機能選択により、レイヤ 3 インターフェイスに IPv6 アドレスを設定することができます。図 3-15 にレイヤ 3 インターフェイスを示します。

**図 3-15　レイヤ 3 インターフェイスの設定**



Data Center Network Manager 機能の詳細については、『*Cisco Data Center Network Manager Fundamentals Guide*』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。

- IPv6 アドレス指定の設定（p.3-21）
- IPv6 セカンダリ アドレスの設定（p.3-22）

## IPv6 アドレス指定の設定

インターフェイスで IPv6 トラフィックを転送するには、インターフェイスで IPv6 アドレスを設定する必要があります。インターフェイスでグローバル IPv6 アドレスを設定すると、リンク ローカル アドレスが自動的に設定され、そのインターフェイスで IPv6 が有効となります。

### 詳細な手順

ルーテッド インターフェイスを設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインから、**Interfaces > Physical > Ethernet** の順に選択します。

Summary 画面に使用できるデバイスが表示されます（図 3-15 を参照）。

**ステップ 2**　Summary ペインでデバイスをダブルクリックして、スロットの一覧を表示します。

**ステップ 3**　スロットをダブルクリックして、インターフェイスの一覧を表示します。

**ステップ 4**　ルーテッド インターフェイスとして設定したいインターフェイスをクリックします。

Summary ペインのインターフェイスが強調表示され、Details ペインにタブが表示されます。

**ステップ 5**　Details ペインで、**Port Details** タブをクリックします。

Port Details タブが表示されます。

**ステップ 6**　Port Details タブで、**Port Mode Settings** セクションを展開表示します。

ポート モードが表示されます。

**ステップ 7**　Mode ドロップダウン リストから、**Routed** を選択します。

Details ペインに IP アドレス情報が表示され、Cisco NX-OS はレイヤ 2 設定を削除します。

**ステップ 8**　IPv6 Address Settings エリアの Primary/prefix-length フィールドから、このルーテッド インターフェイスに IPv6 アドレスとプレフィクス長を設定します。

長さの範囲は 1 ～ 128 です。

**ステップ 9**　（任意）EUI64 を設定するには、**EUI64** をチェックします。

**ステップ 10**（任意）Link local フィールドから、リンク ローカル IPv6 アドレスを入力します。

**ステップ 11**（任意）このルーテッド インターフェイスをリンク ローカル ルーティング専用に設定するには、**Use local only** をチェックします。

**ステップ 12**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# IPv6 セカンダリ アドレスの設定

インターフェイスにセカンダリ アドレスまたはヘルパー アドレスを設定できます。

### 手順詳細

ルーテッド インターフェイスに IPv6 セカンダリ アドレスを設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインから、**Interfaces > Physical > Ethernet** の順に選択します。

Summary 画面に使用できるデバイスが表示されます（図 3-15 を参照）。

**ステップ 2**　Summary ペインでデバイスをダブルクリックして、スロットの一覧を表示します。

**ステップ 3**　スロットをダブルクリックして、インターフェイスの一覧を表示します。

**ステップ 4**　ルーテッド インターフェイスとして設定したいインターフェイスをクリックします。

Summary ペインのインターフェイスが強調表示され、Details ペインにタブが表示されます。

**ステップ 5**　Details ペインで、**Port Details** タブをクリックします。

Port Details タブが表示されます。

**ステップ 6**　Port Details タブで、**Port Mode Settings** セクションを展開表示します。

ポート モードが表示されます。

**ステップ 7**　（任意）IPv6 Address Settings セクションの Secondary エリアで、**Add IPv6 Address** を右クリックして選択し、セカンダリ IP アドレスを追加します。

**ステップ 8**　IP Address/Prefix-length フィールドからこのセカンダリ IPv6 アドレスに、IPv6 アドレスとプレフィクス長を入力します。

**ステップ 9**　（任意）EUI64 フォーマットを設定するには、**EUI64** をチェックします。

**ステップ 10**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# IPv6 フィールドの説明

IPv6 アドレス フィールドの詳細については、『*Cisco DCNM Interfaces Configuration Guide, Release 4.0* 』の「Basic Parameters」の章を参照してください。

# その他の関連資料

IPv6 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.3-23）
- 規格（p.3-23）


## 関連資料

| 関連項目 | マニュアル名 |
|---|---|
| IPv6 CLI コマンド | 『*Cisco NX-OS Unicast Routing Command Reference, Release 4.0*』 |

## 規格

| 規格 | タイトル |
|---|---|
| この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。 | — |

CHAPTER 4

# GLBP の設定

この章では、Gateway Load Balancing Protocol（GLBP）の設定方法について説明します。

ここでは、次の内容を説明します。

# GLBP の概要

GLBP は、冗長ゲートウェイ間でプロトコルおよび MAC（メディア アクセス制御）アドレスを共有することによって、IP にパスの冗長性をもたらします。GLBP はさらに、レイヤ 3 ルータ グループ間で、LAN 上のデフォルト ゲートウェイの負荷が分担されるようにします。GLBP ルータは他のルータで障害が発生した場合、グループの別のルータのフォワーディング機能を自動的に引き受けます。

ここでは、次の内容について説明します。



## GLBP の概要

*GLBP* は、IEEE 802.3 LAN 上でデフォルト ゲートウェイを 1 つだけ指定して設定された IP ホストの自動*ゲートウェイ* バックアップを行います。LAN 上の複数のルータが結びついて、1 つのバーチャル ファーストホップ IP ゲートウェイを提供し、なおかつ IP パケット転送の負荷を分担します。LAN 上の他のルータは、冗長 GLBP ゲートウェイとして動作可能であり、既存のフォワーディング ゲートウェイのいずれかで障害が発生した場合にアクティブになります。

GLBP は、HSRP（ホットスタンバイ冗長プロトコル）および VRRP（仮想ルータ冗長プロトコル）と同様の機能を実行します。HSRP および VRRP は、バーチャル IP アドレスを指定して設定されたバーチャル グループに、複数のルータを参加させます。これらのプロトコルでは、グループのバーチャル IP アドレスにパケットを転送するアクティブ ルータとして、メンバを 1 つ選択します。グループ内の他のルータは、アクティブ ルータで障害が発生するまで冗長構成になります。

GLBP は、他のプロトコルにはないロード バランシング機能を実行します。GLBP は、1 つのバーチャル IP アドレスと複数のバーチャル MAC アドレスを使用し、複数のルータ（ゲートウェイ）間でロード バランスを図ります。GLBP の場合は、1 つのルータに負荷全体を引き受けさせ、他のルータを遊ばせておくのではなく、GLBP グループのすべてのルータ間で転送負荷を分担します。各ホストに同じバーチャル IP アドレスを設定し、バーチャル グループ内のすべてのルータがパケット転送に関与するようにします。GLBP メンバは定期的な hello パケットによって、相互に通信します。

## GLBP アクティブ バーチャル ゲートウェイ

GLBP はゲートウェイにプライオリティを設定して、アクティブ バーチャル ゲートウェイ（*AVG*）を選択します。複数のゲートウェイに同じプライオリティを与えた場合は、実 IP アドレスが最も大きいゲートウェイが AVG になります。AVG は GLBP グループの各メンバにバーチャル MAC アドレスを割り当てます。各メンバはそれぞれ割り当てられたバーチャル MAC アドレスに対応するアクティブ バーチャル フォワーダ（*AVF*）となり、割り当てられたバーチャル MAC アドレスにパケットを転送します。

AVG は、バーチャル IP アドレスに対する ARP（アドレス解決プロトコル）要求にも応答します。ロード シェアリングは、AVG が ARP 要求に異なるバーチャル MAC アドレスで応答したときに行われます。

## GLBP バーチャル MAC アドレス割り当て

AVG はグループの各メンバにバーチャル MAC アドレスを割り当てます。グループ メンバは hello メッセージを通じて AVG を検出したあとで、バーチャル MAC アドレスを要求します。AVG は選択されたロード バランシング アルゴリズムに基づいて、ネクスト MAC アドレスを割り当てます（「GLBP ロード バランシングおよびトラッキング」[p.4-5] を参照）。AVG によってバーチャル MAC アドレスが割り当てられたゲートウェイは、プライマリ バーチャル フォワーダになります。hello メッセージから バーチャル MAC アドレスを学習する、GLBP グループの他のメンバは、セカンダリ バーチャル フォワーダです。

## GLBP によるバーチャル ゲートウェイの冗長性

GLBP は、バーチャル ゲートウェイの冗長性を実現します。グループ メンバは、アクティブ、スタンバイ、またはリッスン ステートになります。GLBP はプライオリティ アルゴリズムを使用し、1 つのゲートウェイを AVG として選択し、もう 1 つのゲートウェイをスタンバイ バーチャル ゲートウェイとして選択します。残りのゲートウェイはリッスン ステートになります。各ゲートウェイ上で GLBP プライオリティを設定できます。GLBP プライオリティが複数のゲートウェイで同じ場合、GLBP は IP アドレスが最大のゲートウェイを AVG として使用します。

AVG で障害が発生すると、スタンバイ バーチャル ゲートウェイがバーチャル IP アドレスに対応する役割を引き受けます。GLBP はリッスン ステートのゲートウェイから新しいスタンバイ バーチャル ゲートウェイを選択します。

## GLBP によるバーチャル フォワーダの冗長性

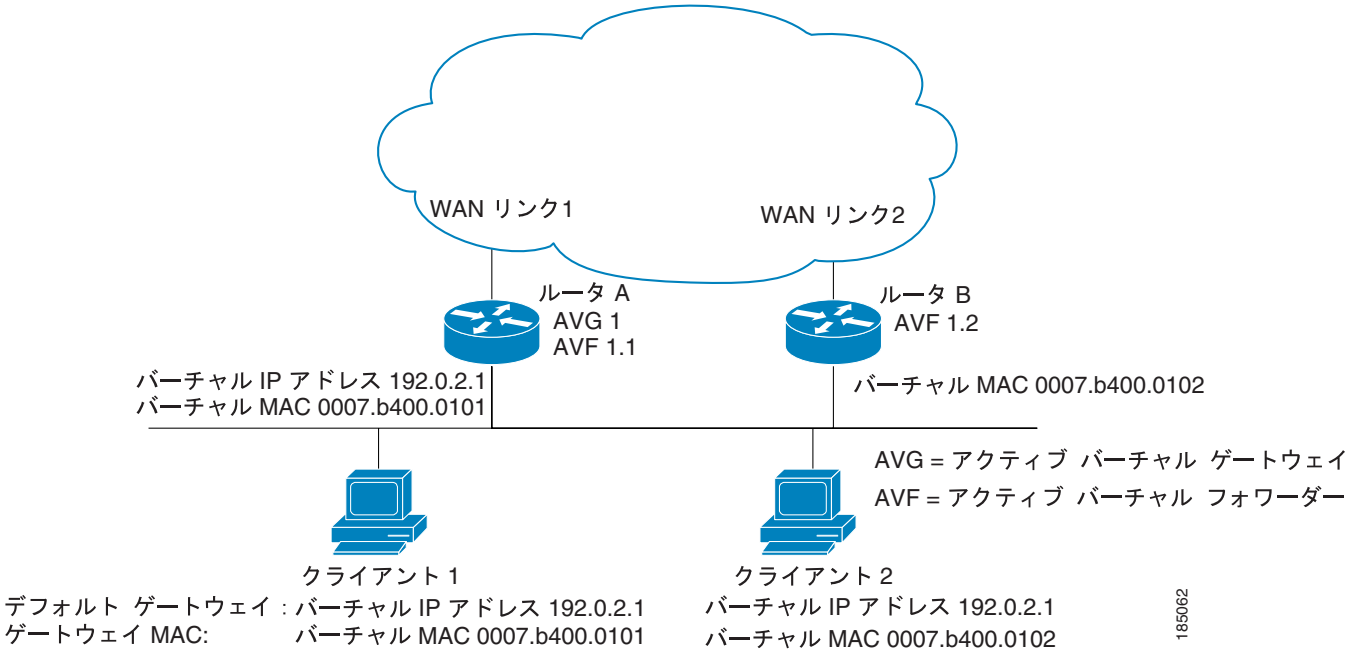
GLBP は、バーチャル フォワーダの冗長性を実現します。バーチャル フォワーダの冗長性は、アクティブ バーチャル フォワーダ（AVF）の点で、バーチャル ゲートウェイの冗長性と類似しています。AVF で障害が発生すると、リッスン ステートのセカンダリ バーチャル フォワーダがバーチャル MAC アドレスに対応する役割を引き受けます。このセカンダリ バーチャル フォワーダは、別のバーチャル MAC アドレスのプライマリ バーチャル フォワーダでもあります。GLBP は次の 2 種類のタイマーを使用して、障害 AVF の古いバーチャル MAC アドレスからホストを移行させます。

- リダイレクト タイマー ― AVG が古いバーチャル MAC アドレスにホストをリダイレクトし続ける時間の長さを指定します。リダイレクト タイムが経過すると、AVG は ARP 応答での古いバーチャル MAC アドレスの使用を中止しますが、セカンダリ バーチャル フォワーダは引き続き、古いバーチャル MAC アドレスに送信されたパケットを転送します。
- セカンダリ ホールド タイマー ― バーチャル MAC アドレスが有効な時間の長さを指定します。セカンダリ ホールド タイムが経過すると、GLBP が GLBP グループのすべてのゲートウェイからバーチャル MAC アドレスを削除し、残りの AVF 間でトラフィックのロード バランスが図られます。時間切れになったバーチャル MAC アドレスは、AVG による再割り当ての対象になります。

GLBP は hello メッセージを使用して、タイマーの現在のステートを伝えます。

図 4-1 では、ルータ A は GLBP グループの AVG であり、バーチャル IP アドレス 192.0.2.1 を担当します。ルータ A は、バーチャル MAC アドレス 0007.b400.0101 に対応する AVF でもあります。ルータ B は、同じ GLBP グループのメンバであり、バーチャル MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 にはデフォルト ゲートウェイ IP アドレス 192.0.2.1、バーチャル IP アドレス、およびゲートウェイ MAC アドレス 0007.b400.0101（ルータ A を指す）が設定されています。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ルータ B がルータ A とトラフィック負荷を分担するので、与えられているゲートウェイ MAC アドレスは 0007.b400.0102 です。

**図 4-1　GLBT トポロジ**




ルータ A が使用不能になっても、ルータ B がルータ A のバーチャル MAC アドレス宛てのパケットの転送を引き受け、自分のバーチャル MAC アドレス宛てのパケットに応答するので、クライアント 1 が WAN にアクセスできなくなることはありません。ルータ B は、GLBP グループ全体の AVG の役割も引き受けます。GLBP グループ内のルータで障害が発生しても、GLBP メンバの通信は継続されます。

## GLBP 認証

GLBP の認証タイプは、次の 3 種類です。

- MD5 認証
- プレーンテキスト認証
- 認証なし

MD5 認証を使用すると、プレーンテキスト認証より強力なセキュリティが得られます。MD5 認証の場合、各 GLBP グループ メンバが秘密鍵を使用して、発信パケットに組み込まれる鍵付き MD5 ハッシュを生成します。受信側では、着信パケットの鍵付きハッシュが生成されます。着信パケット内のハッシュが生成されたハッシュと一致しなかった場合、そのパケットは無視されます。MD5 ハッシュの鍵は、鍵ストリングを使用してコンフィギュレーションに直接指定することも、キーチェーンによって間接的に供給することもできます。

プレーンテキストの単純なパスワードを使用して GLBP を認証する、または GLBP に関して認証を行わないという選択も可能です。

GLBP 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間で異なっている。
- MD5 ダイジェストがルータと着信パケット間で異なっている。
- テキスト認証ストリングがルータと着信パケット間で異なっている。

## GLBP ロード バランシングおよびトラッキング

GLBP で設定できるロード バランシング方式は、次のとおりです。

- ラウンドロビン — GLBP は ARP 応答で送信されたバーチャル MAC アドレスを循環させ、すべての AVF 間でトラフィックのロード バランシングを図ります。
- 重み付き — AVG はアドバタイズされた AVF の重み値を使用して、AVF に与える負荷を決定します。重み値が大きいほど、AVG が AVF に与えるトラフィックが多くなります。
- ホスト依存 — GLBP はホストの MAC アドレスを使用して、使用するホストに指示するバーチャル MAC アドレスを決定します。このアルゴリズムでは、バーチャル フォワーダの数が変わらないかぎり、ホストに同じバーチャル MAC アドレスが与えられることが保証されます。

IPv4 ネットワークのデフォルトは、ラウンドロビンです。インターフェイスで、GLBP に関するすべてのロード バランシングをディセーブルにできます。ロード バランシングを設定しなかった場合、AVG がホストへのすべてのトラフィックを引き受け、他の GLBP グループ メンバはスタンバイまたはリッスン モードになります。

インターフェイスまたはルートを追跡し、追跡対象のリンクがダウンした場合に、セカンダリ バーチャル フォワーダが引き継ぐように GLBP を設定できます。GLBP トラッキングでは、重み付きロード バランシングを使用して、GLBP グループ メンバが AVF として動作するかどうかを判別します。AVF としてのそのグループ メンバを使用できるか、または使用できないかを決定するには、初期重み値およびオプションのしきい値を設定する必要があります。追跡するインターフェイスも設定できます。また、インターフェイスがダウンしたときに、インターフェイスの重みがどれだけ減るか、その値も設定できます。GLBP グループの重みが下限しきい値を下回ると、メンバは AVF ではなくなり、セカンダリ バーチャル フォワーダが引き継ぎます。重みが上限しきい値を上回ると、メンバは AVF としての役割を再び得ます。

図 4-2 に、GLBP トラッキングおよび重み付けの例を示します。

**図 4-2　GLBP オブジェクト トラッキングおよび重み付け**

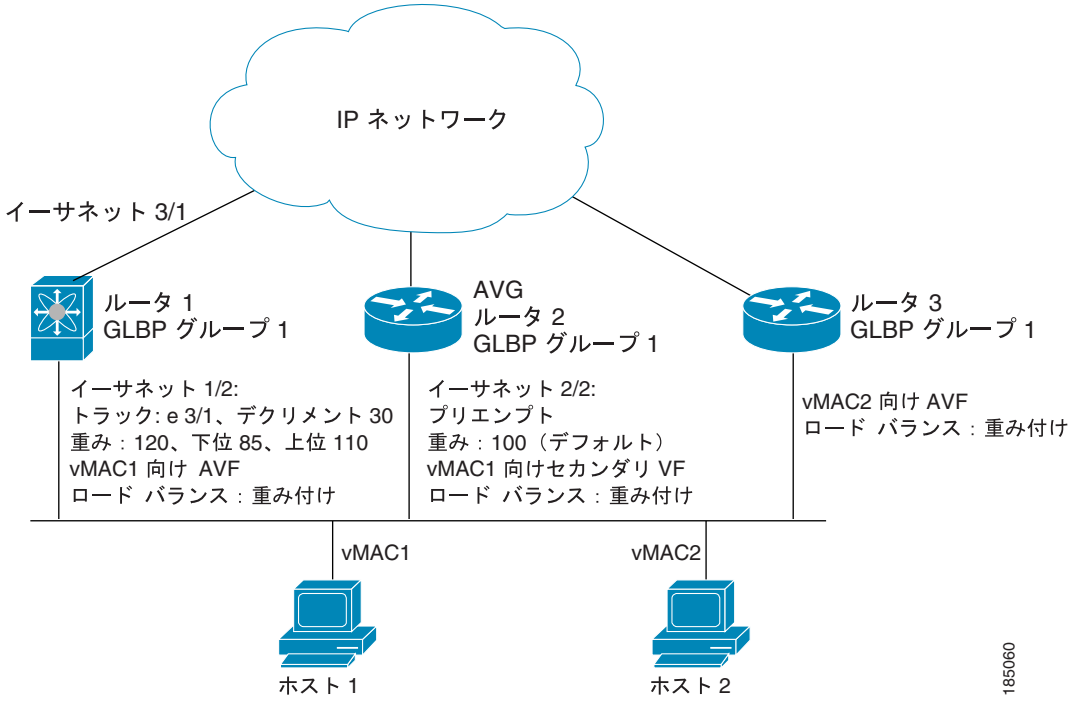



図 4-2 では、ルータ 1 上のインターフェイス Ethernet 1/2 がホスト 1 のゲートウェイ（バーチャル MAC アドレス vMAC に対応する AVF）です。一方、ルータ 2 上の Ethernet 2/2 は、ホスト 1 のセカンダリ バーチャル フォワーダとして動作します。Ethernet 1/2 は、ルータ 1 のネットワーク接続である Ethernet 3/1 を追跡します。Ethernet 3/1 がダウンすると、Ethernet 1/2 の重み値が 90 に下がります。ルータ 2 上の Ethernet 2/2 が Ethernet 1/2 に代わり、AVF として引き継ぎます。Ethernet 2/2 はデフォルトの重み値が 100 であり、AVF に関する優先権が設定されているからです。

重み付けおよび追跡の詳細については、「GLBP 重み付けおよびトラッキングの設定」（p.4-12）を参照してください。

## ハイ アベイラビリティ

GLBP は、ステートフル リスタートおよびステートフル スイッチオーバーをサポートします。ステートフル リスタートは、GLBP が障害を処理してリスタートするときに行われます。ステートフル スイッチオーバーは、アクティブ スーパーバイザがスタンバイ スーパーバイザに切り替わるときに行われます。Cisco NX-OS は、スイッチオーバー後に実行コンフィギュレーションを適用します。

## 仮想化サポート

GLBP 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。VRF は Virtual Device Contexts（VDC; 仮想化デバイス コンテキスト）内にあります。特に VDC および VRF を設定しないかぎり、デフォルトで、Cisco NX-OS はユーザにデフォルト VDC およびデフォルト VRF を使用させます。

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 GLBP 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、『*Cisco DCNM Virtual Device Context Configuration Guide*』を参照してください。

# GLBP 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 |
|---|---|
| DCNM | GLBP には、LAN Enterprise ライセンスが必要です。DCNM ライセンス方式の詳細、ライセンスを取得して適用する方法については、『*Cisco DCNM Licensing Guide*』を参照してください。 |
| NX-OS | GLBP 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、Cisco NX-OS システム イメージにバンドルされて提供されます。追加料金は発生しません。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。 |

# GLBP の前提条件

GLBP の前提条件は、次のとおりです。

- GLBP 機能をグローバルでイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。
- DCNM を使用して GLBP を設定するデバイスごとに、GLBP のロギング レベルを 6（情報）以上に設定する必要があります。必要最低限のロギング レベルにデバイスを設定するには、デバイスにコマンドライン インターフェイス（CLI）でログインし、次のコマンドを使用します。

```
logging event link-status default
logging level glbp 6
logging logfile messages 6
```

- GLBP を設定できるのは、レイヤ 3 インターフェイス上に限られます（『*Cisco DVNM Interface Configuration Guide*』を参照）。
- VDC を設定する場合は、Advanced Services ライセンスをインストールし、所定の VDC を開始してください（『*Cisco DCNM Virtual Device Context Configuration Guide*』を参照）。

# 注意事項および制約事項

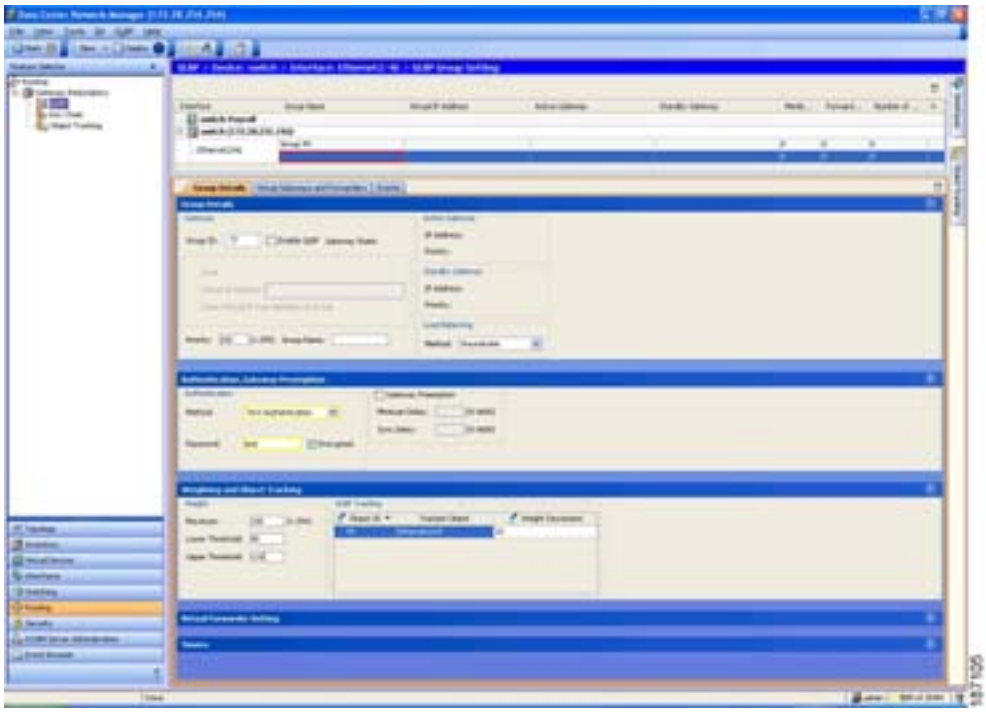
GLBP に関する注意事項および制約事項は、次のとおりです。

- バーチャル IP アドレスを設定することによって GLBP グループをイネーブルにするには、その前にすべての GLBP メンバ ゲートウェイ上で、GLBP に関するすべてのカスタマイズ オプションを設定する必要があります。
- GLBP がサポートする最小 hello タイムは 250 ms、最小ホールド タイムは 1020 ms です。
- GLBP 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、GLBP はアクティブになりません。
- GLBP バーチャル 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。
- VDC、インターフェイス VRF メンバシップ、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。

# GLBP の設定

Routing 機能選択から GLBP にアクセスできます。図 4-3 に GLBP を示します。

**図 4-3　GLBP の設定**



Data Center Network Manager 機能の詳細については、『*Cisco Data Center Network Manager Fundamentals Guide*』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。

## GLBP 機能のイネーブル化

GLBP グループを設定してイネーブルにする前に、GLBP 機能をイネーブルにする必要があります。

### 操作の前に

GLBP のロギング レベルを 6（情報）以上に設定する必要があります。必要最低限のロギング レベルにデバイスを設定するには、デバイスにコマンドライン インターフェイス（CLI）でログインし、次のコマンドを使用します。

```
logging event link-status default
logging level glbp 6
logging logfile messages 6
```

### 詳細な手順

GLBP 機能をイネーブルにするには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　Details ペインで、**Enable GLBP Service** をクリックします。

# GLBP グループの作成

インターフェイスに GLBP グループを作成できます。

### 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

### 手順詳細

GLBP グループを作成するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　メニュー バーから **GLBP > New GroupSetting** を選択します。

Summary ペインの GLBP 行が強調表示され、Details ペインでタブが更新されます。

**ステップ 4**　強調表示された Interface フィールドで、GLBP グループを設定したいインターフェイスをドロップダウン リストから選択します。

**ステップ 5**　Group Name フィールドで、このグループのグループ番号を入力します。

範囲は 0 ～ 1023 です。

システムは新しいグループをデバイスに作成し、Summary ペインの新しい GLBP グループを強調表示します。Details ペインでタブが更新されます。

**ステップ 6**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 7**　Group Details タブから、**Group Details** セクションを展開表示します。

Details ペインにグループの基本情報が表示されます。

**ステップ 8**　（任意）Priority フィールドから、この GLBP グループ メンバの優先順位を入力します。

範囲は 1 ～ 255 です。

**ステップ 9**　（任意）Group Name フィールドから、この GLBP グループ メンバ名を入力します。

**ステップ 10**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# GLBP 認証の設定

クリアテキストまたは MD5 ダイジェストを使用してプロトコルを認証するように、GLBP 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 DCNM Security Configuration Guide*』を参照）。

## 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

**（注）** GLBP グループのすべてのメンバに同じ認証および鍵を設定する必要があります。

## 詳細な手順

GLBP グループの認証をオンに設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　認証を設定したいグループを設定します。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブから、**Authentication, Gateway Preemption** セクションを展開表示します。

Details ペインに認証情報が表示されます。

**ステップ 6**　Authentication エリアの Method ドロップダウン リストから、認証方法を選択します。

**ステップ 7**　（任意）テキスト認証では、パスワード フィールドにパスワード文字列を入力し、暗号化パスワードの **encrypted** をチェックします。

**ステップ 8**　（任意）MD5 認証では、Key または Key Chain を選択します。

**ステップ 9**　（任意）Key オプションでは、キー フィールドにキー文字列を入力し、暗号化キー文字列の **encrypted** をチェックします。

**ステップ 10**　（任意）Key Chain オプションでは、キー チェーン ドロップダウン リストから使用したいキー チェーンを選択します。

**ステップ 11**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

## GLBP ロード バランシングの設定

ラウンドロビン、重み付き、またはホスト依存方式に基づいて、ロード バランシングを使用するように GLBP を設定できます（「GLBP ロード バランシングおよびトラッキング」[p.4-5] を参照）。

### 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

### 手順詳細

インターフェイスに GLBP ロード バランシングを設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing** > **Gateway Redundancy** > **GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　ロード バランシングを設定したいグループをクリックします。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブから、**Group Details** セクションを展開表示します。

Details ペインにグループの基本情報が表示されます。

**ステップ 6**　Load Balancing エリアの Method ドロップダウン リストから、ロード バランシング方法を選択します。

**ステップ 7**　メニュー バーから **File** > **Deploy** を選択して、デバイスに変更を適用します。

## GLBP 重み付けおよびトラッキングの設定

GLBP 重み値および GLBP 重み付きロード バランシング方式と連動するオブジェクト トラッキングを設定できます。

インターフェイスが最初にバーチャル MAC アドレスを指定して割り当てられている場合、またはインターフェイスの重み値が AVF より大きい場合に、そのインターフェイスによる AVF のプリエンプトを任意で設定できます。

### 操作の前に

GLBP 重み付けの変更で使用する、オブジェクト トラッキング エントリを設定したことを確認します（「オブジェクト トラッキングの設定」[p.5-1]）。

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

### 詳細な手順

GLBP 重み付けおよびトラッキングをインターフェイスに設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　重み付けとトラッキングを設定したいグループをクリックします。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブで、**Weighting and Object Tracking** セクションを展開表示します。

Details ペインに重み付けおよびオブジェクト トラッキング の情報が表示されます。

**ステップ 6**　Weight エリアで、重み値の最大値、下限しきい値、上限しきい値を入力します。

範囲は 1 ～ 254 です。

**ステップ 7**　GLBP Tracking エリアで、ポップアップ メニューから **Add Tracked Object** を右クリックして選択します。

**ステップ 8**　Object ID ドロップダウン リストから、GLBP 重み値の変更に使用するオブジェクト ID を選択します。

**ステップ 9**　Weighting フィールドで、トラッキングしたオブジェクトのステートが下がった場合に、GLBP 重み値の減少したい値を入力します。

**ステップ 10**（任意）Group Details タブで、**Virtual Forwarder Setting** セクションを展開表示します。

Details ペインに仮想転送情報が表示されます。

**ステップ 11**（任意）**Virtual Forwarder Preemption** をチェックします。

**ステップ 12**（任意）Preemption Delay フィールドで、遅延時間（秒）を入力します。

**ステップ 13**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# ゲートウェイ プリエンプションの設定

GLBP グループにゲートウェイ プリエンプションを設定できます。

## 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

## 詳細な手順

GLBP プリエンプションを設定するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　認証を設定したいグループを設定します。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブから、**Authentication, Gateway Preemption** セクションを展開表示します。

Details ペインにプリエンプション情報が表示されます。

**ステップ 6**　**Authentication, Gateway Preemption** セクションから、**Gateway Preemption** をチェックします。

**ステップ 7**　Minimum delay フィールドで、プリエンプションが発生する前の最小遅延時間を入力します。

デフォルト値は 3600 秒です。
Sync フィールドで、プリエンプションが発生する前に待機する同期遅延時間を入力します。
デフォルト値は 30 秒です。

**ステップ 8**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

## GLBP のカスタマイズ

GLBP 動作のカスタマイズは任意です。バーチャル IP アドレスを設定することによって、GLBP 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。GLBP をカスタマイズする前に GLBP 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 AVG になる可能性があります。GLBP のカスタマイズを予定している場合は、GLBP をイネーブルにする前に行ってください。

### 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

### 詳細な手順

GLBP タイマーをカスタマイズするには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　タイマーを設定したいグループをクリックします。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブから、**Timers** セクションを展開表示します。

Details ペインにプリエンプション情報が表示されます。

**ステップ 6**　Configured Timers エリアで、Hello Time (msec) フィールドに hello 時間を入力します。

**ステップ 7**　Configured Timers エリアで、Hold Time (msec) フィールドにホールド タイムを入力します。

**ステップ 8**　Configured Timers エリアで、Virtual Forwarders Redirect Time (msec) フィールドにリダイレクト時間を入力します。

**ステップ 9**　Configured Timers エリアで、Virtual Forwarders Hold Time (msec) フィールドにホールド タイムを入力します。

**ステップ 10**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# GLBP グループのイネーブル化

GLBP グループをイネーブルにするインターフェイス上で、バーチャル IP アドレスを設定できます。同じグループ番号を指定して、GLBP グループの各ゲートウェイを設定する必要があります。GLBP メンバは別の GLBP メンバから必要な他のあらゆるパラメータを学習できます。

## 操作の前に

GLBP 機能をイネーブルにします（「GLBP 機能のイネーブル化」[p.4-9] を参照）。

## 詳細な手順

GLBP グループをイネーブルにするには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > GLBP** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、GLBP を設定したいデバイスをクリックします。

**ステップ 3**　タイマーを設定したいグループをクリックします。

**ステップ 4**　Details ペインで、**Group Details** タブをクリックします。

Group Details タブが表示されます。

**ステップ 5**　Group Details タブから、**Group Details** セクションを展開表示します。

Details ペインに一般情報が表示されます。

**ステップ 6**　Gateway エリアで、**Enable GLBP** をチェックします。

**ステップ 7**　**IPv4** をチェックします。

**ステップ 8**　（任意）バーチャル IP アドレスを手動で設定するには、バーチャル IP アドレスを選択して、IP アドレスを入力します。

**ステップ 9**　（任意）バーチャル IP アドレスを学習するには、Learn Virtual IP From Members Of Group を選択します。

**ステップ 10**（任意）Virtual Secondary IP Address フィールドから、セカンダリ IP アドレスを入力します。

**ステップ 11**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# GLBP のフィールドの説明

ここでは、GLBP のフィールドについて説明します。内容は次のとおりです。



## GLBP：Group Details タブ：Group Details セクション

**表 4-1　GLBP：Group Details：Group Details**

| フィールド | 説明 |
|---|---|
| **ゲートウェイ** | |
| Group ID | *表示のみ。*GLBP グループのグループ番号 |
| Enable GLBP | このグループ メンバについて、GLBP をイネーブルにします。 |
| Gateway State | *表示のみ。*グループ メンバの管理状態 |
| IPv4 | グループの IPv4 アドレス |
| Virtual IP Address | グループのバーチャル IP アドレスを使用します。 |
| Learn Virtual IP from Members of Group | グループの学習した IP アドレスを使用します。 |
| Virtual Secondary IP Address | グループのセカンダリ IP アドレス |
| Priority | AVG の選択で使用するグループ メンバの優先順位 |
| Group Name | GLBP グループの名前 |

## GLBP：Group Details タブ：認証、ゲートウェイ プリエンプション セクション

**表 4-2　GLBP：Group Details：認証、ゲートウェイ プリエンプション セクション**

| フィールド | 説明 |
|---|---|
| **IPv4 アドレスの設定** | |
| Primary | IPv4 アドレス（ドット付き 10 進表記） |
| Net Mask | IPv4 アドレスのネットワーク マスク（ドット付き 10 進表記） |
| Secondary IP Address | セカンダリ IPv4 アドレス（ドット付き 10 進表記）。インターフェイスに複数のセカンダリ アドレスを設定できます。 |
| Secondary NetMask | セカンダリ IPv4 アドレスのネットワーク マスク（ドット付き 10 進表記） |
| Helper IP Address | User Datagram Protocol（UDP）ブロードキャスト転送をイネーブルにするために使用するヘルパー アドレス |
| **IPv6 アドレスの設定** | |
| Primary/Prefix-length | x:x:x:x/ 長さ フォーマットの IPv6 プレフィクス |
| EUI64 | Extended Universal Identifier（EUI）64 フォーマットの IPv6 アドレス |

表 4-2　GLBP：Group Details：認証、ゲートウェイ プリエンプション セクション（続き）

| フィールド | 説明 |
|---|---|
| Link Local | リンク ローカル アドレス x:x:x:x フォーマットの IPv6 |
| Use local only | 自動生成された IPv6 アドレスを上書きするリンク ローカル アドレス |
| Secondary IP Address/Prefix Length | x:x:x:x/ 長さ フォーマットのセカンダリ IPv6 プレフィクス。インターフェイスに複数のセカンダリ アドレスを設定できます。 |
| EUI64 | EUI-64 フォーマットのセカンダリ アドレス |

## GLBP：Group Details タブ：Weighting and Object Tracking セクション

表 4-3　GLBP：Group Details：Weighting and Object Tracking

| フィールド | 説明 |
|---|---|
| Status | 統計情報の収集状況。Status でカーソルを移動させると、ポップアップ画面で表示 |
| Select Parameters | ループバック インターフェイスで収集される統計情報の一覧 |
| Show Overview Chart | ポップアップ画面で表示される統計情報の概要 |

## GLBP：Group Details タブ：Virtual Forwarder Setting セクション

表 4-4　GLBP：Group Details：Virtual Forwarder Setting

| フィールド | 説明 |
|---|---|
| Name | *表示のみ*。SVI の名前 |
| Admin Status | SVI の管理ステータス。デフォルトはアップ |
| MTU（バイト） | Maximum Transmission Unit（最大伝送ユニット）。デフォルト値は 1500 です。 |
| delay（数十マイクロ秒） | インターフェイス スループット遅延（数十マイクロ秒）。デフォルトは 1（10 マイクロ秒） |
| 説明 | SVI の説明 |
| Oper Status | SVI の運用状況 |
| Bandwidth（キロバイト） | SVI のインターフェイス帯域幅（岐路バイト）。デフォルト値は 100000 です。 |

## GLBP：Group Details タブ：Timers セクション

表 4-5　GLBP：Group Details：Timers

| フィールド | 説明 |
|---|---|
| **IPv4 アドレスの設定** | |
| Primary | IPv4 アドレス（ドット付き 10 進表記） |
| Net mask | IPv4 アドレスのネットワーク マスク（ドット付き 10 進表記） |
| Secondary IP Address | セカンダリ IPv4 アドレス（ドット付き 10 進表記）。インターフェイスに複数のセカンダリ アドレスを設定できます。 |
| Secondary NetMask | セカンダリ IPv4 アドレスのネットワーク マスク（ドット付き 10 進表記） |
| Helper IP Address | User Datagram Protocol（UDP）ブロードキャスト転送をイネーブルにするために使用するヘルパー アドレス |
| **IPv6 アドレスの設定** | |
| Primary/Prefix-length | x:x:x:x/ 長さ フォーマットの IPv6 プレフィクス |
| EUI64 | EUI-64 フォーマットの IPv6 アドレス |
| Link Local | リンク ローカル アドレス x:x:x:x フォーマットの IPv6 |
| Use local only | 自動生成された IPv6 アドレスを上書きするリンク ローカル アドレス |
| Secondary IP Address/Prefix Length | x:x:x:x/ 長さ フォーマットの IPv6 プレフィクス。インターフェイスに複数のセカンダリ アドレスを設定できます。 |
| EUI64 | EUI-64 フォーマットのセカンダリ アドレス |

## GLBP：Virtual Gateways and Forwarders タブ：Forwarder Details セクション

表 4-6　GLBP：Virtual Gateways and Forwarders：Forwarder Details

| フィールド | 説明 |
|---|---|
| Status | 統計情報の収集状況。Status でカーソルを移動させると、ポップアップ画面で表示 |
| Select Parameters | SVI で収集される統計情報の一覧 |
| Show Overview Chart | ポップアップ画面で表示される統計情報の概要 |

## GLBP：Virtual Gateways and Forwarders タブ：GLBP Group Member Details セクション

表 4-7　GLBP：Virtual Gateways and Forwarders：GLBP Group Member Details

| フィールド | 説明 |
|---|---|
| Status | 統計情報の収集状況。Status でカーソルを移動させると、ポップアップ画面で表示 |
| Select Parameters | SVI で収集される統計情報の一覧 |
| Show Overview Chart | ポップアップ画面で表示される統計情報の概要 |

# その他の関連資料

GLBP 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.4-20）
- 規格（p.4-20）


## 関連資料

| 関連項目 | マニュアル名 |
|---|---|
| GLBP CLI コマンド | 『*Cisco NX-OS Unicast Routing Command Reference, Release 4.0*』 |
| ハイ アベイラビリティの設定 | 『*Cisco NX-OS High Availability and Redundancy Guide, Release 4.0*』 |

## 規格

| 規格 | タイトル |
|---|---|
| この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。 | — |

CHAPTER 5

# オブジェクト トラッキングの設定

この章では、Cisco NX-OS デバイス上でオブジェクト トラッキングを設定する方法について説明します。

ここでは、次の内容を説明します。

# 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、ルータ到達可能性など、ネットワーク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の向上し、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ますが、オブジェクトのステートが変化したときに取るアクションはクライアントごとに異なります。

クライアントには次の機能が含まれます。

- HSRP（ホットスタンバイ冗長プロトコル）
- Gateway Load Balancing Protocol（GLBP）
- Embedded Event Manager（EEM）

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監視し、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 IP アドレスが設定されていて、IP 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 ― ルートが存在していて、ローカル デバイス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。リンク プロトコルがダウンした場合、影響を受ける HSRP ルータのプライオリティを変更し、よりすぐれたネットワーク接続が得られるバックアップ ルータにスイッチオーバーされるようにできます。

## ハイ アベイラビリティ

オブジェクト トラッキングは、ステートフル リスタートを通じてハイ アベイラビリティをサポートします。ステートフル リスタートが実行されるのは、オブジェクト トラッキング プロセスがクラッシュした場合です。オブジェクト トラッキングは、デュアル スーパーバイザ システムでのステートフル スイッチオーバーもサポートします。スイッチオーバー後に Cisco NX-OS が実行コンフィギュレーションを適用します。

オブジェクト トラッキングを使用して、ネットワーク全体の可用性が向上するように、クライアントの動作を変更することもできます。

## 仮想化サポート

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。VRF は Virtual Device Contexts（VDC; 仮想化デバイス コンテキスト）内にあります。特に VDC および VRF を設定しないかぎり、デフォルトで、Cisco NX-OS はユーザにデフォルト VDC およびデフォルト VRF を使用させます。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。

詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』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 |
|---|---|
| DCNM | オブジェクト トラッキングには、LAN Enterprise ライセンスが必要です。DCNM ライセンス方式の詳細、ライセンスを取得して適用する方法については、『*Cisco DCNM Licensing Guide*』を参照してください。 |
| 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、Cisco NX-OS システム イメージにバンドルされて提供されます。追加料金は発生しません。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。 |

# オブジェクト トラッキングの前提条件

オブジェクト トラッキングの前提条件は、次のとおりです。

- DCNM を使用して GLBP を設定するデバイスごとに、GLBP のロギング レベルを 5（情報）以上に設定する必要があります。必要最低限のロギング レベルにデバイスを設定するには、デバイスにコマンドライン インターフェイス（CLI）でログインし、次のコマンドを使用します。

```
logging event link-status default
logging level track 5
logging logfile messages 5
```

- VDC を設定する場合は、Advanced Services ライセンスをインストールし、所定の VDC を開始してください（『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照）。

# 注意事項および制約事項

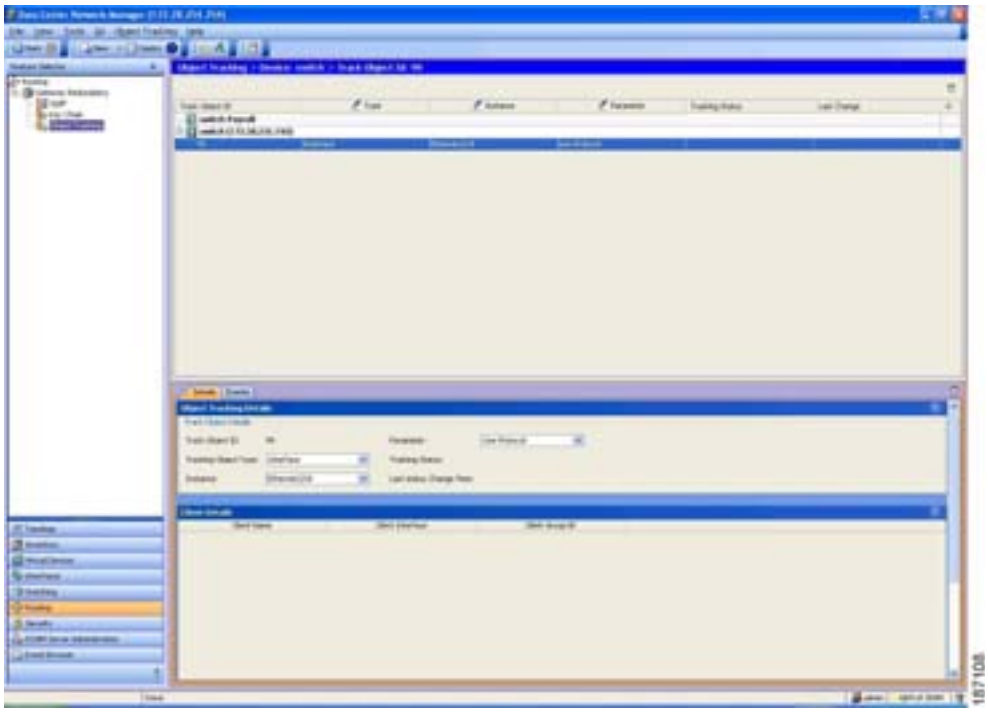
オブジェクト トラッキングに関する注意事項および制約事項は、次のとおりです。

- VDC ごとに最大 500 のトラッキング対象オブジェクトをサポートします。
- サポートするのは、IPv4 アドレスに限られます。
- イーサネット、サブインターフェイス、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。
- 1 つの HSRP グループまたは GLBP グループでサポートするトラッキング対象オブジェクトは 1 つです。

# オブジェクト トラッキングの設定

Routing 機能選択からオブジェクト トラッキングにアクセスできます。図5-1 にオブジェクト トラッキングの設定方法を示します。

**図 5-1　オブジェクト トラッキングの設定**



Data Center Network Manager 機能の詳細については、『*Cisco Data Center Network Manager Fundamentals Guide*』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。


- インターフェイスのオブジェクト トラッキング設定（p.5-5）
- ルート到達可能性のオブジェクト トラッキング設定（p.5-7）


## 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 IP 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。

### 操作の前に

オブジェクト トラッキングのロギング レベルを 5（情報）以上に設定する必要があります。必要最低限のロギング レベルにデバイスを設定するには、デバイスにコマンドライン インターフェイス（CLI）でログインし、次のコマンドを使用します。

```
logging event link-status default
logging level track 5
logging logfile messages 5
```

## 詳細な手順

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するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > Object Tracking** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、オブジェクト トラッキングを設定したいデバイスをクリックします。

**ステップ 3**　メニュー バーから、**Object Tracking > New > Track Object** を選択します。

Summary ペインの新しいトラッキング対象オブジェクトが強調表示され、Details ペインでタブが更新されます。

**ステップ 4**　強調表示された Track Object ID フィールドで、オブジェクト ID を入力します。

**ステップ 5**　Details ペインで、**Object Tracking Details** タブをクリックします。

Object Tracking Details タブが表示されます。

**ステップ 6**　Object Tracking Details タブで、Tracking Object Type ドロップダウン リストから **Interface** を選択します。

**ステップ 7**　Instance ドロップダウン リストから、追跡したいインターフェイスを選択します。

**ステップ 8**　Parameter ドロップダウン リストから、**IP routing** または **Line Protocol** を選択します。

**ステップ 9**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# 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。

## 操作の前に

オブジェクト トラッキングのロギング レベルを 5（情報）以上に設定する必要があります。必要最低限のロギング レベルにデバイスを設定するには、デバイスにコマンドライン インターフェイス（CLI）でログインし、次のコマンドを使用します。

```
logging event link-status default
logging level track 5
logging logfile messages 5
```

## 詳細な手順

ルート到達可能性のトラッキング対象オブジェクトを作成するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > Object Tracking** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、オブジェクト トラッキングを設定したいデバイスをクリックします。

**ステップ 3**　メニュー バーから、**Object Tracking > New > Track Object** を選択します。

Summary ペインの新しいトラッキング対象オブジェクトが強調表示され、Details ペインでタブが更新されます。

**ステップ 4**　強調表示された Track Object ID フィールドで、オブジェクト ID を入力します。

**ステップ 5**　Details ペインで、**Object Tracking Details** タブをクリックします。

Object Tracking Details タブが表示されます。

**ステップ 6**　Object Tracking Details タブで、Tracking Object Type ドロップダウン リストから **IP Route** を選択します。

**ステップ 7**　Instance フィールドで、追跡したい IP プレフィクスとネットワーク マスク長を入力します。

フォーマットは A.B.C.D/ 長さです。

**ステップ 8**　（任意）VRF name ドロップダウン リストから、このルートが存在する VRF を選択します。

デフォルトは、デフォルト設定の VRF です。

**ステップ 9**　メニュー バーから **File > Deploy** を選択して、デバイスに変更を適用します。

# クライアントの詳細の表示

トラッキング対象オブジェクトを使用しているクライアントを表示できます。

### 詳細な手順

トラッキング対象オブジェクトを使用するクライアントの詳細を表示するには、次の手順を実行します。

**ステップ 1**　Feature Selector ペインで、**Routing > Gateway Redundancy > Object Tracking** の順に選択します。

Summary ペインに使用できるデバイスが表示されます。

**ステップ 2**　Summary ペインで、トラッキング対象オブジェクトを表示したいデバイスをクリックします。

**ステップ 3**　クライアントを表示したいトラッキング対象オブジェクトをクリックします。

Summary ペインのトラッキング対象オブジェクトが強調表示され、Details ペインでタブが更新されます。

**ステップ 4**　Details ペインで、**Object Tracking Details** タブをクリックします。

Object Tracking Details タブが表示されます。

**ステップ 5**　Object Tracking Details タブで、**Client Details** セクションをクリックします。

クライアントの詳細が表示されます。

# 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 4 章「GLBP の設定」

# Object Tracking フィールドの説明

ここでは、Object Tracking のフィールドについて説明します。内容は次のとおりです。



## Object Tracking：Details タブ：Object Tracking Details セクション

**表 5-1　Object Tracking：Details：Object Tracking Details**

| フィールド | 説明 |
|---|---|
| Track Object ID | *表示のみ。*トラッキング対象オブジェクトのオブジェクト番号 |
| Tracking Object Type | トラッキングするオブジェクトのタイプ |
| Instance | オブジェクトをトラッキングするための IP アドレスまたはインターフェイス |
| VRF | トラッキング対象インターフェイスのある VRF |
| Parameter | オブジェクトをトラッキングするためのパラメータ タイプ |
| Tracking Status | *表示のみ。*トラッキング対象オブジェクト パラメータのステータス |
| Last status Change Time | *表示のみ。*パラメータが最後にオブジェクトのステータスを変更した時刻 |

## Object Tracking：Details タブ：Client Details セクション

**表 5-2　Object Tracking：Details：Client Details**

| フィールド | 説明 |
|---|---|
| Client Name | *表示のみ。*トラッキング対象オブジェクトを使用する機能の名前 |
| Client Interface | 命名されたクライアント機能のトラッキング対象オブジェクトを使用するインターフェイス |
| Client Group-ID | *表示のみ。*命名されたクライアント機能のトラッキング対象オブジェクトを使用するグループ ID |

# 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.5-10）
- 規格（p.5-10）


## 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 NX-OS Unicast Routing Command Reference, Release 4.0*』 |
| Embedded Event Manager の設定 | 『*Cisco NX-OS System Management Configuration Guide, Release 4.0*』 |

## 規格

| 規格 | タイトル |
|---|---|
| この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。 | — |

APPENDIX **A**

# Cisco NX-OS Unicast Features Release 4.x がサポートする IETF RFC

この付録は、Cisco NX-OS Release 4.x がサポートする IETF RFC の一覧です。

## IP サービスの RFC

| 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*』 |

## IPv6 の RFC

| RFC | タイトル |
|---|---|
| RFC 1981 | 『*Path MTU Discovery for IP version 6*』 |
| RFC 2373 | 『*IP Version 6 Addressing Architecture*』 |
| RFC 2374 | 『*An Aggregatable Global Unicast Address Format*』 |
| RFC 2460 | 『*Internet Protocol, Version 6 (IPv6) Specification*』 |
| RFC 2461 | 『*Neighbor Discovery for IP Version 6 (IPv6)*』 |
| RFC 2462 | 『*IPv6 Stateless Address Autoconfiguration*』 |
| RFC 2463 | 『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』 |
| RFC 2464 | 『*Transmission of IPv6 Packets over Ethernet Networks*』 |
| RFC 2467 | 『*Transmission of IPv6 Packets over FDDI Networks*』 |
| RFC 2472 | 『*IP Version 6 over PPP*』 |
| RFC 2492 | 『*IPv6 over ATM Networks*』 |
| RFC 2590 | 『*Transmission of IPv6 Packets over Frame Relay Networks Specification*』 |
| RFC 3152 | 『*Delegation of IP6.ARPA*』 |

| RFC | タイトル |
|---|---|
| RFC 3162 | 『*RADIUS and IPv6*』 |
| RFC 3513 | 『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』 |
| RFC 3596 | 『*DNS Extensions to Support IP version 6*』 |
| RFC 4193 | 『*Unique Local IPv6 Unicast Addresses*』 |

# 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** 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** 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** バックアップ代表ルータ。マルチアクセス OSPF ネットワークにおいて、代表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、代表ルータと同様、バックアップ代表ルータ（BDR）とも隣接関係を形成します。

**BGP** 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エクステリア ゲートウェイ プロトコルです。

**BGP スピーカ** BGP 対応ルータ。

**BGP ピア** ローカル BGP スピーカと隣接関係が確立されている、リモート BGP スピーカ。

## D

**DHCP** 動的ホスト制御プロトコル。

**Diffusing アップデート アルゴリズム** DUAL を参照してください。

**DNS クライアント** 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** 代表ルータ。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、代表ルータおよびバックアップ代表ルータとだけ隣接関係を確立します。

**DUAL** Diffusing アップデート 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 IGRP。Diffusing アップデート 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** 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。

## G

**GLBP** Gateway Load Balancing Protocol。エンド ホストにハイ アベイラビリティ機能を提供する、シスコ独自のプロトコル。

## H

**hello インターバル** 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。

**HSRP**

## I

**iBGP** 内部 BGP（ボーダー ゲートウェイ プロトコル）。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** インテリア ゲートウェイ プロトコル。同じ自律システム内のルータ間で使用されます。

**IPv4** インターネット プロトコル バージョン 4。

**IPv6** インターネット プロトコル バージョン 6。

**IP トンネル**

**IS-IS** Intermediate System to Intermediate System。ISO インテリア ゲートウェイ プロトコル。

## L

**LSA** 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** 認証鍵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

**NDP** Neighbor Discovery Protocol（近隣探索プロトコル）。IPv6 アドレスに関連付けられた MAC アドレスを検索するために、IPv6 で使用されるプロトコル。

**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、OSPFv3 は IPv6 をサポートします。

## R

**RIB** 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。

**Route Policy Manager** ルート マップおよびポリシーベース ルーティングを制御するプロセス。

## 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

**U6FIB** ユニキャスト IPv6 転送情報ベース。

**U6RIB** ユニキャスト IPv6 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。

**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

**VDC** Virtual Device Context（仮想デバイス コンテキスト）。物理システムを安全で独立した論理システムに分割するために使用されます。

**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

**アトリビュート** BGP UPDATE メッセージで送信される、ルートのプロパティ。これらのアトリビュートには、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含まれます。

**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。

## 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

**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。

**管理ディスタンス** 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。

## き

**キーチェーン管理** A method of controlling authentication keys.『*Cisco NX-OS Security Configuration Guide*』を参照してください。

**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。

## く

**グレースフル リスタート** ルーティング プロトコルのリブート時に、ルータがデータ転送パスにとどまるようにする機能。

## け

**ゲートウェイ** LAN からネットワークのその他の部分にレイヤ 3 トラフィックを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

**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。

**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

**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。

**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。

## た

**帯域幅** リンクの使用可能なトラフィック容量。

**代表ルータ** DR を参照してください。

## 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。

**デッド インターバル** 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 インターバルは通常、hello インターバルの倍数です。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。

## ね

**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。

**ネットワーク レイヤ到達可能性情報** 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。

## は

**ハイ アベイラビリティ** コンポーネントで障害が発生したときに、システムまたはコンポーネントがネットワークの停止を制限または回避する能力。

**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。

**バックアップ代表ルータ** BDR を参照してください。

## ふ

**フィージブル サクセッサ** 現在のフィージブル 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。

**フィージブル 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。フィージブル 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。

**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。

**ポリシーベース ルーティング** パケットに選択されたルートをルート マップを使用して変更する方式。

## 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

**リライアブル トランスポート プロトコル** 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。

**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** ネイバー 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。

**ルーティング情報ベース** RIB を参照してください。

**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。ルート再配布およびポリシー ベース ルーティングで使用されます。

## 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

## N



## O



## あ



## い



## お



## か



## き



## し



## ね



## は



## ら



## る