CHAPTER 36

IPv6 ホスト機能の設定

この章では、Catalyst 2960、2960-S、または 2960-C スイッチの IPv6 ホスト機能を設定する方法について説明します。

IPv6 Multicast Listener Discovery（MLD）スヌーピングの設定の詳細については、第 37 章「IPv6 MLD スヌーピングの設定」を参照してください。

Catalyst 2960 スイッチで（IPv4 と IPv6 の両方をサポートする）デュアル スタック環境をイネーブルにするには、デュアル IPv4 および IPv6 スイッチ データベース管理（SDM）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.36-9）を参照してください。このテンプレートは、Catalyst 2960-S スイッチではサポートされません。

（注） 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 形式のアドレス」（P.36-2）
- 「サポート対象の IPv6 ホスト機能」（P.36-2）
- 「IPv6 とスイッチ スタック」（P.36-11）

IPv6 形式のアドレス

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 フォーマット、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 の『*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」の章にある次の項の内容は、Catalyst 2960、2960-S、または 2960-C スイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレスの出力表示
- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ホスト機能

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。

- 「128 ビット幅のユニキャスト アドレス」（P.36-3）
- 「IPv6 の DNS」（P.36-3）
- 「ICMPv6」（P.36-3）
- 「ネイバー探索」（P.36-4）
- 「IPv6 でのファーストホップ セキュリティ」（P.36-4）
- 「IPv6 のステートレス自動設定および重複アドレス検出」（P.36-8）
- 「IPv6 アプリケーション」（P.36-9）
- 「デュアル IPv4/IPv6 プロトコル スタック」（P.36-9）
- 「OSPFv3 での IPSec の設定 IPv6 による SNMP および Syslog」（P.36-10）
- 「IPv6 による HTTP（S）」（P.36-10）

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。

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。ネイバー探索プロトコル（NDP）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 の『*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、ドメイン ネーム システム（DNS）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。

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 ネイバー探索プロセスは 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.36-5）
- 「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.36-5）
- 「NDP アドレス グリーニング」（P.36-5）
- 「IPv6 DHCP アドレス グリーニング」（P.36-5）
- 「IPv6 DHCP アドレス グリーニング」（P.36-5）
- 「IPv6 ND 検査」（P.36-7）
- 「IPv6 デバイス トラッキング」（P.36-7）
- 「IPv6 ポートベースのアクセス リスト サポート」（P.36-7）
- 「IPv6 ルータ アドバタイズメント ガード」（P.36-7）
- 「IPv6 デバイス トラッキング」（P.36-7）
- 「IPv6 ソース ガード」（P.36-8）

（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 の『*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。
- Catalyst 2960-S LAN Lite イメージは、IPv6 RA ガードのみをサポートしています。さらに、スイッチで IPv6 ACL がサポートされていないため、RA ガード ポリシーに IPv6 ACL を付加できません。
- ファーストホップ セキュリティは、Catalyst 2960-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.36-14）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.36-5）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.36-5）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.36-5）を参照してください。

NDP アドレス グリーニング

NDP アドレス グリーニング機能は、**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）アドレスが既知であり、そのアドレスを確認するために L2 および L3 宛先に重複アドレス検出（DAD）ネイバー送信要求（NS）ユニキャストが送信されます。
  - 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.36-14）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.36-8）および「IPv6 DHCP ガードの設定」（P.36-15）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。

ポートが、バインディングが不明なデータ パケットを受信した場合、つまり、ネイバーが INCOMPLETE ステートにあり、リンク層アドレスがまだ不明な場合、スイッチはそのデータ パケットが受信された元のポートに DAD NS NDP ユニキャスト メッセージを送信します。

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 ガード

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 ガード機能は、ホストが無効な IPv6 送信元アドレスを含むパケットを送信しないように、IPv6 バインディング テーブルを使用して PACL をインストールする機能を提供します。

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。

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 の『*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、および Telnet
- IPv6 トランスポートによるセキュア シェル（SSH）
- 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

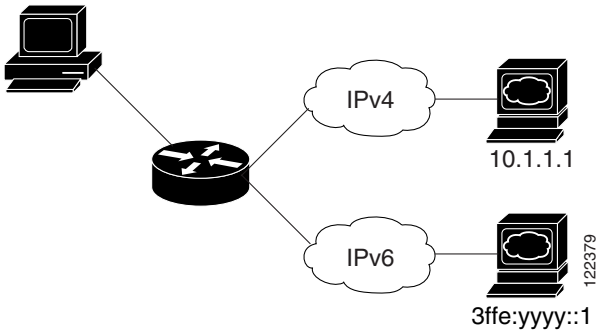
これらのアプリケーションの管理の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

Catalyst 2960 スイッチで、IPv4 および IPv6 プロトコルの両方で Ternary Content Addressable Memory（TCAM）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 36-1 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 36-1　インターフェイス上での IPv4/IPv6 のデュアル サポート



Catalyst 2960 スイッチでデュアル IPv4/IPv6 スイッチング データベース管理（SDM）テンプレートを使用すると、（IPv4 と IPv6 の両方をサポートする）デュアル スタック環境をイネーブルにできます。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。

Catalyst 2960 スイッチで IPv4/IPv6 テンプレートを使用することにより、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 専用環境で、スイッチは Ipv4 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 環境で、スイッチは IPv4 QoS および ACL をハードウェアで適用します。
- IPv6 QoS および ACL 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 スタックの詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

OSPFv3 での IPSec の設定 IPv6 による 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 による SNMP については、Cisco.com から『*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 の『*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 の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

IPv6 とスイッチ スタック

スイッチにより、スタック全体で IPv6 転送がサポートされ、スタック マスターで IPv6 ホスト機能がサポートされます。スタック マスターにより、IPv6 ホスト機能および IPv6 アプリケーションが実行されます。

新しいスタック マスターが選択中およびリセット中の間には、スイッチ スタックによる IPv6 パケットの転送は行われません。スタック MAC アドレスが変更され、これによって IPv6 アドレスが変更されます。**ipv6 address** *ipv6-prefix/prefix length* **eui-64** 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、拡張固有識別子（EUI）でスタック IPv6 アドレスを指定する場合、アドレスは、インターフェイス MAC アドレスに基づきます。「IPv6 アドレス指定の設定および IPv6 ホスト のイネーブル化」（P.36-11）を参照してください。

スタック上で永続的な MAC アドレスを設定し、スタック マスターが変更された場合、スタック MAC アドレスは、約 4 分間、変更されません。詳細については、第 7 章「スイッチ スタックの管理」の「永続的 MAC アドレスのイネーブル化」（P.7-19）を参照してください。

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 36-1 に IPv6 のデフォルト設定を示します。

表 36-1　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 アドレス	未設定

IPv6 アドレス指定の設定および IPv6 ホスト 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。
- **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 の設定の詳細については、Cisco.com の『*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 転送をイネーブルにするは、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**	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。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**reload**	OS（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、設定するインターフェイスを指定します。
ステップ 7	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **ipv6 address** *ipv6-address/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 ビットの拡張固有識別子（EUI）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 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	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show ipv6 interface** *interface-id*	入力内容を確認します。
ステップ 11	**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)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/1
GigabitEthernet1/0/1 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

	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。
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、デフォルトで無効です。 • （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。これが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。
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。

	アクションまたはコマンド	目的
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。
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。

	アクションまたはコマンド	目的
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ための設定例

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、ポリシーを作成せずに、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。

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*]	入力内容を確認します。
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 のスタティック ルートの設定

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 の『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for 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 36-2 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 36-2　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 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 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 route	IPv6 ルート テーブル エントリを表示します。
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 36-3 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 36-3　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 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
   GigabitEthernet2/0/4
    GigabitEthernet2/0/
    GigabitEthernet1/0/12
Redistribution:
    None
```

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
```