Cisco DCNM 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.x

Cisco DCNM Unicast Routing Configuration Guide, Release 5.x

2010 年 10 月

Text Part Number: OL-23436-01-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。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Cisco DCNM 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.x
© 2009–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009–2011, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

新機能と変更された機能 vii

はじめに ix

対象読者 ix

マニュアルの構成 ix

表記法 x

関連資料 x

Cisco DCNM のマニュアル x

Cisco Nexus 1000V シリーズ スイッチ マニュアル xi

Cisco Nexus 2000 シリーズ Fabric Extender のマニュアル xi

Cisco Nexus 4000 シリーズ スイッチ マニュアル xii

Cisco Nexus 5000 シリーズ スイッチ マニュアル xii

Cisco Nexus 7000 シリーズ スイッチ マニュアル xii

マニュアルの入手方法およびテクニカル サポート xiii

CHAPTER 1

概要 1-1

IPv4 と IPv6 1-1

ファーストホップ冗長プロトコル 1-1

オブジェクト トラッキング 1-1

CHAPTER 2

IPv4 の設定 2-1

IPv4 について 2-1

複数の IPv4 アドレス 2-2

IPv4 のライセンス要件 2-2

プラットフォーム サポート 2-3

IPv4 の設定 2-3

IPv4 アドレス指定の設定 2-3

複数の IP アドレスの設定 2-4

IP のフィールドに関する説明 2-4

その他の関連資料 2-5

関連資料 2-5

標準規格 2-5

IP 機能の履歴 2-5

CHAPTER 3 **IPv6 の設定** 3-1

IPv6 について 3-1
IPv6 アドレス フォーマット 3-2
IPv6 ユニキャスト アドレス 3-3
集約可能グローバル アドレス 3-3
リンクローカル アドレス 3-5
IPv4 互換 IPv6 アドレス 3-5
ユニーク ローカル アドレス 3-6
サイトローカル アドレス 3-7
IPv6 エニーキャスト アドレス 3-7
IPv6 マルチキャスト アドレス 3-7
IPv4 パケット ヘッダー 3-9
簡易 IPv6 パケット ヘッダー 3-9
IPv6 の DNS 3-12
IPv6 のパス MTU 探索 3-12
CDP IPv6 アドレスのサポート 3-13
IPv6 の ICMP 3-13
IPv6 ネイバー探索 3-14
IPv6 ネイバー送信要求メッセージ 3-14
IPv6 ルータ アドバタイズメント メッセージ 3-15
IPv6 ネイバー リダイレクト メッセージ 3-17
IPv6 のライセンス要件 3-18
プラットフォーム サポート 3-18
IPv6 の設定 3-18
IPv6 アドレス指定の設定 3-18
IPv6 セカンダリ アドレスの設定 3-19
IPv6 のフィールドに関する説明 3-20
その他の関連資料 3-20
関連資料 3-20
標準規格 3-20
IPv6 機能の履歴 3-20

CHAPTER 4 **GLBP の設定** 4-1

GLBP の概要 4-1
GLBP の概要 4-2
GLBP アクティブ仮想ゲートウェイ 4-2
GLBP 仮想 MAC アドレス割り当て 4-2
GLBP による仮想ゲートウェイの冗長性 4-3

GLBP による仮想フォワーダの冗長性 4-3
GLBP 認証 4-4
GLBP ロード バランシングおよびトラッキング 4-5
ハイ アベイラビリティ 4-6
GLBP のライセンス要件 4-6
GLBP の前提条件 4-6
デフォルト設定 4-7
プラットフォーム サポート 4-7
GLBP の設定 4-7
GLBP グループの作成 4-8
GLBP 認証の設定 4-8
GLBP ロード バランシングの設定 4-9
GLBP 重み付けおよびトラッキングの設定 4-10
ゲートウェイ プリエンプトの設定 4-10
GLBP のカスタマイズ 4-11
GLBP グループのイネーブル化 4-12
GLBP のフィールドに関する説明 4-12
[GLBP] : [Group Details] タブ : [Group Details] セクション 4-13
[GLBP] : [Group Details] タブ : [Authentication, Gateway Preemption] セクション 4-13
[GLBP] : [Group Details] タブ : [Weighting and Object Tracking Sectio] セクション 4-14
[GLBP] : [Group Details] タブ : [Virtual Forwarder Setting] セクション 4-14
[GLBP] : [Group Details] タブ : [Timers] セクション 4-14
[GLBP] : [Virtual Gateways and Forwarders] タブ : [Forwarder Details] セクション 4-15
[GLBP] : [Virtual Gateways and Forwarders] タブ : [GLBP Group Member Details] セクション 4-15
その他の関連資料 4-15
関連資料 4-16
標準規格 4-16
GLBP 機能の履歴 4-16

CHAPTER 5 **HSRP の設定** 5-1
HSRP について 5-1
HSRP の概要 5-2
IPv4 の HSRP 5-3
IPv6 の HSRP 5-4
HSRP IPv6 アドレス 5-4

HSRP のバージョン 5-5
HSRP 認証 5-6
HSRP メッセージ 5-6
HSRP ロード シェアリング 5-6
オブジェクト トラッキングおよび HSRP 5-7
ハイ アベイラビリティ 5-8
HSRP のライセンス要件 5-8
HSRPP の前提条件 5-8
デフォルト設定 5-9
プラットフォーム サポート 5-9
HSRP の設定 5-9
HSRP バージョン設定 5-10
IPv4 の HSRP グループの設定 5-10
IPv6 の HSRP グループの設定 5-11
HSRP 仮想 MAC アドレスの設定 5-12
HSRP の認証 5-13
プリエンプトの設定 5-14
HSRP のオブジェクト トラッキングの設定 5-15
HSRP プライオリティの設定 5-15
HSRP のカスタマイズ 5-16
HSRP のフィールドに関する説明 5-17
[HSRP]: [Group Details] タブ : [Group Details] セクション 5-17
[HSRP]: [Group Details] タブ : [Authentication, Router Preemption] セクション 5-18
[HSRP]: [Group Details] タブ : [Timers] セクション 5-18
[HSRP]: [Group Details] タブ : [Object Tracking] セクション 5-19
[HSRP]: [Interface Settings] タブ 5-19
その他の関連資料 5-19
関連資料 5-20
MIB 5-20
HSRP 機能の履歴 5-20

CHAPTER 6 **オブジェクト トラッキングの設定 6-1**
オブジェクト トラッキング情報 6-1
オブジェクト トラッキングの概要 6-1
ハイ アベイラビリティ 6-2
オブジェクト トラッキングのライセンス要件 6-3
オブジェクト トラッキングの前提条件 6-3

デフォルト設定 6-3
プラットフォーム サポート 6-3
オブジェクト トラッキングの設定 6-4
インターフェイスのオブジェクト トラッキング設定 6-4
IPv6 インターフェイスのオブジェクト トラッキング設定 6-5
インターフェイス IPv6 オブジェクト トラッキングの削除 6-5
新しい IP ルート IPv6 オブジェクト トラッキングの作成 6-6
IP ルート IPv6 オブジェクト トラッキングの削除 6-6
ルート到達可能性のオブジェクト トラッキング設定 6-7
クライアントの詳細情報の表示 6-8
関連資料 6-8
オブジェクト トラッキングのフィールドに関する説明 6-8
[Object Tracking]: [Details] タブ : [Object Tracking Details] セクション 6-8
[Object Tracking]: [Details] タブ : [Client Details] セクション 6-9
その他の関連資料 6-10
関連資料 6-10
標準規格 6-10
オブジェクト トラッキング機能の履歴 6-10

APPENDIX A **Cisco NX-OS Unicast Features Release 5.x がサポートする IETF RFC** A-1
IP サービスに関する RFC の参考資料 A-1
IPv6 の RFC A-1

GLOSSARY

INDEX

新機能と変更された機能

この章では、『*Cisco DCNM Unicast Routing Configuration Guide, Release 5.x*』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。
lhttp://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/unicast/configuration/guide/l3_dcnm-book.htmll

Cisco DCNM Release 5.x に関する追加情報を確認するには、次のシスコ Web サイトにアクセスして、『*Cisco DCNM Release Notes*』を参照してください。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/release/notes/dcnm_5_x_relnotes.html

表 1 では、『*Cisco DCNM Unicast Routing Configuration Guide, Release 5.x*』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.x の新機能および機能変更

機能	説明	変更されたリリース	参照先
オブジェクト トラッキング	IPv6 インターフェイスでオブジェクト トラッキング設定のサポートが追加されました。	5.1(1)	第 6 章「オブジェクト トラッキングの設定」
HSRP	IPv6 のサポートが追加されました。	5.0(2)	第 5 章「HSRP の設定」
オブジェクト トラッキング	IPv6 のサポートが追加されました。	5.0(2)	第 6 章「オブジェクト トラッキングの設定」

はじめに

このマニュアルでは、Cisco Data Center Network Manager（DCNM）での Cisco NX-OS ユニキャスト ルーティング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「IPv6 の設定」	IPv6 を設定および管理する手順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「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 6 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.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。
Appendix B, “Configuration Limits for Cisco NX-OS Layer 3 Unicast Features, Release 5.x”	Cisco Nexus 7000 シリーズの設定の制限の一覧です。

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*」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

ここでは、Cisco DCNM、および Cisco DCNM が管理するプラットフォームについてご利用いただけるマニュアルに関する情報を提供します。

ここでは、次の内容について説明します。

- 「Cisco DCNM のマニュアル」（P.x）
- 「Cisco Nexus 1000V シリーズ スイッチ マニュアル」（P.xi）
- 「Cisco Nexus 2000 シリーズ Fabric Extender のマニュアル」（P.xi）
- 「Cisco Nexus 4000 シリーズ スイッチ マニュアル」（P.xii）
- 「Cisco Nexus 5000 シリーズ スイッチ マニュアル」（P.xii）
- 「Cisco Nexus 7000 シリーズ スイッチ マニュアル」（P.xii）

Cisco DCNM のマニュアル

Cisco DCNM のマニュアルは、次の URL から入手可能です。

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、次の資料が含まれます。

リリース ノート

『*Cisco DCNM Release Notes, Release 5.x*』

コンフィギュレーション ガイド

『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』

『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』

『*Cisco DCNM System Management Configuration Guide, Release 5.x*』

『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』

『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』

『*Cisco DCNM Security Configuration Guide, Release 5.x*』

『*Cisco DCNM Unicast Routing Configuration Guide, Release 5.x*』

『*Cisco DCNM Getting Started with Virtual Device Contexts, Release 5.x*』

『*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*』
『*Cisco DCNM FabricPath Configuration Guide, Release 5.x*』
『*Cisco DCNM Web Services API Guide, Release 5.x*』

Cisco Nexus 1000V シリーズ スイッチ マニュアル

Cisco Nexus 1000V シリーズ スイッチ のマニュアルは、次の URL から入手可能です。
http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
Cisco Nexus 1000V シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(2)*』

コンフィギュレーション ガイド

『*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*』
『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(2)*』

Cisco Nexus 2000 シリーズ Fabric Extender のマニュアル

Cisco Nexus 2000 シリーズ Fabric Extender のマニュアルは、次の URL から入手可能です。
http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html
Cisco Nexus 2000 シリーズ Fabric Extender のマニュアル セットには、次の資料が含まれます。

リリース ノート

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

コンフィギュレーション ガイド

『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

Cisco Nexus 4000 シリーズ スイッチ マニュアル

Cisco Nexus 4000 シリーズ スイッチ のマニュアルは、次の URL から入手可能です。

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 4000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes, Release 4.1(2)E1(1b)*』

コンフィギュレーション ガイド

『*Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*』

Cisco Nexus 5000 シリーズ スイッチ マニュアル

Cisco Nexus 5000 シリーズ スイッチ のマニュアルは、次の URL から入手可能です。

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

Cisco Nexus 5000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Releases 4.1(3)N1(1), 4.1(3)N1(1a), 4.1(3)N2(1), and 4.1(3)N2(1a)*』

コンフィギュレーション ガイド

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

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

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

Cisco Nexus 7000 シリーズ スイッチ マニュアル

Cisco Nexus 7000 シリーズ スイッチ のマニュアルは、次の URL から入手可能です。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 7000 シリーズ スイッチのマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

コンフィギュレーション ガイド

『*Quick Start Guide: Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』

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。

CHAPTER 1

概要

Cisco Data Center Network Manager（DCNM）は、IP アドレッシング、オブジェクト トラッキング、および Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）をサポートします。

この章では、次の内容について説明します。

- 「IPv4 と IPv6」（P.1-1）
- 「ファーストホップ冗長プロトコル」（P.1-1）
- 「オブジェクト トラッキング」（P.1-1）

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。

ファーストホップ冗長プロトコル

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; ゲートウェイ ロード バランシング プロトコル）の詳細については、第 4 章「GLBP の設定」を参照してください。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 5 章「HSRP 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 6 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、Cisco Data Center Network Manager（DCNM）で IPv4（インターネット プロトコル バージョン 4）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。

- 「IPv4 について」（P.2-1）
- 「IPv4 のライセンス要件」（P.2-2）
- 「プラットフォーム サポート」（P.2-3）
- 「IPv4 の設定」（P.2-3）
- 「IP のフィールドに関する説明」（P.2-4）
- 「その他の関連資料」（P.2-5）
- 「IP 機能の履歴」（P.2-5）

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、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 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、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」（P.2-2）

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、同時に複数のアクティブなインターフェイス上に表示できません。

（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。

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 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ていない機能はすべて Cisco DCNM にバンドルされており、追加費用は一切発生しません。Cisco DCNM のライセンス スキームの詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
Cisco 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。使用しているプラットフォームでの Cisco NX-OS ライセンス スキームの詳細については、プラットフォームのライセンスに関するガイドを参照してください。

プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。ただし、実装方法は異なる場合があります。注意事項および制約事項、システムのデフォルト、設定の制限などのプラットフォーム固有の情報については、該当するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 1000V シリーズ スイッチ（mgmt0 ポートのみ）	Cisco Nexus 1000V シリーズ スイッチ マニュアル
Cisco Nexus 4000 シリーズ スイッチ（mgmt0 ポートのみ）	Cisco Nexus 4000 シリーズ スイッチ マニュアル
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000 シリーズ スイッチ マニュアル

IPv4 の設定

インターフェイス機能を選択して、Layer 3 インターフェイスの IP アドレッシングを設定できます。

Data Center Network Manager 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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.2-3）
- 「複数の IP アドレスの設定」（P.2-4）

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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、スロットの一覧を表示するデバイスをダブルクリックします。

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

ステップ 4　ルーティング インターフェイスとして設定するインターフェイスをクリックします。

[Summary] ペインで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 によってすべてのレイヤ 2 設定が削除されます。

ステップ 8　（任意）[IPv4 Address Settings] の [Primary] フィールドにこのルーティング インターフェイスの IPv4 アドレスを設定します。

ステップ 9　（任意）[Net mask] フィールドに、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。

ステップ 10　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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だけ追加できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、スロットの一覧を表示するデバイスをダブルクリックします。

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

ステップ 4　ルーティング インターフェイスとして設定するインターフェイスをクリックします。

[Summary] ペインで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] 領域で、[Add Secondary IP] 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　[Secondary] 領域の [IP address] フィールドに、IPv4 アドレスを入力します。

ステップ 9　[Net mask] フィールドに、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。

ステップ 10　（任意）[IPv4 Address settings] セクションの [Helper] 領域で、[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] 領域の [IP address] 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、変更内容をデバイスに適用します。

IP のフィールドに関する説明

IP アドレスのフィールドの詳細については、『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』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.2-5）
- 「標準規格」（P.2-5）

関連資料

関連項目	マニュアル名
IP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』

標準規格

標準規格	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 2-1　IP 機能の履歴

機能名	リリース	機能情報
IP	4.0(1)	この機能が導入されました。

CHAPTER 3

IPv6 の設定

この章では、Cisco Data Center Network Manager（DCNM）で IPv6（インターネット プロトコル バージョン 6）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。

- 「IPv6 について」（P.3-1）
- 「IPv6 のライセンス要件」（P.3-18）
- 「プラットフォーム サポート」（P.3-18）
- 「IPv6 の設定」（P.3-18）
- 「その他の関連資料」（P.3-20）
- 「IPv6 機能の履歴」（P.3-20）

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 フォーマット」（P.3-2）
- 「IPv6 ユニキャスト アドレス」（P.3-3）
- 「IPv6 エニーキャスト アドレス」（P.3-7）
- 「IPv6 マルチキャスト アドレス」（P.3-7）
- 「IPv4 パケット ヘッダー」（P.3-9）

- 「簡易 IPv6 パケット ヘッダー」（P.3-9）
- 「IPv6 の DNS」（P.3-12）
- 「IPv6 のパス MTU 探索」（P.3-12）
- 「CDP IPv6 アドレスのサポート」（P.3-13）
- 「IPv6 の ICMP」（P.3-13）
- 「IPv6 ネイバー探索」（P.3-14）
- 「IPv6 ネイバー送信要求メッセージ」（P.3-14）
- 「IPv6 ルータ アドバタイズメント メッセージ」（P.3-15）
- 「IPv6 ネイバー リダイレクト メッセージ」（P.3-17）

IPv6 アドレス フォーマット

IPv6 アドレスは 128 ビットつまり 16 バイトです。このアドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 16 ビット 16 進数のブロック 8 つに分かれています。次に、IPv6 アドレスの例を 2 つ示します。

```
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。IPv6 アドレスの先頭、中間、または末尾で、この連続するゼロの代わりに 2 つのコロン（::）を使用できます。表 3-1 は、圧縮された IPv6 アドレス フォーマットの一覧です。

（注）　IPv6 アドレスでは、アドレス中で最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　圧縮された IPv6 アドレス フォーマット

IPv6 アドレス タイプ	元のフォーマット	圧縮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、送信元アドレスまたは宛先アドレスに IPv6 ループバック アドレスを持つ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。たとえば、2001:0DB8:8086:6502::/32 は IPv6 プレフィクスとして有効です。

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。

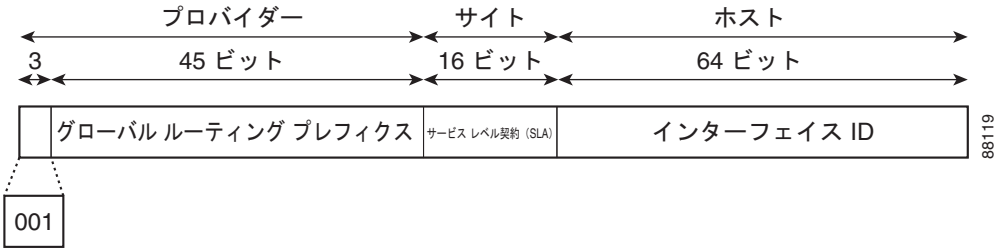
- 「集約可能グローバル アドレス」（P.3-3）
- 「リンクローカル アドレス」（P.3-5）
- 「IPv4 互換 IPv6 アドレス」（P.3-5）
- 「ユニーク ローカル アドレス」（P.3-6）
- 「サイトローカル アドレス」（P.3-7）

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。IPv6 グローバル ユニキャスト アドレスの割り当てには、バイナリ値 001（2000::/3）から始まるアドレスの範囲が使用されます。図 3-1 は、集約可能なグローバル アドレスの構造を示します。

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 を持つ組織では最大 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。ゼロはローカルに管理されている ID を表し、1 はグローバルに一意の IPv6 インターフェイス ID を表します。
- 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。

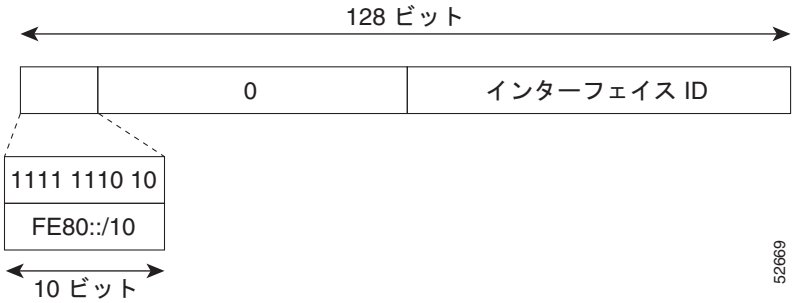
1. ルータに MAC アドレス（ルータ内の MAC アドレス プールの）が照会されます。
2. 使用可能な MAC アドレスがルータにない場合は、ルータのシリアル番号を使用して、リンクローカル アドレスが作成されます。
3. リンクローカル アドレスの作成にルータのシリアル番号を使用できない場合、ルータは MD5 ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

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、ネイバー探索プロトコルおよびステートレス自動コンフィギュレーション プロセスで使用されます。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 は、リンクローカル アドレスの構造を示します。

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。

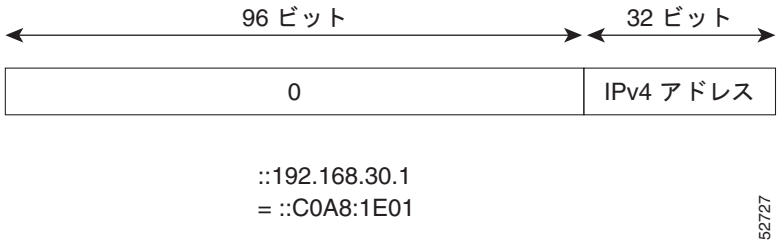
図 3-2　リンクローカル アドレス フォーマット



IPv4 互換 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、アドレスの下位 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、下位 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 は、IPv4 互換 IPv6 アドレスの構造と、許容されるアドレス フォーマットのいくつかを示します。

図 3-3　IPv4 互換 IPv6 アドレスのフォーマット



ユニーク ローカル アドレス

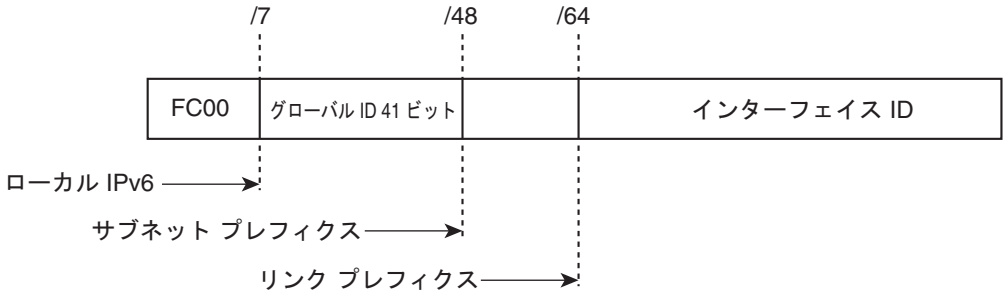
ユニーク ローカル アドレスは、グローバルに一意であり、ローカルでの通信のための IPv6 ユニキャスト アドレスです。グローバルなインターネット上でのルーティングには対応しておらず、サイトなどの限られたエリア内だけでルーティング可能です。限られた複数のサイト間もルーティングできる場合もあります。アプリケーションは、ユニーク ローカル アドレスをグローバルなスコープのアドレスとして扱う場合があります。

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 アドレスを識別するための 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の作成に使用される 41 ビット グローバル ID。
- サブネット ID : 16 ビット サブネット ID はサイト内のサブネットの ID。
- インターフェイス ID : 64 ビット IID

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。

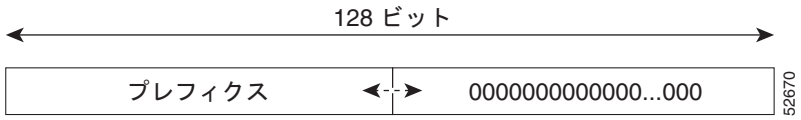
IPv6 エニーキャスト アドレス

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、ルータだけです。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。このアドレスには、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。

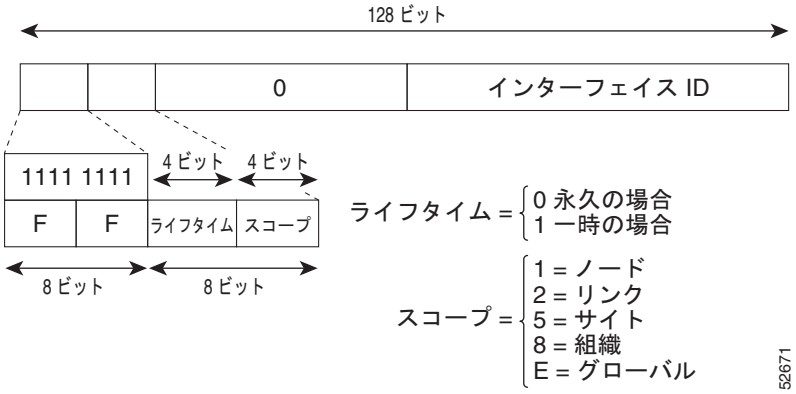
図 3-5　サブネット ルータ エニーキャスト アドレスのフォーマット



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るパケットは、このマルチキャスト アドレスで示されるすべてのインターフェイスに伝送されます。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。永久マルチキャスト アドレスはライフタイム パラメータが 0 に等しく、一時マルチキャスト アドレスのライフタイム パラメータは 1 に等しくなっています。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、プレフィクスが FF02::/16 のマルチキャスト アドレスは、リンク スコープが設定された永続的なマルチキャスト 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 フォーマット



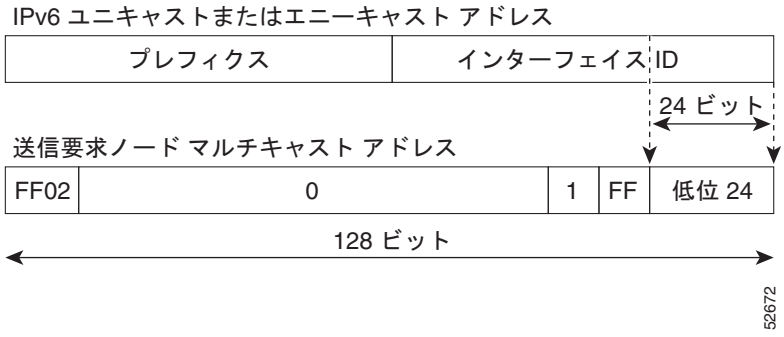
IPv6 ノード（ホストとルータ）は、（受信パケットの宛先となる）次のマルチキャスト グループに加入する必要があります。

- 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 アドレスの下位 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 アドレスのフォーマット

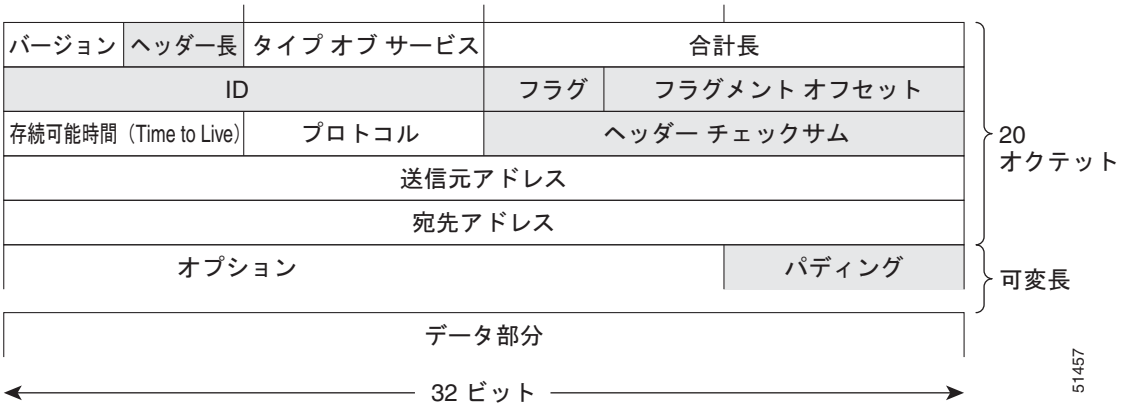


（注）　IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに、IPv6 マルチキャスト アドレスが使用されます。

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 個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 IPv6 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。

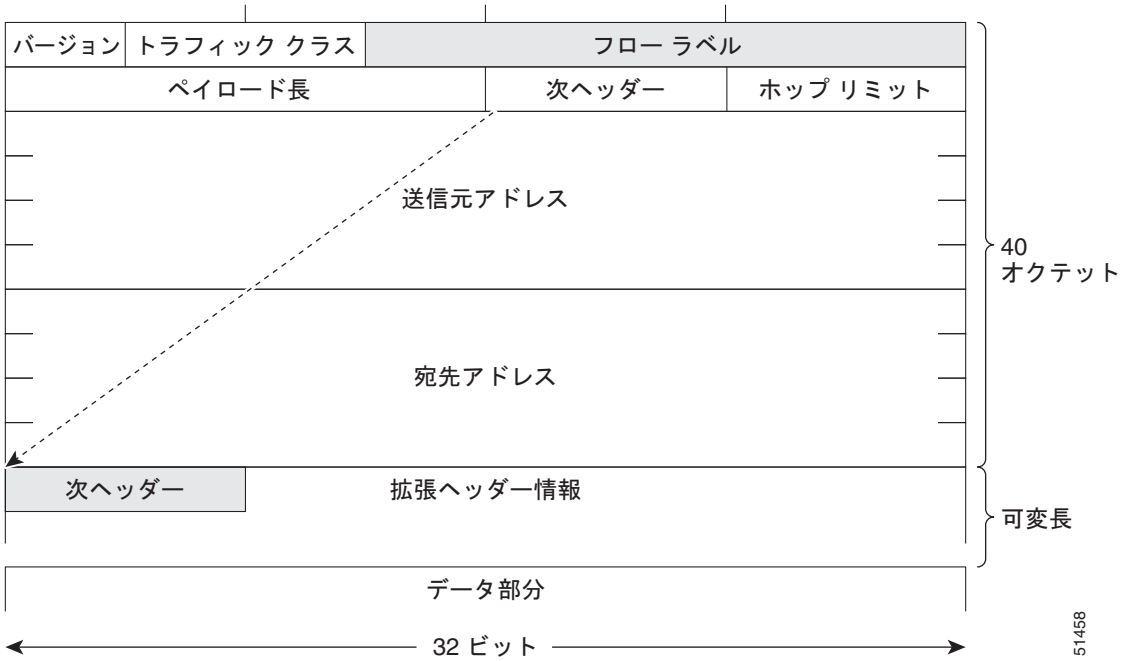
表 3-2　基本 IPv6 パケット ヘッダーのフィールド

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。

表 3-2　基本 IPv6 パケット ヘッダーのフィールド （続き）

フィールド	説明
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 ヘッダーのあとに続く情報のタイプが決まります。基本 IPv6 ヘッダーのあと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 は、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

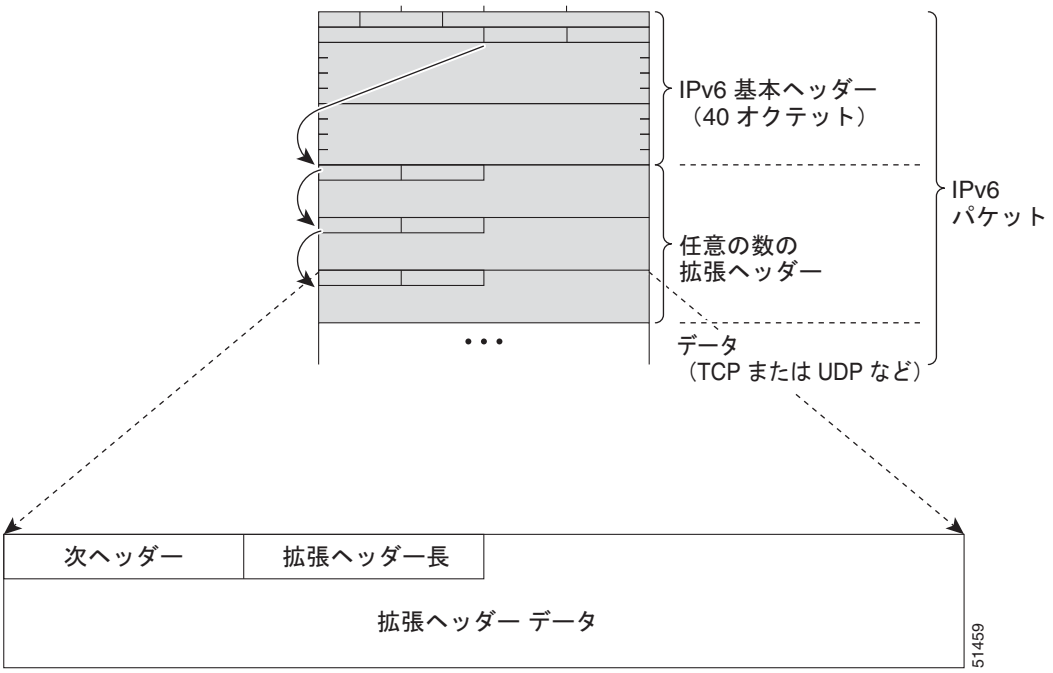


表 3-3 は、拡張ヘッダーのタイプとその次ヘッダー フィールドの値の一覧です。

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 ヘッダーのあと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）ヘッダーのあと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、最終の宛先だけで処理されます。
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。

表 3-3　IPv6 拡張ヘッダーのタイプ （続き）

ヘッダーのタイプ	次ヘッダーの値	説明
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） 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（表 3-4 を参照）。

（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。ICMP の Too Big メッセージの到着によってパス MTU が削減されると、Cisco NX-OS はその低い値を保持します。この接続では、スループットの計測のためにセグメント サイズが定期的に増加することはありません。

（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 値の使用を推奨します。

CDP IPv6 アドレスのサポート

ネイバー情報機能向けの Cisco Discovery Protocol（CDP; シスコ検出プロトコル）IPv6 アドレスの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

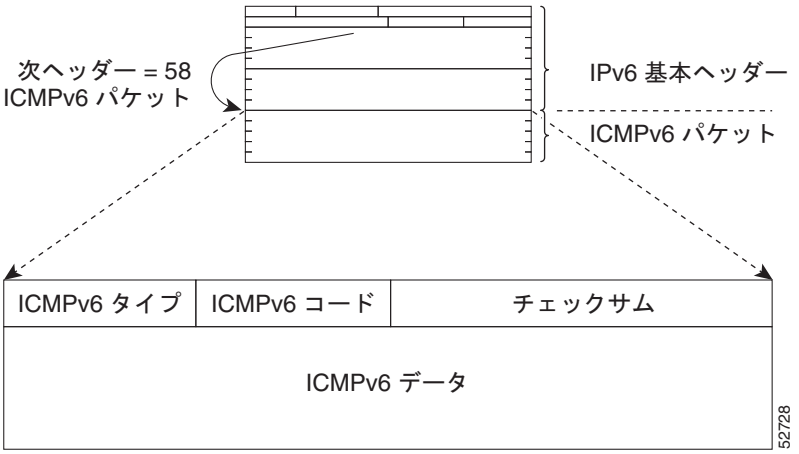
IPv6 で ICMP を使用して、ネットワークの状態に関する情報を提供できます。IPv6 で使用できるバージョンである ICMPv6 は、パケットが正しく処理されない場合にエラーを報告し、ネットワークの状態に関する情報メッセージを送信します。たとえば、パケットが大きすぎて別のネットワークに送信できないために、ルータがパケットを転送できない場合は、ルータにより、送信元のホストに ICMPv6 メッセージが送信されます。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索およびパス MTU 探索に使用されます。パス MTU 探索処理により、パケットが確実に、特定のルートでサポートさ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、すべての拡張ヘッダーのあとに続く、IPv6 パケット中の最後の情報部分です。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 は、IPv6 ICMP パケット ヘッダーの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



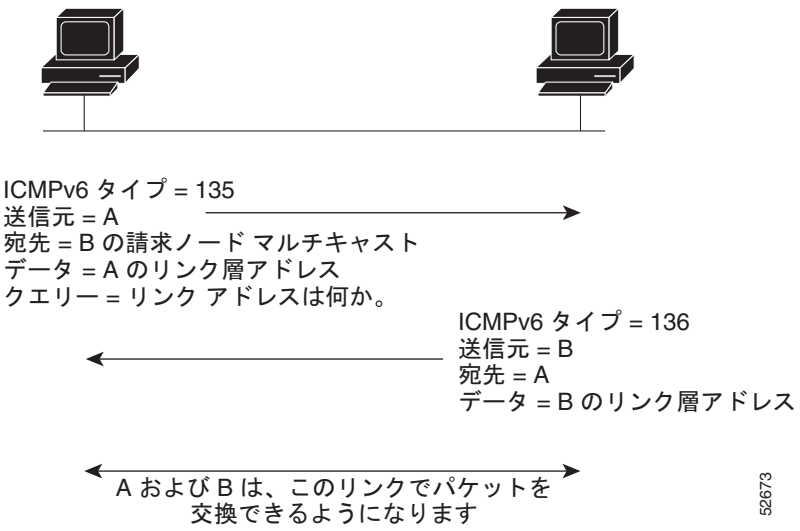
IPv6 ネイバー探索

IPv6 Neighbor Discovery Protocol（NDP; ネイバー探索プロトコル）を使用して、ネイバー ルータが到達可能かどうかを判定できます。IPv6 ノードは、ネイバー探索を使用して、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ネイバー ルータを見つけ、そのネイバー 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ネイバー 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 ネイバー探索：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。

送信元ノードと宛先ノードが通信できるのは、送信元ノードがネイバー アドバタイズメントを受信したあとです。

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。

ローカル リンク上のノードのリンクレイヤ アドレスに変更がある場合も、ネイバー アドバタイズメント メッセージが送信されます。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、ホストとネイバー 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 パケットだけが送信されるネイバーに対してだけ実行され、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、到達可能と見なされます。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だけ送信されます）。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だけ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見なされません。

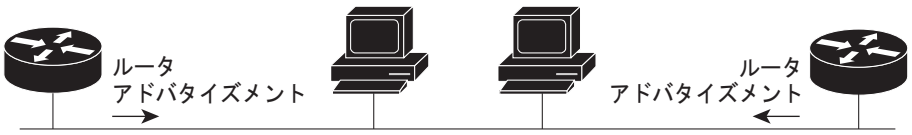
ネイバー送信要求メッセージは、ユニキャスト IPv6 アドレスをインターフェイスに割り当てる前にそのアドレスが一意であることを確認するために、ステートレス自動設定処理でも使用されます。新規のリンクローカル IPv6 アドレスに対しては、インターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（新規アドレスは、重複アドレス検出の実行中は一時的なアドレスのままです）。ノードは、未指定の送信元アドレスと一時的なリンクローカル アドレスがメッセージ本文に含まれるネイバー送信要求メッセージを送信します。そのアドレスがすでに他のノードによって使用されている場合、ノードは、一時的リンクローカル 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 ネイバー探索：RA メッセージ



ルータ アドバタイズメント パケット定義：
ICMPv6 タイプ = 134
送信元 = ルータ リンクローカル アドレス
宛先 = すべてのノードのマルチキャスト アドレス
データ = オプション、プレフィクス、有効期間、自動設定フラグ
52674

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）を示すフラグのセット
- 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。ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐ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。

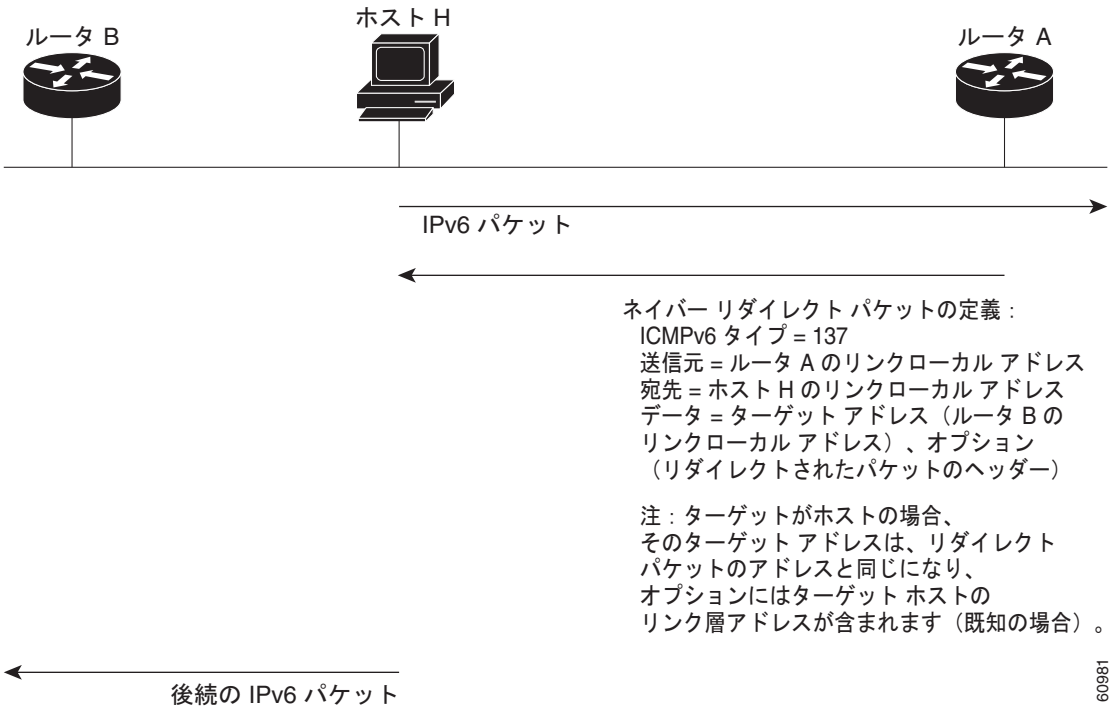
- RA メッセージが定期的に送信される時間の間隔
- デフォルト ルータ（リンクのすべてのノードが使用する）としてのルータの実用性を示すルータのライフタイム値
- リンクで使用されているネットワーク プレフィクス
- （リンクで）ネイバー送信要求メッセージが再送される時間の間隔
- ネイバーが到達可能である（リンク上のすべてのノードが使用できる）とノードが判断するまでの時間

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 ネイバー探索：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、確実にネイバー 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、その各ネイバー 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、ネイバー 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。
- パケットがその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。

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
Cisco 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ていない機能はすべて Cisco DCNM にバンドルされており、追加費用は一切発生しません。Cisco DCNM のライセンス スキームの詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
Cisco 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。使用しているプラットフォームでの Cisco NX-OS ライセンス スキームの詳細については、プラットフォームのライセンスに関するガイドを参照してください。

プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。ただし、実装方法は異なる場合があります。注意事項および制約事項、システムのデフォルト、設定の制限などのプラットフォーム固有の情報については、該当するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 1000V シリーズ スイッチ（mgmt0 ポートのみ）	Cisco Nexus 1000V シリーズ スイッチ マニュアル
Cisco Nexus 4000 シリーズ スイッチ（mgmt0 ポートのみ）	Cisco Nexus 4000 シリーズ スイッチ マニュアル
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000 シリーズ スイッチ マニュアル

IPv6 の設定

インターフェイス機能を選択して、Layer 3 インターフェイスの IPv6 アドレスを設定できます。

Data Center Network Manager 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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.3-18）
- 「IPv6 セカンダリ アドレスの設定」（P.3-19）

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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、スロットの一覧を表示するデバイスをダブルクリックします。

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

ステップ 4　ルーティング インターフェイスとして設定するインターフェイスをクリックします。

[Summary] ペインで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 によってすべてのレイヤ 2 設定が削除されます。

ステップ 8　[IPv6 Address Settings] 領域の [Primary/prefix-length] フィールドに、このルーティング インターフェイスの IPv6 アドレスおよび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] チェックボックスをオンにします。

ステップ 10　（任意）[Link local] フィールドに、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）このルーティング 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] チェックボックスをオンにします。

ステップ 12　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

IPv6 セカンダリ アドレスの設定

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

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、スロットの一覧を表示するデバイスをダブルクリックします。

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

ステップ 4　ルーティング インターフェイスとして設定するインターフェイスをクリックします。

[Summary] ペインで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] セクションを展開します。

ポート モードが表示されます。

ステップ 7　[IPv6 Address settings] セクションの [Secondary] 領域で、[Add IPv6 Address] を右クリックして選択し、セカンダリ IPv6 アドレスを追加します。

ステップ 8　[IP Address/Prefix-length] フィールドに、このセカンダリ IPv6 アドレスの IPv6 アドレスおよび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] チェックボックスをオンにします。

ステップ 10　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

IPv6 のフィールドに関する説明

IPv6 アドレスのフィールドの詳細については、『*Cisco DCNM Interfaces Configuration Guide, Release 5.x*』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.3-20）
- 「標準規格」（P.3-20）

関連資料

関連項目	マニュアル名
IPv6 CLI コマンド	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』

標準規格

標準規格	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。	—

IPv6 機能の履歴

表 3-5 は、この機能のリリースの履歴です。

表 3-5　IPv6 機能の履歴

機能名	リリース	機能情報
IPv6	4.0(1)	この機能が導入されました。

CHAPTER 4

GLBP の設定

この章では、Cisco Data Center Network Manager（DCNM）で Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）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。

- 「GLBP の概要」（P.4-1）
- 「GLBP のライセンス要件」（P.4-6）
- 「GLBP の前提条件」（P.4-6）
- 「デフォルト設定」（P.4-7）
- 「プラットフォーム サポート」（P.4-7）
- 「GLBP の設定」（P.4-7）
- 「GLBP のフィールドに関する説明」（P.4-12）
- 「その他の関連資料」（P.4-15）
- 「GLBP 機能の履歴」（P.4-16）

GLBP の概要

GLBP は、冗長ゲートウェイ間でプロトコルおよび Media Access Control（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。また、GLBP を使用すると、レイヤ 3 ルータ グループで、LAN 上のデフォルト ゲートウェイの負荷を分担できます。GLBP ルータは、グループ内の別のルータで障害が発生したとき、そのルータのフォワーディング機能を自動的に引き継ぎます。

ここでは、次の内容について説明します。

- 「GLBP の概要」（P.4-2）
- 「GLBP アクティブ仮想ゲートウェイ」（P.4-2）
- 「GLBP 仮想 MAC アドレス割り当て」（P.4-2）
- 「GLBP による仮想ゲートウェイの冗長性」（P.4-3）
- 「GLBP による仮想フォワーダの冗長性」（P.4-3）
- 「GLBP 認証」（P.4-4）
- 「GLBP ロード バランシングおよびトラッキング」（P.4-5）
- 「ハイ アベイラビリティ」（P.4-6）

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 つの仮想ファーストホップ 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、Hot Standby Redundancy Protocol（HSRP; ホットスタンバイ冗長プロトコル）および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）と同様の機能を実行します。HSRP および VRRP は、仮想 IP アドレスを指定して設定された仮想グループに、複数のルータを参加させます。これらのプロトコルでは、グループの仮想 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、メンバーを 1 つ選択します。グループ内の残りのルータは、アクティブなルータで障害が発生するまで冗長なルータとなります。

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 つの仮想 IP アドレスと複数の仮想 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 では、グループ内のすべてのルータ間でフォワーディングの負荷を分担します。アイドル状態のルータが他に存在してるにもかかわらず 1 台のルータにすべてのフォワーディング負荷を処理させることはありません。各ホストに同じ仮想 IP アドレスを設定し、仮想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 メンバーは定期的な hello パケットによって、相互に通信します。

GLBP アクティブ仮想ゲートウェイ

GLBP はゲートウェイにプライオリティを設定して、Active Virtual Gateway（*「AVG」*; アクティブ仮想ゲートウェイ）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ーに仮想 MAC アドレスを割り当てます。各メンバーはそれぞれ割り当てられた仮想 MAC アドレスに対応する Active Virtual Forwarder（*「AVF」*; アクティブ仮想フォワーダ）となり、割り当てられた仮想 MAC アドレスにパケットを転送します。

AVG は、仮想 IP アドレスに対する Address Resolution Protocol（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 要求に異なる仮想 MAC アドレスで応答したときに行われます。

（注）　ルーテッド ポートで受信した GLBP 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 GLBP ルータであるのか冗長 GLBP 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 GLBP 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。

GLBP 仮想 MAC アドレス割り当て

AVG はグループの各メンバーに仮想 MAC アドレスを割り当てます。グループ メンバーは hello メッセージを通じて AVG を検出したあとで、仮想 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 によって仮想 MAC アドレスが割り当てられたゲートウェイは、プライマリ仮想フォワーダになります。hello メッセージから仮想 MAC アドレスを学習する、GLBP グループの他のメンバーは、セカンダリ仮想フォワーダです。

GLBP による仮想ゲートウェイの冗長性

GLBP は、仮想ゲートウェイの冗長性を実現します。グループ メンバーは、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仮想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、スタンバイ仮想ゲートウェイが仮想 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仮想ゲートウェイを選択します。

GLBP による仮想フォワーダの冗長性

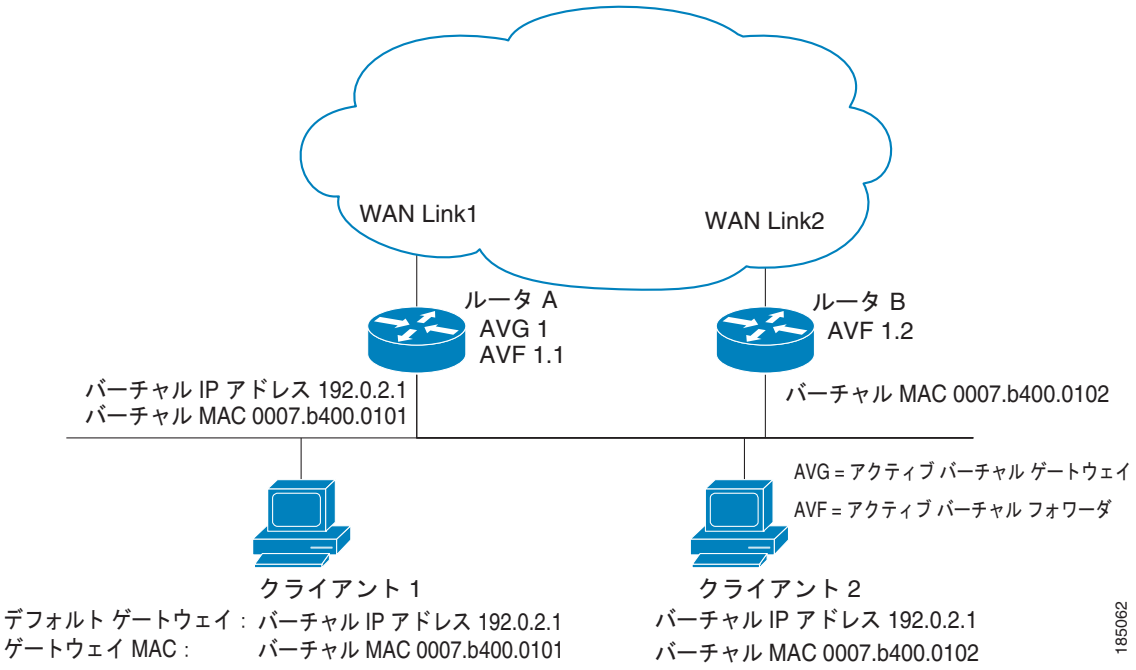
GLBP は、仮想フォワーダの冗長性を実現します。仮想フォワーダの冗長性は、アクティブ仮想フォワーダ（AVF）の点で、仮想ゲートウェイの冗長性と類似しています。AVF で障害が発生すると、リッスン ステートのセカンダリ仮想フォワーダが仮想 MAC アドレスに対応する役割を引き受けます。このセカンダリ仮想フォワーダは、別の仮想 MAC アドレスのプライマリ仮想フォワーダでもあります。GLBP は次の 2 種類のタイマーを使用して、障害 AVF の古い仮想 MAC アドレスからホストを移行させます。

- リダイレクト タイマー：AVG が古い仮想 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 応答での古い仮想 MAC アドレスの使用を中止しますが、セカンダリ仮想フォワーダは引き続き、古い仮想 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：仮想 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仮想 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。時間切れになった仮想 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、仮想 IP アドレス 192.0.2.1 を担当します。ルータ A は、仮想 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 グループのメンバーであり、仮想 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、仮想 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 の仮想 MAC アドレス宛てのパケットの転送を引き受け、自分の仮想 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 メンバー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 メンバーが秘密キーを使用して、発信パケットに組み込まれるキー付き MD5 ハッシュを生成します。受信側では、着信パケットのキー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 ハッシュのキーは、キー 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指定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の間で異なっている。
- 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の間で異なっている。

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 応答で送信された仮想 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仮想 MAC アドレスを決定します。このアルゴリズムでは、仮想フォワーダの数が変わらないかぎり、ホストに同じ仮想 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 メンバー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、セカンダリ仮想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 メンバーが 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 メンバーを使用できるか、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、メンバーは AVF ではなくなり、セカンダリ仮想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、メンバーは AVF としての役割を再び得ます。

図 4-2 に、GLBP トラン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

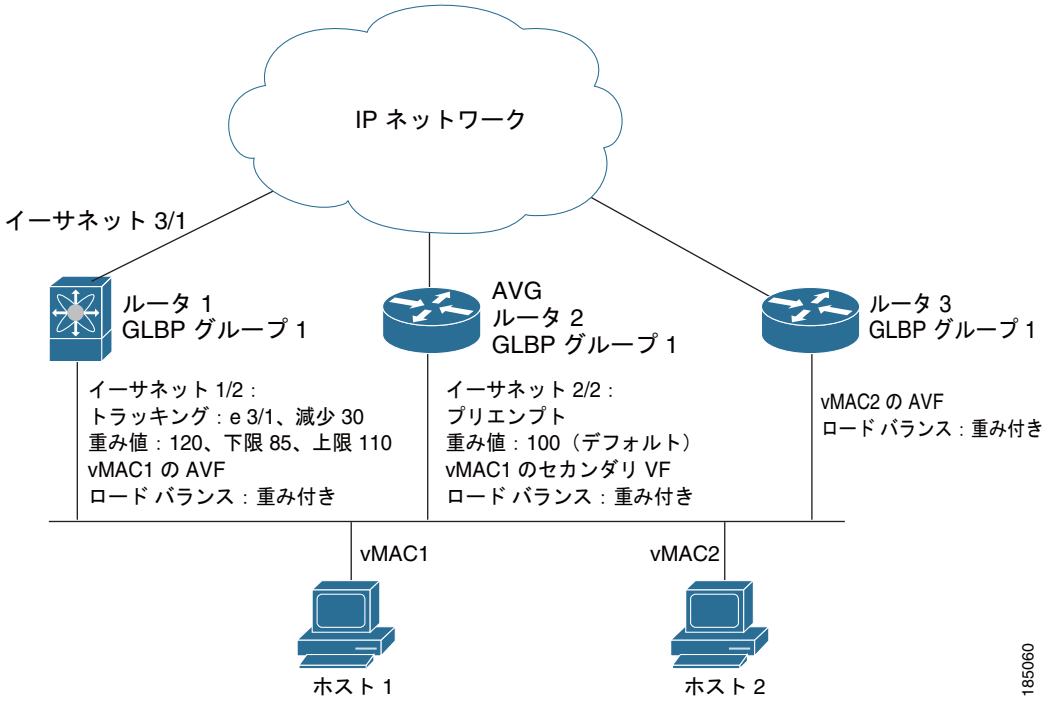


図 4-2 では、ルータ 1 上のインターフェイス Ethernet 1/2 がホスト 1 のゲートウェイ（仮想 MAC アドレス vMAC に対応する AVF）です。一方、ルータ 2 上の Ethernet 2/2 は、ホスト 1 のセカンダリ仮想フォワーダとして動作します。Ethernet 1/2 は、ルータ 1 のネットワーク接続である Ethernet 3/1 を追跡します。Ethernet 3/1 がダウンすると、Ethernet 1/2 の重み値が 90 に下がります。ルータ 2 上の Ethernet 2/2 が Ethernet 1/2 に代わり、AVF として引き継ぎます。Ethernet 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。

重み付けおよびトラッキングの詳細については、「GLBP 重み付けおよびトラッキングの設定」（P.4-10）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。

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
Cisco DCNM	GLBP には LAN Enterprise ライセンスが必要です。Cisco DCNM 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 DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
Cisco 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。使用しているプラットフォームでの Cisco NX-OS ライセンス スキームの詳細については、プラットフォームのライセンスに関するガイドを参照してください。

GLBP の前提条件

Cisco DCNM の機能を使用するための前提条件は、次のとおりです。機能固有の前提条件については、プラットフォームのマニュアルを参照してください。

GLBP の前提条件は、次のとおりです。

- GLBP 機能のシステム メッセージ ロギング レベルは、Cisco DCNM 要件を満たすか、それ以上でなければなりません。デバイス検出処理で、Cisco DCNM は不適切なロギング レベルを検出し、レベルを高くして最小限の要件を満たすようにします。Cisco NX-OS Release 4.0 を実行する Cisco Nexus 7000 シリーズ スイッチは例外です。Cisco NX-OS Release 4.0 では、デバイス検出を行う前に、コマンドライン インターフェイスを使用して、ロギング レベルが Cisco DCNM 要件を満たすか、それ以上になるように設定されます。詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
- 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 DCNM Interfaces Configuration Guide, Release 5.x*』を参照）。

デフォルト設定

表 4-1 に、GLBP パラメータのデフォルト設定を示します。

表 4-1　デフォルトの GLBP パラメータ

パラメータ	デフォルト
認証	認証なし
フォワーダ プリエンプト遅延	30 秒
フォワーダ タイムアウト	14400 秒
hello タイマー	3 秒
ホールド タイマー	10 秒
GLBP 機能	ディセーブル
ロード バランシング	ラウンドロビン
プリエンプト	ディセーブル
プライオリティ	100
リダイレクト タイマー	600 秒
重み付け	100

プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。注意事項および制約事項、システムのデフォルト、設定の制限などのプラットフォーム固有の情報については、該当するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000 シリーズ スイッチ マニュアル

GLBP の設定

ルーティング機能を選択して、GLBP にアクセスできます。

Data Center Network Manager 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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 グループの作成」（P.4-8）
- 「GLBP 認証の設定」（P.4-8）
- 「GLBP ロード バランシングの設定」（P.4-9）
- 「GLBP 重み付けおよびトラッキングの設定」（P.4-10）
- 「ゲートウェイ プリエンプトの設定」（P.4-10）
- 「GLBP のカスタマイズ」（P.4-11）
- 「GLBP グループのイネーブル化」（P.4-12）

GLBP グループの作成

インターフェイス上で GLBP グループを作成できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定する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 [Actions] > [New GroupSetting] を選択します。

[Summary] ペインで新しい GLBP の行が強調表示され、[Details] ペインの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 グループを設定する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 ID] フィールドに、このグループのグループ番号を入力します。

指定できる範囲は 0 ～ 1023 です。

デバイスに新しいグループが作成されます。[Summary] ペインでは新しい GLBP グループが強調表示され、[Details] ペインでは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] タブで、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 8　（任意）[Priority] フィールドに、この GLBP グループ メンバーのプライオリティを入力します。

ステップ 9　（任意）[Group Name] フィールドに、この GLBP グループ メンバーの名前を入力します。

ステップ 10　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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, Release 5.x*』を参照）。

操作の前に

（注）　GLBP グループのすべてのメンバーに同じ認証およびキーを設定する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定するデバイスをクリックします。

ステップ 3　認証を設定する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、[Authentication, Gateway Preemption] セクションを展開します。

[Details] ペインに認証情報が表示されます。

ステップ 6　[Authentication] 領域の [Method] ドロップダウン リストから、認証方式を選択します。

ステップ 7　（任意）テキスト認証の場合、パスワードのフィールドにパスワード文字列を入力します。

ステップ 8　（任意）MD5 認証の場合、[Key] または [Key Chain] チェックボックスをオンにします。

ステップ 9　（任意）[Key] オプションについては、キーのフィールドにキー ストリングを入力し、暗号化されたキー ストリングの場合は [encrypted] チェックボックスをオンにします。

ステップ 10　（任意）[Key Chain] オプションについては、キーチェーンのドロップダウン リストから、使用する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、変更内容をデバイスに適用します。

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）。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定する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する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、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 6　[Method] ドロップダウン リストから、ロード バランシング方式を選択します。

ステップ 7　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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仮想 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 重み付けの変更に使用するオブジェクト トラッキング エントリを設定していることを確認してください（「オブジェクト トラッキングの設定」（P.6-4）を参照）。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定する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する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] セクションを展開します。

[Details] ペインに重み付けとオブジェクト トラッキング情報が表示されます。

ステップ 6　[Weight] 領域に、上限しきい値、下限のしきい値、および上限しきい値の重み値を入力します。

ステップ 7　[GLBP Tracking] 領域で右クリックし、ポップアップ メニューから [Add TrackObject] を選択します。

ステップ 8　[Object ID] ドロップダウン リストから、GLBP 重み値を変更するために使用するオブジェクト ID を選択します。

ステップ 9　[Weight Decrement] フィールドに、トラッキング対象オブジェクトがダウン状態となった場合に GLBP 重み付けを減少させる値を入力します。

ステップ 10　[Group Details] タブで、[Virtual Forwarder Setting] セクションを展開します。

[Details] ペインに仮想フォワーダ情報が表示されます。

ステップ 11　（任意）[Virtual Forwarder Preemption] チェックボックスをオンにします。

ステップ 12　（任意）[Preemption Delay] フィールドに、遅延値を秒単位で入力します。

ステップ 13　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

ゲートウェイ プリエンプトの設定

ゲートウェイ プリエンプトを設定できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定するデバイスをクリックします。

ステップ 3　認証を設定する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、[Authentication, Gateway Preemption] セクションを展開します。

[Details] ペインにプリエンプト情報が表示されます。

ステップ 6　[Authentication, Gateway Preemption] セクションで、[Gateway Preemption] チェックボックスをオンにします。

ステップ 7　[Minimum Delay] フィールドに、プリエンプトを発生させる前に待機する最小遅延時間を入力します。

デフォルトは 3600 秒です。

ステップ 8　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

GLBP のカスタマイズ

GLBP 動作のカスタマイズは任意です。仮想 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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定するデバイスをクリックします。

ステップ 3　タイマーを設定する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、[Timers] セクションを展開します。

[Details] ペインにタイマー情報が表示されます。

ステップ 6　[Configured Timers] 領域の [Hello Time (msec)] フィールドに、hello タイムを入力します。

ステップ 7　[Configured Timers] 領域の [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] 領域の [Redirect Time (sec)] フィールドに、リダイレクト タイムを入力します。

ステップ 9　[Configured Timers] 領域の [Forwarder Time-out (sec)] 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、変更内容をデバイスに適用します。

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、仮想 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 メンバーは、他の GLBP メンバーから、必要なその他すべてのパラメータを学習できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [GLBP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、GLBP を設定するデバイスをクリックします。

ステップ 3　タイマーを設定する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、[Group Details] セクションを展開します。

[Details] ペインに一般情報が表示されます。

ステップ 6　（任意）仮想 IP アドレスを手動で設定するには、[Virtual IP address] フィールドに IP アドレスを入力します。

ステップ 7　（任意）仮想 IP アドレスを学習させるには、[Learn Virtual IP from Members Of Group] チェックボックスをオンにします。

ステップ 8　（任意）[Virtual Secondary IP Address] フィールドに、セカンダリ IP アドレスを入力します。

ステップ 9　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

GLBP のフィールドに関する説明

ここでは、GLBP の次のフィールドについて説明します。

- 「[GLBP] : [Group Details] タブ : [Group Details] セクション」（P.4-13）
- 「[GLBP] : [Group Details] タブ : [Authentication, Gateway Preemption] セクション」（P.4-13）
- 「[GLBP] : [Group Details] タブ : [Weighting and Object Tracking Sectio] セクション」（P.4-14）
- 「[GLBP] : [Group Details] タブ : [Virtual Forwarder Setting] セクション」（P.4-14）
- 「[GLBP] : [Group Details] タブ : [Timers] セクション」（P.4-14）
- 「[GLBP] : [Virtual Gateways and Forwarders] タブ : [Forwarder Details] セクション」（P.4-15）
- 「[GLBP] : [Virtual Gateways and Forwarders] タブ : [GLBP Group Member Details] セクション」（P.4-15）

[GLBP]：[Group Details] タブ：[Group Details] セクション

表 4-2　[GLBP]：[Group Details]：[Group Details]

フィールド	説明
Gateway	
Group ID	*表示専用。*GLBP グループのグループ番号。
Priority	AVG の選択に使用するグループ メンバーのプライオリティ。
Group Name	GLBP グループの名前。
Method	この GLBP グループのロード バランシングの方式。
Gateway State	*表示専用。*グループ メンバーの管理状態。
State Change Count	*表示専用。*GLBP ゲートウェイの状態が変更された回数。
Last State Change	*表示専用。*GLBP ゲートウェイの状態が最後に変更されたとき。
Active Gateway	
IP Address	アクティブ ゲートウェイのアドレス。
Priority	アクティブ ゲートウェイのプライオリティ。
Standby Gateway	
IP Address	スタンバイ ゲートウェイのアドレス。
Priority	スタンバイ ゲートウェイのプライオリティ。
IP Address Settings	
Learn Virtual IP from Members of Group	学習された、グループの IP アドレス。
Virtual IP Address	グループの仮想 IP アドレス。
Secondary IP Address	グループのセカンダリ IP アドレス。

[GLBP]：[Group Details] タブ：[Authentication, Gateway Preemption] セクション

表 4-3　[GLBP]：[Group Details]：[Authentication, Gateway Preemption]

フィールド	説明
Authentication	
Method	認証方法。
Password	テキスト認証のパスワード。
Key	MD5 認証のキー ストリング。
Encrypted	キー ストリングは MD5 認証用に暗号化されます。
Key Chain	MD5 認証のキーチェーン名。
Gateway Preemption	
Gateway Preemption	ゲートウェイ プリエンプト。
Minimum Delay	プリエンプトを発生させる前に待機する最小遅延時間。

[GLBP]：[Group Details] タブ：[Weighting and Object Tracking Sectio] セクション

表 4-4　[GLBP]：[Group Details]：[Weighting and Object Tracking]

フィールド	説明
Weight	
Maximum	最大重み値。
Lower Threshold	重み値の下限しきい値。
Upper Threshold	重み値の上限しきい値。
GLBP Tracking	
Object ID	トラッキング対象オブジェクトの ID。
Tracked Object	トラッキング対象オブジェクトの詳細。
Weight Decrement	トラッキング対象オブジェクトがダウン状態となった場合に GLBP 重み付けを減少させる値。

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

表 4-5　[GLBP]：[Group Details]：[Virtual Forwarder Setting]

フィールド	説明
Forwarder ID	仮想フォワーダの ID。
Virtual MAC Address	GLBP グループの仮想 MAC アドレス。
Virtual Forwarder Preemption	GLBP グループの現在の AVF が重みの下限しきい値を下回った場合に、GLBP グループの AVF を引き継ぐデバイス。
Preemption Delay	仮想フォワーダ プリエンプトの発生を遅延させる時間。

[GLBP]：[Group Details] タブ：[Timers] セクション

表 4-6　[GLBP]：[Group Details]：[Timers]

フィールド	説明
Active Timer Values	
Hello Time	*表示専用。*GLBP グループの hello タイム。
Hold Time	*表示専用。*GLBP グループのホールド タイム。
Virtual Forwarder Redirect Time	*表示専用。*アクティブ仮想ゲートウェイがアクティブ仮想フォワーダにクライアントのリダイレクトを続ける時間の長さ（秒数）。
Secondary Forwarder Hold Time	*表示専用。*セカンダリ仮想フォワーダが無効になるまでの時間の長さ（秒数）。

表 4-6　[GLBP] : [Group Details] : [Timers] （続き）

フィールド	説明
Configured Timers	
Hello Time	GLBP グループの hello タイム。
Hold Time	GLBP グループのホールド タイム。
Virtual Forwarder Redirect Time	アクティブ仮想ゲートウェイがアクティブ仮想フォワーダにクライアントのリダイレクトを続ける時間の長さ（秒数）。
Secondary Forwarder Hold Time	セカンダリ仮想フォワーダが無効になるまでの時間の長さ（秒数）。

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

表 4-7　[GLBP] : [Virtual Gateways and Forwarders] : [Forwarder Details]

フィールド	説明
Forwarder ID	*表示専用。*仮想フォワーダの ID。
MAC Address	*表示専用。*GLBP グループの MAC アドレス。
Virtual MAC Address	*表示専用。*GLBP グループの仮想 MAC アドレス。
Redirection	*表示専用。*リダイレクションの状態。
Weighting	*表示専用。*このフォワーダの重み値。
Gateway State	*表示専用。*グループ メンバーの管理状態。
State Change Count	*表示専用。*GLBP ゲートウェイの状態が変更された回数。
Last State Change	*表示専用。*GLBP ゲートウェイの状態が最後に変更されたとき。

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

表 4-8　[GLBP] : [Virtual Gateways and Forwarders] : [GLBP Group Member Details]

フィールド	説明
IP Address	グループ メンバーの IP アドレス。
MAC Address	グループ メンバーの MAC アドレス。

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.4-16）
- 「標準規格」（P.4-16）

関連資料

関連項目	マニュアル名
HSRP の設定	第 5 章「HSRP の設定」
GLBP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』
ハイ アベイラビリティの設定	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』

標準規格

標準規格	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。	—

GLBP 機能の履歴

表 4-9 は、この機能のリリースの履歴です。

表 4-9　GLBP 機能の履歴

機能名	リリース	機能情報
GLBP	4.0(1)	この機能が導入されました。

CHAPTER 5

HSRP の設定

この章では、Data Center Network Manager（DCNM）で Hot Standby Router Protocol（*HSRP*; ホット スタンバイ ルータ プロトコル）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」（P.5-1）
- 「HSRP のライセンス要件」（P.5-8）
- 「HSRPP の前提条件」（P.5-8）
- 「デフォルト設定」（P.5-9）
- 「プラットフォーム サポート」（P.5-9）
- 「HSRP の設定」（P.5-9）
- 「HSRP のフィールドに関する説明」（P.5-17）
- 「その他の関連資料」（P.5-19）
- 「HSRP 機能の履歴」（P.5-20）

HSRP について

HSRP は、ファーストホップ IP ルータの透過的フェールオーバーが可能な、First-Hop Redundancy Protocol（*FHRP*; ファーストホップ冗長プロトコル）です。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」（P.5-2）
- 「IPv4 の HSRP」（P.5-3）
- 「HSRP のバージョン」（P.5-5）

- 「HSRP 認証」（P.5-6）
- 「HSRP メッセージ」（P.5-6）
- 「HSRP ロード シェアリング」（P.5-6）
- 「オブジェクト トラッキングおよび HSRP」（P.5-7）
- 「ハイ アベイラビリティ」（P.5-8）

HSRP の概要

HSRP を使用する場合は、ホストのデフォルト ルータとして（実際のルータの IP アドレスではなく）、HSRP *仮想 IP アドレス*を設定します。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 または IPv6 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の*仮想 MAC アドレス*および仮想 IP アドレスを指定します。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 1 つを*アクティブ ルータ*として選択します。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。この時点で、選択されている*スタンバイ ルータ*が HSRP グループの仮想 MAC および IP アドレスの制御を引き継ぎます。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。

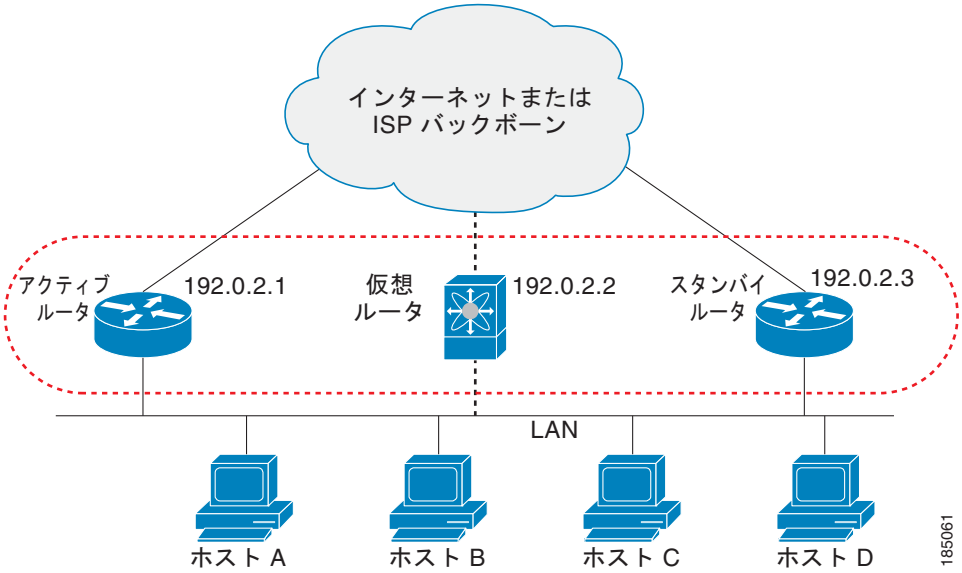
HSRP ではプライオリティ メカニズムを使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

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 フォワーディング機能の移動は、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 5-1 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*仮想ルータ*として動作させることができます。

図 5-1　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、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 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 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; バーンドイン MAC アドレス）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、Network Interface Card（NIC; ネットワーク インターフェイス カード）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 ARP（アドレス解決プロトコル）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。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。

IPv6 の HSRP

IPv6 ホストは、IPv6 Neighbor Discovery（ND; ネイバー探索）Router Advertisement（RA; ルータ アドバタイズメント）メッセージを通じて使用可能な IPv6 ルータを学習します。これらのメッセージは、定期的にマルチキャストされる他、ホストによって送信要求されることもあります。ただし、デフォルト ルートがダウンしていることを検出したときの遅延時間は 30 秒以上になることもあります。IPv6 の HSRP は、IPv6 ND プロトコルを使用した場合よりも、代替デフォルト ルータへのスイッチオーバーが大幅に高速であり、ミリ秒タイマーが使用される場合は 1 秒未満になります。IPv6 の HSRP では、IPv6 ホストの仮想ファースト ホップを提供します。

HSRP の IPv6 インターフェイスを設定すると、IPv6 ND がルータのライフタイムがゼロで最終 RA を送信した後で、インターフェイスのリンクローカル アドレスに対する定期 RA が停止します。インターフェイスの IPv6 リンクローカル アドレスに制限はありません。他のプロトコルによるこのアドレスに対するパケットの送受信は続行されます。

IPv6 ND は、HSRP グループがアクティブなときに、HSRP 仮想 IPv6 リンクローカル アドレスの定期 RA を送信します。これらの RA は、HSRP グループがアクティブ状態のままのときに、ルータのライフタイムがゼロで最終 RA が送信されると停止します。HSRP は、アクティブ HSRP グループ メッセージ（hello、coup、redesign）でのみ仮想 MAC アドレスを使用します。

IPv6 の HSRP は、次のパラメータを使用します。

- HSRP バージョン 2
- UDP ポート 2029
- 0005.73A0.0000 ～ 0005.73A0.0FFF の範囲の仮想 MAC アドレス
- マルチキャスト リンクローカル IP 宛先アドレス FF02::66
- ホップ リミット 255

HSRP IPv6 アドレス

HSRP IPv6 グループには、HSRP グループ番号から導出される仮想 MAC アドレス、および HSRP 仮想 MAC アドレスからデフォルトで導出される仮想 IPv6 リンクローカル アドレスがあります。仮想 IPv6 リンクローカル アドレスを形成するために HSRP IPv6 グループのデフォルトの仮想 MAC アドレスが常に使用されます。グループによって実際に使用されている仮想 MAC アドレスは関係ありません。

表 5-1 に、IPv6 ND パケットおよび HSRP パケットに使用される MAC アドレスおよび IP アドレスを示します。

表 5-1　HSRP および IPv6 ND アドレス

パケット	送信元 MAC アドレス	送信元 IPv6 アドレス	宛先 IPv6 アドレス	リンクレイヤ アドレス オプション
Neighbor solicitation（NS; ネイバー送信要求）	インターフェイス MAC アドレス	インターフェイス IPv6 アドレス	—	インターフェイス MAC アドレス
Router solicitation（RS; ルータ送信要求）	インターフェイス MAC アドレス	インターフェイス IPv6 アドレス	—	インターフェイス MAC アドレス

表 5-1　HSRP および IPv6 ND アドレス （続き）

パケット	送信元 MAC アドレス	送信元 IPv6 アドレス	宛先 IPv6 アドレス	リンクレイヤ アドレス オプション
Neighbor advertisement（NA; ネイバー アドバタイズメント）	インターフェイス MAC アドレス	インターフェイス IPv6 アドレス	仮想 IPv6 アドレス	HSRP 仮想 MAC アドレス
Route advertisement（RA; ルート アドバタイズメント）	インターフェイス MAC アドレス	仮想 IPv6 アドレス	—	HSRP 仮想 MAC アドレス
HSRP（非アクティブ）	インターフェイス MAC アドレス	インターフェイス IPv6 アドレス	—	—
HSRP（アクティブ）	仮想 MAC アドレス	インターフェイス IPv6 アドレス	—	—

HSRP は、IPv6 リンクローカル アドレスを Unicast Routing Information Base（URIB; ユニキャスト ルーティング情報ベース）に追加しません。リンクローカル アドレスにはセカンダリ仮想 IP アドレスもありません。

グローバル ユニキャスト アドレスの場合は、HSRP によって仮想 IPv6 アドレスが URIB および IPv6 に追加されますが、ICMPv6 には登録されません。ICMPv6 リダイレクトは HSRP IPv6 グループでサポートされません。

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、HSRP バージョン 1 で使用する IP マルチキャスト アドレス 224.0.0.2 の代わりに、IPv4 マルチキャスト アドレス 224.0.0.102 または IPv6 マルチキャスト アドレス FF02::66 を使用して hello パケットを送信します。
- IPv4 では 0000.0C9F.F000 ～ 0000.0C9F.FFFF、IPv6 アドレスでは 0005.73A0.0000 ～ 0005.73A0.0FFF の MAC アドレス範囲を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ～ 0000.0C07.ACFF です。
- 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 では、認証 TLV に IPv4 または IPv6 アドレスが含まれます。

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 5-2 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 5-2　HSRP ロード シェアリング

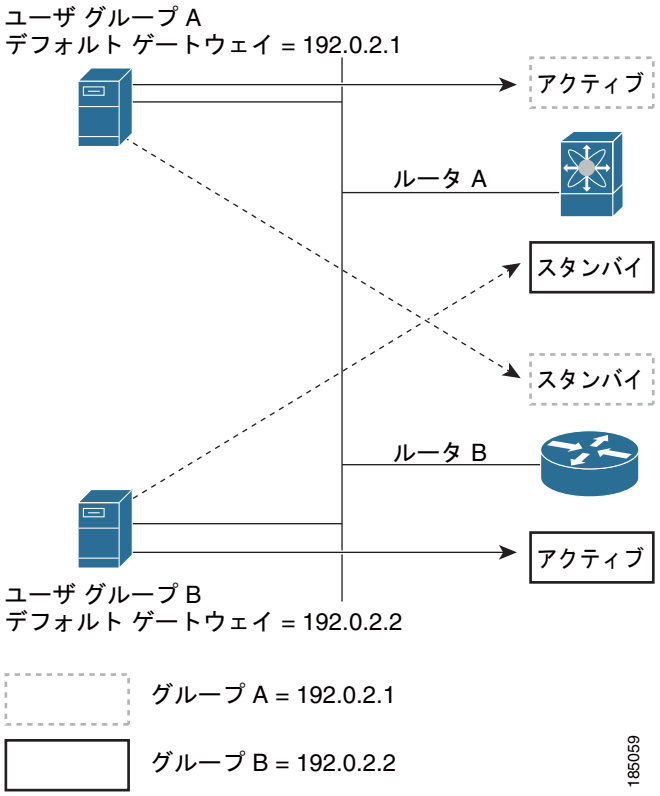


図 5-2 に、ルータ A、ルータ B、および 2 つの HSRP グループを示します。ルータ A はグループ A のアクティブ ルータであり、グループ B のスタンバイ ルータです。同様に、ルータ B は グループ B のアクティブ ルータであり、グループ A のスタンバイ ルータです。両方のルータがアクティブであるかぎり、HSRP は両方のルータにわたって、ホストからのトラフィックのロード バランシングを図ります。どちらかのルータで障害が発生すると、残りのルータが引き続き、両方のホストのトラフィックを処理します。

（注）　IPv6 の HSRP では、デフォルトでロード バランシングを行います。サブネットに 2 つの HSRP IPv6 グループがある場合、ホストはそれぞれの RA から両方を学習し、アドバタイズされているルータ間で負荷が共有されるように一方のグループを選択します。

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 のオブジェクト トラッキングの設定」（P.5-15）を参照してください。

（注）　プライマリ vPC ピア デバイス上の HSRP をアクティブ、vPC セカンダリ デバイス上の HSRP をスタンバイとして設定する必要があります。

ハイ アベイラビリティ

HSRP 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、HSRP 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。

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 DCNM	HSRP には Enterprise LAN ライセンスが必要です。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 DCNM にバンドルされており、追加費用は一切発生しません。Cisco DCNM のライセンス スキームの詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
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。使用しているプラットフォームでの Cisco NX-OS ライセンス スキームの詳細については、プラットフォームのライセンスに関するガイドを参照してください。

HSRPP の前提条件

Cisco DCNM の機能を使用するための前提条件は、次のとおりです。機能固有の前提条件については、プラットフォームのマニュアルを参照してください。

HSRP の前提条件は、次のとおりです。

- HSRP 機能のシステム メッセージ ロギング レベルは、Cisco DCNM 要件を満たすか、それ以上でなければなりません。デバイス検出処理で、Cisco DCNM は不適切なロギング レベルを検出し、レベルを高くして最小限の要件を満たすようにします。Cisco NX-OS Release 4.0 を実行する Cisco Nexus 7000 シリーズ スイッチは例外です。Cisco NX-OS Release 4.0 では、デバイス検出を行う前に、コマンドライン インターフェイスを使用して、ロギング レベルが Cisco DCNM 要件を満たすか、それ以上になるように設定されます。詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

デフォルト設定

表 5-2 に、HSRP 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 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

プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。注意事項および制約事項、システムのデフォルト、設定の制限などのプラットフォーム固有の情報については、該当するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000 シリーズ スイッチ マニュアル

HSRP の設定

ルーティング機能を選択して、HSRP にアクセスできます。

Cisco Data Center Network Manager 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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。

- 「HSRP バージョン設定」（P.5-10）
- 「IPv4 の HSRP グループの設定」（P.5-10）
- 「IPv6 の HSRP グループの設定」（P.5-11）
- 「HSRP 仮想 MAC アドレスの設定」（P.5-12）
- 「HSRP の認証」（P.5-13）
- 「プリエンプトの設定」（P.5-14）
- 「HSRP のオブジェクト トラッキングの設定」（P.5-15）
- 「HSRP プライオリティの設定」（P.5-15）
- 「HSRP のカスタマイズ」（P.5-16）

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。

（注）　IPv6 HSRP グループは、HSRP バージョン 2 として設定する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 4　[Details] ペインで、[Interface Settings] タブをクリックします。

[Interface Settings] タブが表示されます。

ステップ 5　[Interface Settings] タブの [HSRP Version] フィールドに、「**1**」（HSRP バージョン 1 の場合）または「**2**」（HSRP バージョン 2 の場合）を入力します。

ステップ 6　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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。

操作の前に

グループのいずれかのメンバー 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 アトリビュートを設定する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

ステップ 3　右クリックし、[New IPv4 GroupSetting] を選択します。

ステップ 4　[Interface] ドロップダウン リストから、HSRP グループを設定するインターフェイスまたはインターフェイス グループを選択します。

ステップ 5　[Group ID] フィールドに、このグループのグループ番号を入力します。

指定できる範囲は 0 ～ 255 です。

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] タブで、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 8　（任意）[Group Name] フィールドに、この HSRP グループ メンバーの名前を入力します。

ステップ 9　（任意）[Virtual IP Address Settings] 領域で、[Learn Virtual IP from Members of Group] チェックボックスをオンにして、他の HSRP グループ メンバーから仮想 IP アドレスを学習するようにします。

ステップ 10　（任意）[Virtual IP Address Settings] 領域の [Virtual IP Address] フィールドに、IPv4 アドレスを入力します。

ステップ 11　（任意）[Virtual IP Address Settings] 領域の [Secondary IP Address] フィールドに、セカンダリ IP アドレスの 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、変更内容をデバイスに適用します。

IPv6 の HSRP グループの設定

IPv6 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 MAC アドレスを設定できます。

IPv6 の HSRP グループを設定すると、HSRP はリンクローカル プレフィクスからリンクローカル アドレスを生成します。HSRP では、Modified EUI-64 形式のインターフェイス ID も生成します。EUI-64 インターフェイス ID は、関連の HSRP 仮想 MAC アドレスから作成されます。

HSRP IPv6 セカンダリ アドレスはありません。

操作の前に

IPv6 HSRP グループを設定するインターフェイスで HSRP バージョン 2 がイネーブルになっていることを確認します。

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 アトリビュートを設定してあることを確認します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

ステップ 3　右クリックし、[New IPv6 GroupSetting] を選択します。

ステップ 4　[Interface] ドロップダウン リストから、HSRP グループを設定するインターフェイスまたはインターフェイス グループを選択します。

ステップ 5　[Group ID] フィールドに、このグループのグループ番号を入力します。

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] タブで、[Interfaces] セクションを展開します。

[Details] ペインに HSRP インターフェイス情報が表示されます。

ステップ 8　[HSRP Version] フィールドに、「**2**」（HSRP バージョン 2 の場合）を入力します。

ステップ 9　[Group Details] タブで、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 10　（任意）[Group Name] フィールドに、この HSRP グループ メンバーの名前を入力します。

ステップ 11　（任意）[Virtual IP Address Settings] 領域で [Autoconfigure IP address] チェックボックスをオンにして、リンクローカル アドレスの仮想 IPv6 アドレスおよび HSRP 仮想 MAC アドレスを設定します。

ステップ 12　（任意）[Virtual IP Address Settings] 領域で、[Learn Virtual IP from Members of Group] チェックボックスをオンにして、他の HSRP グループ メンバーから仮想 IP アドレスを学習するようにします。

ステップ 13　（任意）[Virtual IP Address Settings] 領域の [Virtual IPv6 Address] フィールドに、IPv6 アドレスを入力します。

ステップ 14　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 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、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 6　[Virtual MAC Address] フィールドに、仮想 MAC アドレスを入力します。

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。

ステップ 7　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

インターフェイスで仮想 MAC アドレスとしてバーンドイン MAC アドレスを使用するように、HSRP を設定できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 4　[Details] ペインで、[Interface Settings] タブをクリックします。

[Interface Settings] タブが表示されます。

ステップ 5　[Interface Settings] タブで、[Use Burned In Address (use-bia)] チェックボックスをオンにします。

ステップ 6　（任意）すべてのグループでバーンドイン アドレスを使用するには、[Apply Use Burned In Address (use-bia) to all Groups] チェックボックスをオンにします。

ステップ 7　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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 7000 Series NX-OS Security Configuration Guide, Release 5.x*』を参照）。

操作の前に

HSRP グループのすべてのメンバー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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 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、[Authentication, Router Preemption] セクションを展開します。

[Details] ペインに認証情報が表示されます。

ステップ 6　[Authentication] 領域の [Method] ドロップダウン リストから、認証方式を選択します。

ステップ 7　（任意）テキスト認証の場合、パスワードのフィールドにパスワード文字列を入力します。

ステップ 8　（任意）MD5 認証の場合、[Key] または [Key Chain] を選択します。

ステップ 9　（任意）[Key] オプションについては、キーのフィールドにキー ストリングとタイムアウト値を入力し、暗号化されたキー ストリングの場合は [encrypted] チェックボックスをオンにします。

ステップ 10　（任意）[Key Chain] オプションについては、キーチェーンのドロップダウン リストから、使用する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、変更内容をデバイスに適用します。

プリエンプトの設定

設定されたプライオリティに基づいて他のアクティブ ルータを引き継ぐように HSRP を設定できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 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、[Authentication, Router Preemption] セクションを展開します。

[Details] ペインに認証情報が表示されます。

ステップ 6　[Router Preemption] チェックボックスをオンにします。

ステップ 7　[Minimum Delay(sec)] フィールドに、最小遅延時間を入力します。

ステップ 8　[Sync Delay(sec)] フィールドに、同期遅延時間を入力します。

ステップ 9　[Reload Delay(sec)] フィールドに、リロード後の遅延時間を入力します。

ステップ 10　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

HSRP のオブジェクト 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。デバイスがオブジェクト 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、デバイス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。オブジェクト トラッキングの詳細については、「プリエンプトの設定」（P.5-14）を参照してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 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、[Object Tracking] セクションを展開します。

[Details] ペインにオブジェクト トラッキング情報が表示されます。

ステップ 6　右クリックし、[Add Track Object] を選択します。

ステップ 7　[Object ID] ドロップダウン リストから、HSRP プライオリティ値を変更するために使用するオブジェクト ID を選択します。

ステップ 8　[Decrement] フィールドに、トラッキング対象オブジェクトがダウン状態となった場合に HSRP プライオリティ値を減少させる値を入力します。

ステップ 9　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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 メンバーを決定します。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。

IPv6 HSRP グループでは、すべてのグループ メンバーのプライオリティが同じ場合、HSRP は IPv6 リンクローカル アドレスに基づいてアクティブ ルータを選択します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP プライオリティを設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP プライオリティを設定する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 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、[Group Details] セクションを展開します。

[Details] ペインに基本グループ情報が表示されます。

ステップ 6　（任意）[Configured Priority] フィールドに、この HSRP グループ メンバーのプライオリティを入力します。

指定できる範囲は 1 ～ 255 です。デフォルトは 100 です。

ステップ 7　（任意）[Forwarding Threshold] チェックボックスをオンにして、vPC が使用する上限および下限のしきい値を設定し、vPC トランクに対するフェールオーバーのタイミングを定義します。

指定できる範囲は 1 ～ 255 です。下限のしきい値のデフォルトは 1 です。上限のしきい値のデフォルトは 100 です。

ステップ 8　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [HSRP] を選択します。

[Summary] ペインに、使用可能なデバイスが表示されます。

ステップ 2　[Summary] ペインで、HSRP を設定するデバイスをクリックします。

[Summary] ペインで HSRP の行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 3　強調表示された [Interface] フィールドで、HSRP グループを設定する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 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、[Timers] セクションを展開します。

[Details] ペインに HSRP タイマー情報が表示されます。

ステップ 6　[Configured Timers] 領域の [Hello Time] フィールドに、hello タイムを入力します。

ステップ 7　ドロップダウン リストから「**sec**」または「**msec**」を選択します。

ステップ 8　[Configured Timers] 領域の [Hold Time] フィールドに、ホールド タイムを入力します。

ステップ 9　ドロップダウン リストから「**sec**」または「**msec**」を選択します。

ステップ 10　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

HSRP のフィールドに関する説明

ここでは、HSRP の次のフィールドについて説明します。

- 「[HSRP]: [Group Details] タブ : [Group Details] セクション」（P.5-17）
- 「[HSRP]: [Group Details] タブ : [Authentication, Router Preemption] セクション」（P.5-18）
- 「[HSRP]: [Group Details] タブ : [Timers] セクション」（P.5-18）
- 「[HSRP]: [Group Details] タブ : [Object Tracking] セクション」（P.5-19）
- 「[HSRP]: [Interface Settings] タブ」（P.5-19）

[HSRP]: [Group Details] タブ : [Group Details] セクション

表 5-3　[HSRP]: [Group Details]: [Group Details]

フィールド	説明
Router	
Group ID	*表示専用。*HSRP グループのグループ番号。
Group Name	HSRP グループの名前。
Configured Priority	グループに設定されたプライオリティ。
Virtual MAC Address	仮想ルータの MAC アドレス。
Active Priority	*表示専用。*グループのプライオリティ。
Router State	*表示専用。*グループの状態
State Change Count	*表示専用。*グループの状態が変更された回数。
Last State Change	*表示専用。*グループの状態が最後に変更されたとき。
IP Address Settings	
Autoconfigure IP address	リンクローカル アドレスの仮想 IPv6 アドレスと、HSRP 仮想 MAC アドレスを設定します。
Learn Virtual IP from Members of Group	HSRP グループの他のメンバーから仮想 IPv4 アドレスまたは仮想 IPv6 アドレスを学習します。
Virtual IP Address	仮想ルータの IPv4 アドレス。
Secondary IP Address	仮想ルータのセカンダリ IPv4 アドレス。
Forwarding Threshold	
Forwarding Threshold	vPC のしきい値をイネーブルにします。

表 5-3　[HSRP]: [Group Details]: [Group Details] （続き）

フィールド	説明
Lower Threshold	フォワーディングの下限しきい値。
Upper Threshold	フォワーディングの上限しきい値。
Active Router	
IP Address	*表示専用。*アクティブ ルータの IPv4 アドレスまたは IPv6 アドレス。
Priority	*表示専用。*アクティブ ルータのプライオリティ。
Standby Router	
IP Address	*表示専用。*スタンバイ ルータの IPv4 アドレスまたは IPv6 アドレス。
Priority	*表示専用。*スタンバイ ルータのプライオリティ。

[HSRP]: [Group Details] タブ: [Authentication, Router Preemption] セクション

表 5-4　[HSRP]: [Group Details]: [Authentication, Router Preemption]

フィールド	説明
認証	
Method	この HSRP グループの認証方式。
Password	テキスト認証が選択された場合のパスワード。
Key Chain	キーチェーン認証が選択された場合のキーチェーン。
Key	キーチェーン認証が選択されていない場合のパスワード。
Encrypted	この HSRP グループのパスワードを暗号化します。
Router Preemption	
Router Preemption	ルータのプリエンプトをイネーブルにします。
Minimum Delay	プリエンプトの最小遅延時間。
Sync Delay	IP 冗長クライアントがルータのプリエンプトを回避できる最大時間。
Reload Delay	ルータのリロード後、HSRP がインターフェイス アップ イベントを検出するまでの時間。

[HSRP]: [Group Details] タブ: [Timers] セクション

表 5-5　[HSRP]: [Group Details]: [Timers]

フィールド	説明
Active Timer Values	
Hello Time	*表示専用。*この HSRP グループの Hello タイム。
Hold Time	*表示専用。*この HSRP グループのホールド タイム。
Configured Timers	
Hello Time	この HSRP グループの Hello タイム。
Hold Time	この HSRP グループのホールド タイム。

表 5-5　[HSRP]: [Group Details]: [Timers] （続き）

フィールド	説明
sec/msec	設定されたタイマーの時間単位。

[HSRP]: [Group Details] タブ : [Object Tracking] セクション

表 5-6　[HSRP]: [Group Details]: [Object Tracking]

フィールド	説明
Track ID	オブジェクト トラッキング ID。
Tracked Object	*表示専用*。トラッキング対象オブジェクトの名前。
Decrement	トラッキング対象オブジェクトがダウン状態となった場合に HSRP グループのプライオリティを減少させる値。

[HSRP]: [Interface Settings] タブ

表 5-7　[HSRP]:[Interface Settings] タブ

フィールド	説明
HSRP Version	このインターフェイスにあるすべてのグループの HSRP のバージョン。
Minimum Delay	このインターフェイスがオンライン状態になった後、HSRP グループの初期化を遅延させる最小時間。
Reload Delay	ルータのリロード後、HSRP がこのインターフェイスがアップになったことを検出するまでに遅延させる時間。
Use Burned In Address	HSRP 仮想 MAC アドレスの代わりにバーンドイン MAC アドレスを使用します。

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.5-20）
- 「MIB」（P.5-20）

関連資料

関連項目	マニュアル名
ゲートウェイ ロード バランシング プロトコルの設定	第 4 章「GLBP の設定」
HSRP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』
ハイ アベイラビリティの設定	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 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 5-8 は、この機能のリリースの履歴です。

表 5-8　HSRP 機能の履歴

機能名	リリース	機能情報
IPv6	5.0(2)	IPv6 のサポートが追加されました。
DCNM のサポート	4.1(2)	DCNM に HSRP のサポートが追加されました。

CHAPTER 6

オブジェクト トラッキングの設定

この章では、Cisco Data Center Network Manager（DCNM）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」（P.6-1）
- 「オブジェクト トラッキングのライセンス要件」（P.6-3）
- 「オブジェクト トラッキングの前提条件」（P.6-3）
- 「デフォルト設定」（P.6-3）
- 「プラットフォーム サポート」（P.6-3）
- 「オブジェクト トラッキングの設定」（P.6-4）
- 「クライアントの詳細情報の表示」（P.6-8）
- 「関連資料」（P.6-8）
- 「オブジェクト トラッキングのフィールドに関する説明」（P.6-8）
- 「オブジェクト トラッキング機能の履歴」（P.6-10）

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、デバイス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」（P.6-1）
- 「ハイ アベイラビリティ」（P.6-2）

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。

- Embedded Event Manager（EEM）
- Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）
- Hot Standby Redundancy Protocol（HSRP; ホットスタンバイ冗長プロトコル）
- Virtual port channel（vPC; 仮想ポート チャネル）
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）

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 または IPv6 アドレスが設定されていて、IPv4 または IPv6 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 または IPv6 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。

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 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。Cisco DCNM 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 DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。
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。使用しているプラットフォームでの Cisco NX-OS ライセンス スキームの詳細については、プラットフォームのライセンスに関するガイド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。

- オブジェクト トラッキング機能のシステム メッセージ ロギング レベルは、Cisco DCNM 要件を満たすか、それ以上でなければなりません。デバイス検出処理で、Cisco DCNM は不適切なロギング レベルを検出し、レベルを高くして最小限の要件を満たすようにします。Cisco NX-OS Release 4.0 を実行する Cisco Nexus 7000 シリーズ スイッチは例外です。Cisco NX-OS Release 4.0 では、デバイス検出を行う前に、コマンドライン インターフェイスを使用して、ロギング レベルが Cisco DCNM 要件を満たすか、それ以上になるように設定されます。

（注）　機能固有の前提条件については、プラットフォームのマニュアルを参照してください。

デフォルト設定

表 6-1 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 6-1　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
トラック対象オブジェクト VRF	デフォルト VRF のメンバー

プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。注意事項および制約事項、システムのデフォルト、設定の制限などのプラットフォーム固有の情報については、該当するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000 シリーズ スイッチ マニュアル

オブジェクト トラッキングの設定

ルーティング機能を選択して、オブジェクト トラッキングにアクセスできます。

Data Center Network Manager 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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.6-4）
- 「インターフェイス IPv6 オブジェクト トラッキングの削除」（P.6-5）
- 「新しい IP ルート IPv6 オブジェクト トラッキングの作成」（P.6-6）
- 「IP ルート IPv6 オブジェクト トラッキングの削除」（P.6-6）
- 「ルート到達可能性のオブジェクト トラッキング設定」（P.6-7）

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 IPv4 または IPv6 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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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、トラッキング対象とする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]、[IPv6 Routing]、[Line Protocol] のいずれかを選択します。

ステップ 9　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

IPv6 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 IPv6 ルーティングの状態をトラッキングするように Cisco NX-OS を設定できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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、トラッキング対象とする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、[IPv6 Routing] 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、変更内容をデバイスに適用します。

インターフェイス IPv6 オブジェクト トラッキングの削除

インターフェイス IPv6 オブジェクト トラッキングを削除できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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、トラッキング対象とする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、[IPv6 Routing] を選択します。

ステップ 9　[IPv6 Routing] を右クリックし、[Track Object] を選択します。

ポップアップ ダイアログボックスが表示されます。

ステップ 10　[Yes] または [No] を選択し、変更内容をデバイスに適用します。

新しい IP ルート IPv6 オブジェクト トラッキングの作成

新しい IP ルート IPv6 オブジェクト トラッキングを作成できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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] フィールドに、トラッキング対象とするプレフィクスおよびネットワーク マスクの長さを入力します。

IPv6 の場合、「A:B:C::D/ 長さ」のフォーマットで入力します。

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 VRF です。

ステップ 9　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

IP ルート IPv6 オブジェクト トラッキングの削除

IP ルート IPv6 オブジェクト トラッキングを削除できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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、トラッキング対象とする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] を選択します。

ステップ 9　右クリックし、[Track Object] を選択します。

ポップアップ ダイアログボックスが表示されます。

ステップ 10　[Yes] または [No] を選択し、変更内容をデバイスに適用します。

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。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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 [Actions] > [New Track Object] を選択します。

[Summary] ペインで新しいトラッキング対象オブジェクトの行が強調表示され、[Details] ペインのタブが更新されます。

ステップ 4　強調表示された [Track Object ID] フィールドにで、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] タブの [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] フィールドに、トラッキング対象とするプレフィクスおよびネットワーク マスクの長さを入力します。

IPv4 の場合、「A.B.C.D/ 長さ」のフォーマットで入力します。IPv6 の場合、「A:B:C::D/ 長さ」のフォーマットで入力します。

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 VRF です。

ステップ 9　メニュー バーから [File] > [Deploy] を選択し、変更内容をデバイスに適用します。

クライアントの詳細情報の表示

トラッキング対象オブジェクトのクライアントの詳細情報を表示できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[Routing] > [Gateway Redundancy] > [Object Tracking] を選択します。

[Summary] ペインに、使用可能な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する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するトラッキング対象オブジェクトをクリックします。

[Summary] ペインでトラッキング対象オブジェクトの行が強調表示され、[Details] ペインの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情報が表示されます。

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」
- 第 5 章「HSRP の設定」

オブジェクト トラッキングのフィールドに関する説明

ここでは、オブジェクト トラッキングの次のフィールドについて説明します。

- 「[Object Tracking]: [Details] タブ : [Object Tracking Details] セクション」（P.6-8）
- 「[Object Tracking]: [Details] タブ : [Client Details] セクション」（P.6-9）

[Object Tracking]: [Details] タブ : [Object Tracking Details] セクション

表 6-2　[Object Tracking]: [Details]: [Object Tracking Details]

フィールド	説明
Track Object ID	*表示専用*。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	トラッキング対象オブジェクトのタイプ。

表 6-2　[Object Tracking]: [Details]: [Object Tracking Details] （続き）

フィールド	説明
Instance	このオブジェクトをトラッキングする IPv4/IPv6 アドレスまたはインターフェイス。
VRF	トラッキング対象のインターフェイスが存在する VRF。
Parameter	このオブジェクトのトラッキングに使用されるパラメータ タイプ。
Tracking Status	*表示専用。*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	*表示専用。*このオブジェクトのパラメータ ステータスが最後に変更されたとき。

[Object Tracking]: [Details] タブ: [Client Details] セクション

表 6-3　[Object Tracking]: [Details]: [Client Details]

フィールド	説明
Client Name	*表示専用。*この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	指定されたクライアント機能にこ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	*表示専用。*指定されたクライアント機能にこのトラッキング対象オブジェクトを使用するグループの 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.6-10）
- 「標準規格」（P.6-10）

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 Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*』
Embedded Event Manager の設定	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』

標準規格

標準規格	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 6-4 は、この機能のリリースの履歴です。

表 6-4　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
IPv6 のサポート	5.0(2)	IPv6 のサポートが追加されました。
オブジェクト トラッキング	4.0(1)	この機能が導入されました。

APPENDIX A

Cisco NX-OS Unicast Features Release 5.x がサポートする IETF RFC

この付録は、Cisco NX-OS Release 5.x がサポートする IETF RFC の一覧です。

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*』

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 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』

RFC	タイトル
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 Active Virtual Forwarder（アクティブ仮想フォワーダ）。**特定の仮想 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（アクティブ仮想ゲートウェイ）。**アクティブ仮想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 つの仮想ゲートウェイ。**

B

BDR Backup Designated Router（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 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 スピーカとネイバー関係が確立されている、リモート BGP スピーカ。

D

DHCP Dynamic Host Control Protocol（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 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（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 Update Algorithm（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 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。

G

GLBP Gateway Load Balancing Protocol（ゲートウェイ ロード バランシング プロトコル）。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 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。

High Availability（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。

HSRP Hot Standby Router Protocol（ホットスタンバイ ルータ プロトコル）。

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 Interior Gateway Protocol（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。

instance 独立した設定可能なエンティティ。通常はプロトコル。

IP トンネル

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。

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

K

Keepalive（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。

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

NDP Neighbor Discovery Protocol（ネイバー探索プロトコル）。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

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。

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あります。

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。

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 認証キーを制御する方法の 1 つ。詳細については『*Cisco NX-OS Security Configuration Guide*』を参照してください。

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

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。

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

バックアップ代表ルータ 「BDR」を参照してください。

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。

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。

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。

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 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。

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。

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

C

CDP 3-13

D

DNS 3-12

G

GLBP
- 重み付けおよびトラッキングの設定 4-10
- カスタマイズ 4-11
- 機能の履歴（表） 4-16
- グループのイネーブル化 4-12
- グループの作成 4-8
- ゲートウェイ プリエンプトの設定 4-10
- 説明 4-1
- タイマー 4-11
- デフォルト設定 4-7
- 認証の設定 4-8
- ロード バランシングの設定 4-9

H

HSRP
- IPv6 グループの設定 5-11
- アドレッシング 5-3
- カスタマイズ 5-16
- 機能の履歴（表） 5-20
- グループの設定 5-10
- スタンバイ ルータ 5-2
- 説明 5-2
- 前提条件 5-8
- デフォルト設定 5-9
- プライオリティの設定 5-15
- メッセージ 5-6
- ライセンス要件 5-8
- ロード シェアリング 5-6

HSRP オブジェクト トラッキング
- 設定 5-15
- 説明 5-7

HSRP 仮想 MAC アドレス
- 設定 5-12
- 説明 5-2

HSRP 認証
- 設定 5-13
- 説明 5-6

HSRP のバージョン
- 設定 5-10
- 説明 5-5

I

ICMPv6 3-13
- パケット ヘッダーのフォーマット（図） 3-13

IP
- アドレス 2-2
- アドレスの設定 2-3
- 機能の履歴（表） 2-5
- サブネット マスク 2-1
- セカンダリ アドレス（注） 2-2
- セカンダリ アドレスの設定 2-4
- 説明 2-1
- パケット ヘッダー 3-9
- ライセンス要件 2-2

IPv4。「IP」を参照
IPv6
CDP 3-13
DNS 3-12
EUI-64 フォーマット 3-4
ICMP 3-13
IPv4 と互換性のあるアドレス 3-5
RFC 3-3, 3-4
アドレスの設定 3-18
アドレス フォーマット 3-2
アドレス フォーマット（表） 3-2
インターフェイス ID 3-4
エニーキャスト アドレス 3-7
機能の履歴（表） 3-20
サイトローカル アドレス 3-7
サブネット ID 3-4
セカンダリ アドレスの設定 3-19
説明 3-1
ネイバー送信要求メッセージ 3-14
ネイバー探索 3-14
ネイバー リダイレクト メッセージ 3-17
パケット ヘッダー 3-9
パス MTU 探索 3-12
マルチキャスト アドレス 3-7
未指定アドレス（注） 3-3
ユニーク ローカル アドレス 3-6
ユニキャスト アドレス 3-3
ライセンス要件 3-18
リンクローカル アドレス 3-5
ルータ アドバタイズメント メッセージ 3-15
ループバック アドレス（注） 3-3

M

MIB
OSPF 5-20

N

ND
説明 3-14

O

OSPF
MIB 5-20

R

Really Simple Syndication。「RSS」を参照
RSS
ドキュメンテーション フィード xiii

あ

新しい機能と変更された機能（表） vii
アドレス フォーマット
IPv4 2-2
IPv6 3-2
IPv6（表） 3-2

い

インターフェイス
セカンダリ IPv6 アドレスの設定 3-19

お

オブジェクト トラッキング
GLBP の設定 4-10
インターフェイスでの設定 6-4
機能の履歴（表） 6-10
クライアントの詳細情報の表示 6-8
説明 6-1
前提条件 6-3

デフォルト設定　6-3
ハイ アベイラビリティ　6-2
ライセンス要件　6-3
ルート到達可能性の設定　6-7

か

関連資料　x

け

ゲートウェイ ロード バランシング プロトコル。「GLBP」を参照

さ

サービス
依頼　xiii

し

集約可能グローバル アドレス。「IPv6」を参照
ユニキャスト アドレス

て

デフォルト設定
GLBP　4-7
HSRP　5-9
オブジェクト トラッキング　6-3

ね

ネイバー探索。「ND」を参照
ネイバー リダイレクト メッセージ　3-17

は

ハイ アベイラビリティ
オブジェクト トラッキング　6-2
パス MTU 探索　3-12

ほ

ホットスタンバイ ルータ プロトコル。「HSRP」を参照

ま

マニュアル
更新　xiii
その他の資料　x

ら

ライセンス要件
HSRP　5-8
IP　2-2
IPv6　3-18
オブジェクト トラッキング　6-3

る

ルータ アドバタイズメント メッセージ　3-15