CHAPTER 40

IPv6 ユニキャスト ルーティングの設定

この章では、Catalyst 3560 または 3560-C スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

（注） この章で説明するすべての IPv6 機能を使用するには、スイッチで IP サービス イメージが稼働している必要があります。IP ベースのイメージが稼働しているスイッチは、IPv6 スタティック ルーティングと IPv6 の RIP だけをサポートします。

IPv6 Multicast Listener Discovery（MLD）スヌーピングの設定については、第 42 章「IPv6 MLD スヌーピングの設定」を参照してください。IPv6 アクセス コントロール リスト（ACL）の設定については、第 41 章「IPv6 ACL の設定」を参照してください。IPv4 ユニキャスト ルーティングの設定については、第 39 章「IP ユニキャスト ルーティングの設定」を参照してください。

（注） IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを使用するようにスイッチを設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」（P.40-10）を参照してください。この章で使用しているコマンドの完全な構文と使用方法については、手順の中で参照している Cisco IOS のマニュアルを参照してください。

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータでネットワーク アドレス変換（NAT）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 次の URL にある『*Cisco IOS IPv6 Configuration Library*』を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- Cisco IOS ソフトウェア マニュアルを検索するには、検索フィールドを使用します。たとえば、スタティック ルートに関する情報を取得する場合は、検索フィールドに「*Implementing Static Routes for IPv6*」と入力してスタティック ルートに関する資料を取得します。
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

これらの項では、スイッチへの IPv6 の実装について説明します。

- 「IPv6 アドレス」（P.40-2）
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」（P.40-3）
- 「サポートされていない IPv6 ユニキャスト ルーティング機能」（P.40-15）
- 「制限事項」（P.40-15）

IPv6 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。スイッチはサイトローカルなユニキャスト アドレス、エニキャスト アドレス、またはマルチキャスト アドレスをサポートしません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章では、次の項の内容は Catalyst 3560 または 3560-C スイッチに適用されます。

- 「IPv6 Address Formats」
- 「IPv6 Address Type: Unicast」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

スイッチは、ネイティブ イーサネット Inter-Switch Link（ISL; スイッチ間リンク）または 802.1Q トランク ポートによる IPv6 ルーティング機能（スタティック ルートの場合）、IPv6 対応の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルを提供します。等コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、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 エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィックス FE80::/10（1111 1110 10）およびインターフェイス ID を使用します。Neighbor Discovery Protocol（NDP; ネイバー探索プロトコル）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の DNS

IPv6 は、Domain Name System（DNS; ドメイン ネーム システム）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチはシステム Maximum Transmission Unit（MTU; 最大伝送単位）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合せて調整できます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャスト パケットのパス MTU ディスカバリをサポートしません。

ICMPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 NDP は ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクスト ホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

IPv6 でのファーストホップ セキュリティ

ここでは、IPv6 でのファーストホップ セキュリティ（FHS）機能を構成する機能の設定について説明します。

FHS の下で使用可能な機能は、IPv6 ポリシーとも呼ばれます。ポリシーは、インターフェイスまたは VLAN レベルで適用できます。IPv6 ポリシーは、これらのポリシーの保存とアクセスに関する機能にポリシー データベース サービスを提供します。ポリシーが設定されるたびに、そのポリシーの属性がソフトウェア ポリシー データベース内に保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。次の IPv6 ポリシーを使用できます。

- 「IPv6 スヌーピング」（P.40-6）
- 「IPv6 ファーストホップ セキュリティ バインディング テーブル」（P.40-6）
- 「NDP アドレス グリーニング」（P.40-6）
- 「IPv6 DHCP アドレス グリーニング」（P.40-6）
- 「IPv6 DHCP アドレス グリーニング」（P.40-6）
- 「IPv6 ND 検査」（P.40-8）
- 「IPv6 デバイス トラッキング」（P.40-8）
- 「IPv6 ポートベースのアクセス リスト サポート」（P.40-8）
- 「IPv6 ルータ アドバタイズメント ガイド」（P.40-8）
- 「IPv6 デバイス トラッキング」（P.40-8）
- 「IPv6 ソース ガード」（P.40-9）

（注） IPv6 でファーストホップ セキュリティを実装するための前提条件：

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

（注） IPv6 でファーストホップ セキュリティを実装するための制約事項：

- この機能は、ギガビット イーサネット スイッチでのみサポートされています。
- ファーストホップ セキュリティは、Catalyst 3560-CG シリーズ スイッチでのみサポートされています。

- VLAN ターゲットは、スタックが混在した状況ではサポートされません。

IPv6 スヌーピング

IPv6 スヌーピングは、IPv6 での FHS で使用可能なほとんどの機能を可能にするコンテナ ポリシーとして機能します。詳細については、「IPv6 スヌーピング ポリシーの設定」（P.40-20）を参照してください。

IPv6 ファーストホップ セキュリティ バインディング テーブル

スイッチに接続された IPv6 ネイバーのデータベース テーブルは、ネイバー探索プロトコル（NDP）スヌーピングやダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングなどの複数の情報ソースから作成されます。このデータベースまたはバインディング テーブルは、IPv6 ネイバー探索（ND）検査（リンク層アドレス（LLA）を検証するため）、ポート単位のアドレス制限（IPv4 または IPv6 アドレスを検証するため）、IPv6 デバイス トラッキング（スプーフィングやリダイレクト攻撃を防止するためにネイバーのバインディングを付加するため）などの、さまざまな IPv6 ガード機能によって使用されます。

次のトラフィックのカテゴリは、バインディング テーブルのスヌーピング対象の情報を伝送します。

- ND トラフィック：詳細については、「NDP アドレス グリーニング」（P.40-6）を参照してください。
- DHCP トラフィック：詳細については、「IPv6 DHCP アドレス グリーニング」（P.40-6）を参照してください。
- データ トラフィック：詳細については、「IPv6 DHCP アドレス グリーニング」（P.40-6）を参照してください。

NDP アドレス グリーニング

ipv6 snooping policy グローバル コンフィギュレーション コマンドを設定すると、NDP アドレス グリーニング機能がデフォルトでイネーブルになります。この機能をディセーブルにするには、**no protocol ndp** グローバル コンフィギュレーション コマンドを入力し、このポリシーをターゲット ポートまたは VLAN に適用します。

IPv6 DHCP アドレス グリーニング

IPv6 DHCP アドレス グリーニング機能は、DHCP メッセージからアドレスを抽出し、バインディング テーブルに入力する機能を提供します。スイッチは、次のタイプの DHCPv6 交換からアドレス バインディング情報を抽出します（ユーザ データグラム プロトコル（UDP）、ポート 546 および 547 を使用）。

- DHCP-REQUEST
- DHCP-CONFIRM
- DHCP-RENEW
- DHCP-REBIND
- DHCP-REPLY
- DHCP-RELEASE
- DHCP-DECLINE

スイッチがクライアントから DHCP-REQUEST メッセージを受信した後、次のいずれかが発生することがあります。

- スイッチが DHCP サーバから DHCP-REPLY メッセージを受信し、バインディング テーブル エントリが REACHABLE ステートで作成されて完成されます。この応答の Layer 2 (L2) DMAC フィールドには、IP アドレスと MAC アドレスが含まれています。

  バインディング テーブル内にエントリを作成すると、スイッチは DHCP によって割り当てられたアドレスを学習できるようになります。バインディング テーブルは、次のいずれかのステートになります。

  - INCOMPLETE：アドレス解決中であり、リンク層アドレスはまだ不明です。
  - REACHABLE：このテーブルは、最後の到達可能時間間隔内で到達可能であることがわかっています。
  - STALE：このテーブルには再解決が必要です。
  - SEARCH：エントリを作成している機能には L2 アドレスが存在せず、バインディング テーブルが L2 アドレスを検索するよう要求しています。
  - VERIFY：L2 およびレイヤ 3（L3）アドレスが知られており、アドレスを確認するために重複アドレス検出（DAD）ネイバー送信要求（NS）ユニキャスト メッセージを L2 および L3 宛先に送信します。
  - DOWN：エントリを学習する元のインターフェイスがダウンしており、検証を行えません。
- DHCP サーバは DHCP-DECLINE メッセージまたは DHCP-RELEASE メッセージを送信し、エントリが削除されます。
- クライアントが、アドレスを割り当てたサーバに DHCP-RENEW メッセージを送信するか、または任意のサーバに DHCP-REBIND メッセージを送信し、そのエントリの有効期限が延長されます。
- サーバが応答せず、セッションがタイムアウトします。

この機能をイネーブルにするには、**ipv6 snooping policy** *policy-name* グローバル コンフィギュレーション コマンドを使用してポリシーを設定します。詳細については、「IPv6 スヌーピング ポリシーの設定」（P.40-20）を参照してください。

ポリシーを設定し、それを DHCP ガードに適用することにより、偽造された DHCP メッセージがバインディング テーブルに入力されることを防止できます。詳細については、「IPv6 DHCP ガード」（P.40-9）および「IPv6 DHCP ガードの設定」（P.40-22）を参照してください。

IPv6 データ アドレス グリーニング

IPv6 データ アドレス グリーニング機能は、リダイレクトされたデータ トラフィックからアドレスを抽出し、ネイバーを探索して、バインディング テーブルに入力する機能を提供します。

バインディングが不明（ネイバーが INCOMPLETE 状態で、リンク層アドレスがまだ不明）なデータ パケットをポートが受信すると、スイッチは DAD NS NDP ユニキャスト メッセージを、そのデータ パケットの送信元ポートに送信します。

ホストが DAD ネイバー アドバタイズメント（NA）NDP メッセージで応答した後、バインディング テーブルが更新され、プライベート VLAN ACL（PVACL）がこのバインディングのためのハードウェアにインストールされます。

ホストが DAD NA で応答しない場合は、バインディング テーブル タイマーが期限切れになった後にハードウェアに通知され、そのバインディングに関連付けられたリソースがすべて解放されます。

この機能をイネーブルにするには、**data-glean** を使用してポリシーを設定し、そのポリシーをターゲット ポートに適用します。ポリシーをデバッグするには、**debug ipv6 snooping** 特権 EXEC コマンドを使用します。

IPv6 ND 検査

IPv6 ND 検査は、L2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージはドロップされます。SA ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。

この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキング機能は、IPv6 ホストが非表示になったときにネイバー テーブルを更新できるように、IPv6 ホストの活性トラッキングを提供します。この機能は、ネットワーク アクセス権限が非アクティブになったときに取り消すために、L2 スイッチ経由で接続されたネイバーの活性を定期的に追跡します。

IPv6 ポートベースのアクセス リスト サポート

IPv6 ポートベースのアクセス リスト（PACL）機能は、IPv6 トラフィック用の L2 スイッチ ポートでアクセス コントロール（許可または拒否）を提供する機能を備えています。IPv6 PACL は、IPv4 トラフィック用の L2 スイッチ ポートでアクセス コントロールを提供する IPv4 PACL と似ています。

Catalyst 3750-E、3750X、3560E、3560-X、3750v2、および 3560 v2 スイッチでは、この機能はハードウェアで、かつ入力方向だけでサポートされています。IPv6 FHS をサポートしていないスイッチがスタックに含まれている、スタックが混在した状況では、セキュリティのために、VLAN ターゲットはスイッチ全体でディセーブルになります。スイッチの IPv6 FHS 対応ポートでは、ポート ターゲットが許可されます。サポートしていないスイッチがスタック マスターになった場合、IPv6 FHS 機能は引き続き、スイッチの IPv6 FHS 対応ポートでサポートされます。

アクセス リストによって、スイッチ インターフェイスでどのトラフィックがブロックされ、どのトラフィックが転送されるかが決定され、送信元アドレスと宛先アドレスに基づいて、特定のインターフェイスへの着信と発信をフィルタリングできます。各アクセス リストの末尾には、暗黙的な deny 文があります。IPv6 PACL を設定するには、IPv6 アクセス リストを作成した後、指定した IPv6 L2 インターフェイスで PACL モードを設定する必要があります。

PACL は、L3 およびレイヤ 4（L4）ヘッダー情報または非 IP L2 情報に基づいて L2 インターフェイスで入力トラフィックをフィルタリングできます。

IPv6 ルータ アドバタイズメント ガイド

IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、L2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

IPv6 DHCP ガード

DHCP ガードを使用すると、偽造されたメッセージがバインディング テーブルに入力されることを防止できます。DHCP ガードは、DHCP サーバまたは DHCP リレー側であることが明示的に設定されていないポートで DHCP サーバ メッセージが受信されると、それらのメッセージをブロックします。

この機能を使用するには、ポリシーを設定し、それを DHCP ガードに適用します。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

IPv6 ソース ガード

ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

IPv6 ソース ガードとは、IPv6 バインディング テーブルを使用して PACL をインストールし、ホストが無効な IPv6 送信元アドレスを持つパケットを送信しないようにする機能です。

ソース ガード パケットをデバッグするには、**debug ipv6 snooping source-guard** 特権 EXEC コマンドを使用します。

（注）　IPv6 PACL 機能は、入力方向だけでサポートされ、出力方向ではサポートされません。

次の制約事項が適用されます。

- IPv6 ソース ガードがスイッチポートでイネーブルになっている場合は、そのスイッチポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにする必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。
- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。
- EtherChannels では、IPv6 ソース ガードはサポートされません。

IPv6 アクセス リストの設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Traffic Filters and Firewalls for IPv6 Security」の章を参照してください。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDP は、到達可能または到達可能の可能性があるルータとして、常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

IPv6 の DRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、Traceroute、Telnet、および Trivial File Transfer Protocol（TFTP）
- IPv6 トランスポートによる Secure Shell（SSH; セキュア シェル）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方に Ternary Content Addressable Memory（TCAM; 3 値連想メモリ）の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 40-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 40-1　インターフェイス上での IPv4/IPv6 のデュアル サポート

IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management（SDM; スイッチング データベース管理）テンプレートを使用します。デュアル IPv4/IPv6 SDM テンプレートについての詳細は、第 8 章「SDM テンプレートの設定」を参照してください。

デュアル IPv4 および IPv6 テンプレートを使用すると、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 専用環境のスイッチは、IPv4 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境のスイッチは、IPv4 および IPv6 パケットをルーティングし、IPv4 QoS をハードウェアで適用します。
- 完全な IPv6 QoS はサポートされていません。IPv6 QoS trust はサポートされていません。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4/IPv6 プロトコル スタックについての詳細は、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 により、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能により、ホストが接続されているネットワークに基づいた適切なプレフィックスで重複のないアドレス割り当てが行われます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

Cisco IOS Release 12.2(58)SE 以降のリリースでは、IP ベース フィーチャ セットを実行するスイッチは次の機能をサポートします。

- DHCPv6 バルクリース クエリー

  DHCPv6 バルクリース クエリーでは、クライアントが、DHCPv6 バインディングに関する情報を要求できます。この機能により、新しいクエリー タイプが追加され、TCP を使用した DHCPv6 バインディング データのバルク転送が可能になります。DHCPv6 バインディング データのバルク転送は、リレー サーバ スイッチが再起動されて、リレー サーバにあるバインディング情報がすべて失われたときに役に立ちます。再起動後、リレー サーバは自動的にバルクリース クエリーを生成して、DHCP サーバからバインディング情報を取得します。

- DHCPv6 リレー ソース設定

  DHCPv6 サーバは、DHCP リレー エージェントの送信元アドレスに対して応答します。通常、DHCPv6 リレー エージェントからのメッセージには、それらの送信元インターフェイスが送信元アドレスとして示されます。DHCPv6 リレー送信元設定機能を使用して、より安定したアドレス（ループバック インターフェイスなど）をリレー エージェントからのメッセージの送信元アドレスとして設定できます。送信元アドレスは、スイッチに対してグローバルに、または特定のインターフェイスに設定できます。インターフェイスに設定されたアドレスは、グローバルに設定されたアドレスよりも優先されます。

これらの機能の詳細および設定方法については、『*Cisco IOS IPv6 Configuration Guide, Release 12.4*』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 の RIP

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 の OSPF の設定

IP サービス イメージが稼働するスイッチは IP のリンクステート プロトコルの IPv6 Open Shortest Path First（OSPF）をサポートしています。詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

OSPFv3 グレースフル リスタート

Cisco IOS Release 12.2(58)SE 以降のリリースでは、IP サービス フィーチャ セットを実行するスイッチは OSPFv3 のグレースフル リスタート機能をサポートします。この機能により、OSPFv3 ルーティング プロトコル情報が復元されている間も、既知のルート上でノンストップのデータの転送が可能になります。スイッチでは、グレースフル リスタートがリスタート モード（グレースフル リスタート対応スイッチの場合）とヘルパー モード（グレースフル リスタート認識スイッチの場合）のいずれかで使用されます。

グレースフル リスタート機能を使用するには、スイッチがハイアベイラビリティ ステートフル スイッチオーバー（SSO）モードである必要があります（デュアル ルート プロセッサ）。グレースフル リスタートに対応したスイッチでは、次の障害が発生したときにグレースフル リスタートが使用されます。

- スタンバイ ルート プロセッサへの切り替えが起こるルート プロセッサ障害
- 計画されたスタンバイ ルート プロセッサへのルート プロセッサの切り替え

グレースフル リスタート機能では、隣接スイッチがグレースフル リスタート認識である必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

高速コンバージェンス：LSA および SPF スロットリング

OSPFv3 リンク ステート アドバタイズメント（LSA）および Shortest Path First（SPF）スロットリング機能は、ネットワークが不安定なときに、OSPFv3 でのリンク ステート アドバタイズメントの更新の速度を低下させる動的な方法ダイナミック方式を提供します。またこの機能を使用すると、LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮が可能になります。

OSPFv3 では以前はレート制限 SPF 計算および LSA 生成にスタティック タイマーを使用しました。これらのタイマーを設定することもできますが、値は秒単位で指定するため、OSPFv3 コンバージェンスに制限が課せられます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限方式を提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPFv3」の章を参照してください。

IPsec による OSPFv3 認証のサポート

OSPF for IPv6（OSPFv3）パケットが変更されずにスイッチに再送信されるようにするには、OSPFv3 パケットを認証する必要があります。OSPFv3 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。OSPFv3 で使用するために必要な IPsec API は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「OSPFv3 Authentication Support with IPsec」の章を参照してください。

EIGRP IPv6

IP サービス イメージが稼働しているスイッチは、Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 をサポートします。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。

（注）　IP ベースのイメージが稼働しているスイッチは、IPv6 EIGRP スタブ ルーティングなどの IPv6 EIGRP 機能をサポートしません。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼働するため、使用可能な IPv4 ルータ ID がない場合があります。

IPv6 の EIGRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の HSRP

IP サービス イメージが稼働するスイッチは、IPv6 対応のホットスタンバイ ルータ プロトコル（HSRP）をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能な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か、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

IPv6 の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 上の SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 に関連する SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP（S）

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続が確立するためには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 ポリシーベース ルーティング
- IPv6 バーチャル プライベート ネットワーク（VPN）Routing And Forwarding（VRF; VPN ルーティングおよび転送）テーブルのサポート
- Multiprotocol ボーダー ゲートウェイ プロトコル（BGP）、および Intermediate System-to-Intermediate System（IS-IS）ルーティングの IPv6 ルーティング プロトコルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding
- IPv6 の汎用プレフィックス

制限事項

IPv6 はスイッチのハードウェアに実装されるため、TCAM 内の IPv6 圧縮アドレスによるいくつかの制限があります。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- ICMPv6 リダイレクト機能は、IPv6 ホスト ルート（特定のホストに到達するのに使用されるルート）、またはマスク長が 64 ビットを超える IPv6 ルートではサポートされません。スイッチは、ホスト ルートまたはマスク長が 64 ビットを超えるルートを介して到達可能な特定の宛先へのより最適なファーストホップ ルータに、ホストをリダイレクトできません。
- マスク長が 64 ビットを超える IPv6 ホスト ルートまたは IPv6 ルートでは、等価コストおよび不等価コスト ルートを使用するロード バランシングはサポートされません。
- スイッチは、SNAP カプセル化 IPv6 パケットを転送できません。

（注） IPv4 SNAP カプセル化パケットにも同様の制限がありますが、パケットはスイッチでドロップされ、転送されません。

- スイッチは、IPv6/IPv4 および IPv4/IPv6 パケットをハードウェアでルーティングしますが、スイッチを IPv6/IPv4 または IPv4/IPv6 トンネル エンドポイントにはできません。
- ホップバイホップの拡張ヘッダーを持つブリッジング済みの IPv6 パケットは、ソフトウェアで転送されます。IPv4 の場合、これらのパケットはソフトウェアでルーティングされ、ハードウェアでブリッジングされます。
- IPv6 トラフィックのインターフェイス カウンタには、ソフトウェアによって転送されたトラフィックだけが含まれます。ハードウェアでスイッチングされたトラフィックは含まれません。
- ソフトウェア コンフィギュレーション ガイドで定義された標準の SPAN および RSPAN 制限のほかに、次のような IPv6 パケット固有の制限事項があります。
  - RSPAN IPv6 ルーテッド パケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスが不正である場合があります。
  - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスが不正である場合があります。標準トラフィックは影響を受けません。
- スイッチはソースルート IPv6 パケットに関する QoS 分類または PBR をハードウェアで適用できません。
- スイッチはマルチキャスト パケットに対して ICMPv6 *Packet Too Big* メッセージを生成できません。

IPv6 の設定

ここでは、次の IPv6 転送の設定情報について説明します。

IPv6 のデフォルト設定

表 40-1 に IPv6 のデフォルト設定を示します。

表 40-1　IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	ディセーブル（IPv4 CEF および dCEF はデフォルトでイネーブル） **（注）** IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- この章に記載されたすべての機能が IP サービス イメージが稼働する Catalyst 3560 スイッチでサポートされているわけではありません。「サポートされていない IPv6 ユニキャスト ルーティング機能」（P.40-15）を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで指定した *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**default**| **routing** | **vlan**}	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **default**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **routing**：IPv4 PBR などの IPv4 および IPv6 ルーティングをサポートするためにスイッチをルーティング テンプレートに設定します。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	オペレーティング システムをリロードします。
ステップ 5	**configure terminal**	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、Switch Virtual Intertface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 8	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address/prefix length* または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	IPv6 アドレスの下位 64 ビットの Extended Unique Identifier（EUI; 拡張固有識別子）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスの IPv6 アドレスを手動で設定します。 インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing**	スイッチ上で IP ルーティングをイネーブルに設定します。

	コマンド	目的
ステップ 11	**ipv6 unicast-routing**	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

IPv6 でのファーストホップ セキュリティの設定

- 「IPv6 スヌーピング ポリシーの設定」（P.40-20）
- IPv6 バインディング テーブルの内容の設定
- IPv6 デバイス トラッキングの設定

- IPv6 ND 検査の設定
- IPv6 RA ガードの設定
- IPv6 PACL の設定
- 「IPv6 DHCP ガードの設定」（P.40-22）
- 「IPv6 ソース ガードの設定」（P.40-23）
- 「IPv6 でファーストホップ セキュリティを実装する場合の設定例」（P.40-23）

IPv6 スヌーピング ポリシーの設定

	アクションまたはコマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 snooping policy** *policy-name*	グローバル コンフィギュレーション モードでスヌーピング ポリシーを作成します。

	アクションまたはコマンド	目的
ステップ 4	**[data-glean | default | device-role [node | switch] | limit {address-count** *value* **}| no | protocol [all | dhcp | ndp] | security-level [glean | guard | inspect]| tracking [disable | enable]| trusted-port}**	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**data-glean**：データ アドレス グリーニングをイネーブルにします。このオプションは、デフォルトでディセーブルになっています。 • （任意）**default**：すべてのデフォルト オプションを設定します。 • （任意）**device-role [node | switch]**：ポートに接続されたデバイスのロールを認定します。 • （任意）**limit {address-count** *value*}：ターゲット当たりに許可されるアドレスの数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol [all | dhcp | ndp]**：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは **all** です。デフォルトを変更するには、**no protocol** コマンドを使用します。 • （任意）**security-level [glean | guard | inspect]**：この機能によって適用されるセキュリティのレベルを指定します。 – **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 – **guard**：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これはデフォルトのオプションです。 – **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking [disable | enable]**：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。 • （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。また、テーブル内にエントリを作成しているときに衝突が発生した場合も、信頼できるポートが優先されます。
ステップ 5	**exit**	スヌーピング ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 snooping policy** *policy-name*	スヌーピング ポリシー設定を表示します。

スヌーピング ポリシーをインターフェイスまたは VLAN に適用するには、次の手順を実行します。

	アクションまたはコマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	アクションまたはコマンド	目的
ステップ 3	**interface** *type number*	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** **ipv6 snooping attach-policy** *policy-name* または **vlan configuration** *vlan list* **ipv6 snooping attach-policy** *policy-name*	スヌーピング ポリシー（データ グリーニングがイネーブル）をインターフェイスに適用します。ポートと、そのポートに適用されるポリシーを指定します。 （注）　スヌーピング ポリシーで **data-glean** をイネーブルにした場合は、そのポリシーを VLAN ではなく、インターフェイスに適用する必要があります。
ステップ 5	**show ipv6 snooping policy** *policy-name*	スヌーピング ポリシー設定を表示します。
ステップ 6	**show ipv6 neighbors binding**	スヌーピング ポリシーによって入力されたバインディング テーブル エントリを表示します。

IPv6 DHCP ガードの設定

	アクションまたはコマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp guard policy** *policy-name*	グローバル コンフィギュレーション モードでポリシーを作成し、DHCP ガード ポリシー グローバル コンフィギュレーション モードを開始します。
ステップ 4	[**default** | **device-role** [**client** | **server**] | **no** | **exit** | **trusted-port**]	DHCP ガード ポリシーのパラメータを設定します。 • （任意）**default**：コマンドをそのデフォルトに設定します。 • （任意）**device-role** [**client** | **server**]：ポートに接続されたデバイスのロールを認定します。 – **client**：適用されたデバイスがクライアントであることを指定します。これはデフォルトです。このポートでは、すべてのサーバ メッセージがドロップされます。 – **server**：適用されたデバイスが DHCP サーバであることを指定します。このポートでは、サーバ メッセージが許可されます。 • （任意）**no**：設定されたポリシー パラメータを削除します。 • （任意）**exit**：DHCP ガード ポリシー グローバル コンフィギュレーション モードを終了します。 • （任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。 （注）　信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 5	**exit**	DHCP ガード ポリシー グローバル コンフィギュレーション モードを終了します。

	アクションまたはコマンド	目的
ステップ 6	**interface** *type number*	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ipv6 dhcp guard attach-policy** *policy-name* または **vlan configuration** *vlan-id*	DHCP ガード ポリシーをインターフェイスまたは VLAN に適用します。
ステップ 8	**show ipv6 dhcp guard policy** *policy-name*	DHCP ガード ポリシー設定を表示します。

IPv6 ソース ガードの設定

	アクションまたはコマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *policy-name*	ソース ガード ポリシー名を指定し、ソース ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**permit link-local**	リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。
ステップ 5	**deny global-autoconf**	自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられているときに、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。
ステップ 6	**ipv6 source-guard** [**attach-policy** *policy-name*]	ポリシー名を指定します。 （任意）**attach-policy** *policy-name*：ポリシー名に基づいてフィルタリングします。
ステップ 7	**exit**	ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 8	**show ipv6 source-guard policy** *policy name*	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 でファーストホップ セキュリティを実装する場合の設定例

次に、スヌーピング ポリシーを VLAN に適用する例と、信頼できる RA ルータ ポートおよび信頼できる DHCP サーバ ポートを設定する例を示します。

```
Switch(config)# vlan configuration 100
Switch(config-vlan-config)# ipv6 snooping
Switch(config-vlan-config)# exit

Switch(config)# ipv6 nd raguard policy router
Switch(config-nd-raguard)# device-role router
Switch(config-nd-raguard)# exit

Switch(config)# ipv6 dhcp guard policy server
```

```
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)# exit
```

ここで、2/1/2 はルータ側のポートです。

```
Switch(config)# interface fastethernet 2/1/2
Switch(config-if)# switchport
Switch(config-if)# swithport access vlan 100
Switch(config-if)# ipv6 nd raguard attach-policy router
Switch(config-if)# exit
```

ここで、1/0/17 は DHCP サーバ側のポートです。

```
Switch(config)# interface gigabitethernet 1/0/17
Switch(config-if)# switchport access vlan 100
Switch(config-if)# ipv6 dhcp guard attach-policy server
Switch(config-if)# exit
Switch(config)# exit

Switch# show ipv6 snooping policies
Target               Type  Policy              Feature        Target range
Gi1/0/17             PORT  server              DHCP Guard     vlan all
Te2/1/2              PORT  router              RA guard       vlan all
vlan 100             VLAN  default             Snooping       vlan all
```

次に、*Test* という名前のスヌーピング ポリシーを作成し、そのポリシーでデータ アドレス グリーニングをイネーブルにする例を示します。

```
Switch(config)# ipv6 snooping policy Test
Switch(config-ipv6-snooping)# data-glean
Switch(config-ipv6-snooping)# device-role node
Switch(config-ipv6-snooping)# limit address-count 1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)# security-level glean
Switch(config-ipv6-snooping)# tracking enable
Switch(config-ipv6-snooping)# no trusted-port
Switch(config-ipv6-snooping)# exit
```

次に、スヌーピング ポリシー *Test* を設定し、そのポリシーでデータ アドレス グリーニングをイネーブルにした後、リンクローカル アドレスが許可され、グローバルな自動設定アドレスが拒否されるソース ガードをイネーブルにする例を示します。

```
Switch(config)# ipv6 snooping policy Test
Switch(config-ipv6-snooping)# data-glean
Switch(config-ipv6-snooping)# exit
Switch(config)# ipv6 source-guard policy Test
Switch(config-sisf-sourceguard)# permit link-local
Switch(config-sisf-sourceguard)# deny global-autoconf
Switch(config-sisf-sourceguard)# exit
```

次に、ソース ガードを含むスヌーピング ポリシーをインターフェイスに適用する例を示します。

```
Switch(config)# interface gigabitethernet2/0/3
Switch(config-if)# ipv6 snooping attach-policy Test
Switch(config-if)# ipv6 source-guard attach-policy Test

Switch# show ipv6 source-guard policy Test
Policy Test configuration:
    permit link-local
    deny global-autoconf
Policy Test is applied on the following targets:
    Target  Type  Policy Feature      Target range
    Gi2/0/3 PORT  Test   Source guard vlan all
```

次に、DHCP ガード ポリシー *Test* を設定し、それをインターフェイスに適用する例を示します。

```
Switch(config)# ipv6 dhcp-guard policy Test
Switch(config-dhcp-guard)# no trusted-port
Switch(config-dhcp-guard)# exit

Switch(config)# interface gigabitethernet2/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy Test
Switch(config-if)# exit
または
Switch(config)# vlan configuration 1-10
Switch(config-vlan-config)# ipv6 dhcp guard attach-policy Test
Switch(config-vlan-config)# exit

Switch# show ipv6 dhcp-guard policy Test
Dhcp guard policy: Test
Device Role: dhcp server
Target: Gi2/0/3 vlan 1 vlan 2 vlan 3 vlan 4 vlan 5 vlan 6 vlan 7 vlan 8 vlan 9 vlan 10
Max Preference: 255
Min Preference: 0
```

次に、スヌーピング ポリシーを作成しないで、インターフェイスまたは VLAN で FHS 機能をイネーブルにする例を示します。

（注） ポリシーを作成すると、ニーズに応じて設定する柔軟性が得られます。ポリシーを作成せずにこの機能をイネーブルにした場合は、デフォルトのポリシー設定が適用されます。

```
Switch(config)# interface GigabitEthernet1/0/9
Switch(config-if)# ipv6 nd inspection
Switch(config-if)# ipv6 nd raguard
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 dhcp guard
Switch(config-if)# ipv6 source-guard
Switch(config-if)# end
```

または

```
Switch(config)# vlan configuration 1
Switch(config-vlan-config)# ipv6 nd inspection
Switch(config-vlan-config)# ipv6 nd raguard
Switch(config-vlan-config)# ipv6 dhcp guard
Switch(config-vlan-config)# ipv6 snooping
```

（注） ソース ガード ポリシーを VLAN に適用することはできません。

この他の例については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Configuration Examples for Implementing First Hop Security in IPv6」を参照してください。

DRP の設定

Router Advertisement（RA; ルータ アドバタイズメント）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**}	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 DRP をディセーブルにするには、**no ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上のルータに*高い* DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv4 および IPv6 プロトコル スタックの設定

IPv6 ルーティングを設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。まだ設定していない場合、**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} [**desktop**] グローバル コンフィギュレーション コマンドを使用して IPv6 をサポートするテンプレートを設定します。新規テンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	スイッチ上でルーティングをイネーブルに設定します。
ステップ 3	**ipv6 unicast-routing**	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 6	**ip address** *ip-address mask* [**secondary**]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address* **link-local** または **ipv6 enable**	グローバルな IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクローカルなアドレスでなく、インターフェイス上の特定の、リンクローカルなアドレスを使用するように指定します。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show interface** *interface-id* **show ip interface** *interface-id* **show ipv6 interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv4 ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。IPv6 ルーティングをディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。インターフェイスから IPv4 アドレスを削除するには、**no ip address** *ip-address mask* インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6**

address インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

DHCP for IPv6 アドレス割り当ての設定

ここでは、IPv6 DHCP（DHCPv6）アドレス割り当ての設定方法について説明します。

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- DHCPv6 を設定する場合は、事前に IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。
ステップ 3	**address prefix** *IPv6-prefix* **lifetime** *{t1 t1* | **infinite***}*	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効ステートを維持するタイム インターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address** *IPv6-prefix*	（任意）リンクアドレスの IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
ステップ 5	**vendor-specific** *vendor-id*	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を入力します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption** *number {***address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string}*	（任意）*ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。*
ステップ 7	**exit**	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 10	**ipv6 dhcp server** [*poolname* | **automatic***]* *[***rapid-commit***]* *[***preference** *value]* *[***allow-hint***]*	インターフェイスで DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前 プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。 • **automatic**：（任意）システムが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージの交換方法を許可します。 • **preference** *value*：（任意）サーバによって送信されるアドバタイズメント メッセージ内のプリファレンス オプションで指定されるプリファレンス値 有効な範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバが、SOLICIT メッセージ内のクライアントからの指示を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 dhcp pool** または **show ipv6 dhcp interface**	DHCPv6 プール設定を確認します。 DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool** *poolname* グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで DHCPv6 クライアント機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**]	インターフェイスで、DHCPv6 サーバから IPv6 アドレスを取得するようにします。 **rapid-commit**：（任意）アドレス割り当てで、2 つのメッセージの交換方法を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**]	（任意）インターフェイスでベンダー固有のオプションを要求するようにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 dhcp interface**	DHCPv6 クライアント機能がインターフェイス上でイネーブルであることを確認します。

DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除にするには、**no ipv6 address dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*]	IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定します。 • *interval :* バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*]	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ipv6 icmp error-interval** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 の CEF の設定

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は、ネットワーク パフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。IPv6 CEF はデフォルトでディセーブルになっていますが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケット フォワーディングをグローバルに設定する必要があります。そして、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

IPv6 CEF をディセーブルにするには、**no ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。IPv6 CEF または dCEF をディセーブルにした後に再びイネーブルにするには、**ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。IPv6 ステートを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

CEF および dCEF の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルートの設定

スタティック IPv6 ルートを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*]	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */prefix length*：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 **（注）** リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります（リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**] または **show ipv6 route static** [*updated*]	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 • **interface** *interface-id*：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。 • **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。 • **detail**：（任意）次に示す追加情報を表示します。 – 有効な再帰ルートの場合、出力パス セットおよび最大分解深度 – 無効なルートの場合、ルートが無効な理由
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定されたスタティック ルートを削除するには、**no ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] グローバル コンフィギュレーション コマンドを使用します。

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 RIP の設定

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip** *name*	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーション モードを開始します。
ステップ 3	**maximum-paths** *number-paths*	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip** *name* **enable**	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。

	コマンド	目的
ステップ 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。 **（注）** 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：デフォルト ルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • **originate**：デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 rip** [*name*] [**database**] [**next-hops**] または **show ipv6 route rip** [*updated*]	IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをディセーブルにするには、**no ipv6 router rip** *name* グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して RIP ルーティング プロセスをディセーブルにするには、**no ipv6 rip** *name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF の設定

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- スイッチ上で IP サービス イメージが稼働している必要があります。
- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id*	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*]	（任意）エリア境界でルートを統合し、サマライズします。 • *area-id*：ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefix length*：宛先 IPv6 ネットワーク、およびプレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost** *cost*：（任意）現在のサマリー ルートのメトリックまたはコスト。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths** *number-paths*	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 64 で、デフォルトは 16 です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]	インターフェイス上で IPv6 OSPF をイネーブルにします。 **instance** *instance-id*：（任意）インスタンス ID
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*] または **show ipv6 ospf** [*process-id*] [*area-id*]	OSPF インターフェイスの情報を表示します。 OSPF ルーティング プロセスに関する一般的な情報を表示します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスをディセーブルするには、no **ipv6 router ospf** *process-id* グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf** *process-id* **area** *area-id* インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整

特権 EXEC モードから LSA および SPF タイマーを調整するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospfv3** [*process-id*]	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 3	**timers lsa arrival** *milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 4	**timers pacing flood** *milliseconds*	LSA フラッド パケット ペーシングを設定します。
ステップ 5	**timers pacing lsa-group** *seconds*	OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。
ステップ 6	**timers pacing retransmission** *milliseconds*	IPv4 OSPFv3 での LSA 再送信パケット ペーシングを設定します。

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

特権 EXEC モードから LSA および SPF スロットリングを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id*	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 3	**timers throttle spf** *spf-start spf-hold spf-max-wait*	SPF スロットリングをオンにします。
ステップ 4	**timers throttle lsa** *start-interval hold-interval max-interval*	OSPFv3 LSA 生成に対するレート制限値を設定します。

	コマンド	目的
ステップ 5	**timers lsa arrival** *milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 6	**timers pacing flood** *milliseconds*	LSA フラッド パケット ペーシングを設定します。

イベント ロギングのイネーブル化の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Enabling Event Logging for LSA and SPF Rate Limiting」および「Verifying OSPFv3 Configuration and Operation」の章を参照してください。

OSPFv3 での IPSec の設定

（注）　認証および暗号化をイネーブルにするには、OSPFv3 で IP Security（IPSec）セキュア ソケットのアプリケーション プログラム インターフェイス（API）を設定します。

IPSec の設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の次の章を参照してください。

- インターフェイスでの認証の定義
- インターフェイスでの暗号化の定義
- OSPFv3 エリア内の認証の定義
- OSPFv3 エリア内の暗号化の定義
- OSPFv3 エリア内の仮想リンクに対する認証および暗号化の定義
- OSPFv3 の設定と動作の確認

IPv6 の EIGRP の設定

EIGRP IPv6 をイネーブルにするには、インターフェイスで **ipv6 router eigrp** *as-number* コマンドおよび **ipv6 eigrp** *as-number* コマンドを設定します。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**eigrp router-id** *ip-address* コマンドを使用します。

スイッチ上で IP サービス イメージが稼働している必要があります。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv4 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface default** コマンドを使用して、すべてのインターフェイスをパッシブに設定してから、選択されたインターフェイスで **no passive-interface** コマンドを使用し、これらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、『*Cisco IOS IPv6 Configuration Guide*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の HSRP の設定

IPv6 の HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。

スイッチで IPv6 の HSRP がイネーブルである場合、IPv6 ホストは IPv6 ネイバー探索ルータのアドバタイズメント メッセージから使用可能な IPv6 ルータを学習します。HSRP IPv6 グループには、HSRP グループ番号に基づいて作成される仮想 MAC アドレスがあります。グループには、デフォルトで、HSRP 仮想 MAC アドレスに基づいて作成される仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。

スイッチ上で IP サービス イメージが稼働している必要があります。

IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

HSRPv1 および HSRPv2 を使用して IPv6 の HSRP を設定する場合の設定に関する注意事項については、「HSRP 設定時の注意事項」（P.43-6）および「HSRP のトラブルシューティング」（P.43-13）を参照してください。

IPv6 の HSRP および HSRPv2 の詳細については、第 43 章「HSRP および VRRP の設定」を参照してください。

（注）　IPv6 の HSRP グループを設定する前に、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 の HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

レイヤ 3 インターフェイス上で HSRPv2 をイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始して、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version** {**1** | **2**}	HSRP バージョンを変更するには、**2** を入力します。デフォルトは 1 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show standby**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の HSRP グループのイネーブル化

レイヤ 3 インターフェイス上で IPv6 の HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、IPv6 の HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}	IPv6 の HSRP グループを作成、（またはイネーブルに）する • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 4095 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • ホット スタンバイ ルータ インターフェイスのリンクローカル アドレスを入力するか、リンクローカル プレフィックスおよび変更された EUI-64 形式のインターフェイス ID から自動的に生成されるリンクローカル アドレスをイネーブルにします。この場合、EUI-64 インターフェイス ID は、関連する HSRP 仮想 MAC アドレスから作成されます。
ステップ 4	**standby** [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 • （任意）**delay**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒です（1 時間）。デフォルトは 0 です（引き継ぐまで遅延がない）。 • （任意）**reload**：リロード後のプリエンプション遅延（秒）を設定します。遅延時間は、ルータのリロード後の最初のインターフェイスアップ イベントに対してだけ適用されます。 • （任意）**sync**：IP 冗長クライアントの最大同期化時間（秒）を設定します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** [*group-number*] **priority** *priority*	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show standby** [*interface-id* [*group-number*]]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の HSRP をディセーブルにするには、**no standby** [*group-number*] **ipv6** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのグループ 1 で IPv6 の HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、IPv6 の HSRP を使用して学習されます。

（注）　これは、IPv6 の HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

IPv6 の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 40-2 に、スイッチ上で IPv6 をモニタするための特権 EXEC コマンドを示します。

表 40-2　IPv6 のモニタリング用コマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 CEF を表示します。
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスおよび設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 40-3 に、EIGRP IPv6 情報を表示するための特権 EXEC コマンドを示します。

表 40-3　EIGRP IPv6 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。
show ipv6 eigrp [*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。
show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 40-4 に、IPv4 および IPv6 のアドレス タイプに関する情報を表示するための特権 EXEC コマンドを示します。

表 40-4　IPv4 および IPv6 のアドレス タイプの表示用コマンド

コマンド	目的
show ip http server history	アクセスした IP アドレス、接続が終了したときの時間を含む、最近 20 回の HTTP サーバへの接続を表示します。
show ip http server connection	アクセスしているローカルおよびリモート IP アドレスを含む、HTTP サーバへの現在の接続を表示します。
show ip http client connection	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
show ip http client history	サーバに対して HTTP クライアントが行った最後の 20 回の要求のリストを表示します。

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

次に、**show ipv6 cef** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
```

```
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to FastEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to FastEthernet2/0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
  attached to Loopback10

3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<output truncated>
```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is “connected”
IPv6 Routing Protocol is “static”
IPv6 Routing Protocol is “rip fer”
  Interfaces:
    Vlan6
    FastEthernet0/4
    FastEthernet0/11
    FastEthernet0/12
Redistribution:
    None
```

次に、**show ipv6 rip** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
     Administrative distance is 120.Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
    なし
```

次に、**show ipv6 static** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1
```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 neighbors
IPv6 Address                                Age Link-layer Addr State Interface
3FFE:C000:0:7::777                            - 0007.0007.0007  REACH Vl7
3FFE:C101:113:1::33                           - 0000.0000.0033  REACH Fa1/0/13
```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L   FF00::/8 [0/0]
     via Null0, receive
```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  36861 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
         0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```