



IPv6 ユニキャスト ルーティングの設定

インターネットプロトコルバージョン 6 (IPv6) は、TCP/IP プロトコルスイートで IP Version 4 (IPv4) を置き換えることを意図したネットワーク層インターネットプロトコルです。この章では、Catalyst 3560 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。IPv4 ユニキャスト ルーティングの設定については、第 34 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。IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、第 36 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 37 章「[IPv6 ACL の設定](#)」を参照してください。

この機能を使用するには、スイッチ上で拡張 IP サービス イメージ (シスコに発注可能) が稼働している必要があります。このイメージには、すべての IP サービス イメージ (以前の拡張マルチレイヤ イメージ [EMI]) 機能に加え、IPv6 ホストおよびユニキャスト ルーティングのサポートが含まれています。IPv6 ルーティングをイネーブルにするには、スイッチ データベース管理 (SDM) デュアル IPv4/IPv6 テンプレートも設定する必要があります。「[SDM テンプレート](#)」(P.35-8) を参照してください。



(注) この章で説明するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は、次のとおりです。

- 「[IPv6 の概要](#)」 (P.35-1)
- 「[IPv6 の設定](#)」 (P.35-9)
- 「[IPv6 の表示](#)」 (P.35-21)

IPv6 の概要

IPv6 を使用する主な目的は、ユーザ数および一意なグローバル IP アドレスを必要とするアプリケーションの急激な増加に対応できるように、インターネット グローバル アドレス空間を拡張することです。IPv4 は 32 ビット アドレスを使用して、約 40 億の使用可能アドレスを提供します。これらのアドレスの大部分は政府機関や大規模な組織に割り当てられていて、使用可能な IP アドレス数が急速に減少しています。IPv6 は 128 ビットの送信元および宛先アドレスを使用しているため、グローバルに一意な IP アドレスを IPv4 よりもはるかに多く提供できます。

IPv6 のアーキテクチャを使用すると、既存の IPv4 ユーザは IPv6 に簡単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)、グローバルに一意的なアドレスなどのサービスを利用できます。IPv6 アドレス空間は柔軟であるため、プライベートアドレスの必要性が減少し、ネットワーク エッジ上の境界ルータでネットワーク アドレス変換 (NAT) 処理を使用する必要がなくなります。IPv6 では、より新しいユニキャスト方式が採用されています。IP アドレスに 16 進値が導入され、デリミタとしてピリオド (.) でなくコロン (:) が使用されます。

IPv6 には、IPv4 と比べて次の利点もあります。

- アドレスの管理および委任が容易
- ステートレス自動設定 (Dynamic Host Configuration Protocol [DHCP] と似ているが、指定された DHCP アプリケーションまたはサーバが不要) によるアドレス自動設定が容易
- IPSec (暗号化セキュリティ) 内蔵
- モバイル デバイス向けに最適化されたルーティング
- Duplicate Address Detection (DAD) 機能

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/warp/public/732/Tech/ipv6/>

ここでは、スイッチへの IPv6 の実装について説明します。内容は次のとおりです。

- 「IPv6 形式のアドレス」(P.35-2)
- 「サポート対象の IPv6 ユニキャストルーティング機能」(P.35-3)
- 「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.35-6)
- 「制限事項」(P.35-7)
- 「SDM テンプレート」(P.35-8)

IPv6 形式のアドレス

IPv6 はユニキャスト (1 対 1)、マルチキャスト (1 対多)、およびエニキャスト (1 対最近接) の 3 つのアドレス タイプをサポートします。マルチキャスト アドレスは、ブロードキャスト アドレスの代わりに使用されます。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。

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 (x:x:x:x:x:x:x 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、次の URL にある「Implementing Basic Connectivity for IPv6」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

「Information About Implementing Basic Connectivity for IPv6」の、次の項の内容が Catalyst 3560 スイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：ユニキャスト
- IPv6 アドレスの出力表示
- 簡易 IPv6 パケット ヘッダー

このリリースでは、スイッチはサイトローカルなユニキャスト アドレス、ユニキャスト 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。

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 (RFC 2460) 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.35-3)
- 「IPv6 ユニキャストのパス MTU ディスカバリ」(P.35-4)
- 「ICMPv6」(P.35-4)
- 「IPv6 ステートレス自動設定および重複アドレス検出」(P.35-5)
- 「IPv6 アプリケーション」(P.35-5)
- 「IPv4 と IPv6 の二重プロトコル スタック」(P.35-6)

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。

スイッチでは、スタティック ルート用のネイティブ形式のイーサネット スイッチ間リンク (ISL) または 802.1Q トランク ポート、IPv6 (RFC 2080) 用の Routing Information Protocol (RIP)、および Open Shortest Path First (OSPF) バージョン 3 プロトコル (RFC 2740) の IPv6 ルーティング機能が提供されています。最大 16 の等コストのルートをサポートし、IPv4 および IPv6 フレームを同時にラインレートで転送できます。

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 (RFC 2373)。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 Universal 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。リンクローカルアドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。ローカルリンク上のノードは、リンク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、グローバルに一意的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。

次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing Basis Connectivity for IPv6」の章にある「IPv6 Unicast Addresses」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

各 IPv6 ホスト インターフェイスは、ハードウェア内で最大 3 つのアドレスをサポートできます (集約可能なグローバルユニキャストアドレスを 1 つ、リンクに対してローカルなユニキャストアドレスを 1 つ、およびプライベートアドレスをゼロ個以上)。

IPv6 の DNS

IPv6 には、Domain Name System (DNS; ドメインネームシステム) の名前/アドレスおよびアドレス/名前の検索プロセスをサポートする新しい DNS レコードタイプが導入されています。新しい 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、IPv6 ノードへのシステム MTU 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 (RFC 1981) を使用すると、ホストは、特定のデータパスに沿ったすべてのリンクの MTU サイズの差を動的に検出して適応できます。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) (RFC 2463) 機能は、IPv4 と同じです。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。基本的な IPv6 パケットヘッダーの Next Header フィールド値が 58 の場合は、IPv6 ICMP パケットであることを意味します。

スイッチはまた、ICMPv6 の上で稼働するプロトコルである IPv6 対応のネイバー探索プロトコル (NDP) (RFC 2461) や、NDP をサポートしない IPv6 ステーションのための Static Neighbor Discovery もサポートします。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。

ICMP パケットヘッダーのタイプフィールドの値 135 は、ネイバー送信要求メッセージを示します。ノードが同じローカルリンク上の別のノードのリンク層アドレスを判別する必要がある場合は、ローカルリンク上でこれらのメッセージが送信されます。ネイバー送信請求メッセージを受信した宛先ノードは、ICMP パケットヘッダーの Type フィールド値が 136 のネイバーアドバタイズメントメッセージを送信して、応答します。

ICMP パケットヘッダーの Type フィールド値が 137 の場合は、IPv6 ネイバーリダイレクトメッセージであることを意味します。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

(RFC 2463) をサポートしています。マスク長が 64 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。宛先へのパス上にさらに適した先頭ホップ ノードが存在することをホストに通知する場合、ルータはネイバー リダイレクト メッセージを送信します。ルータがネイバー リダイレクト メッセージを受信しても、ルーティング テーブルは更新されず、ホストはネイバー リダイレクト メッセージを送信しません。

IPv6 ステートレス自動設定および重複アドレス検出

IPv6 は 2 つのタイプの自動設定をサポートします。

- ステートレス自動設定 (RFC 2462) : 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。
- ステートフル自動設定 : DHCP バージョン 6 を使用します。

スイッチではステートレス自動設定がサポートされているため、ホストやモバイル IP アドレスの管理など、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。

IPv6 ノードのすべてのインターフェイスには、インターフェイス ID (ルータの MAC アドレス) およびリンクに対してローカルなプレフィックス FE80::/10 に基づいて自動設定された、リンクに対してローカルなアドレスが必要です。リンクローカルアドレスを使用すると、ノードがリンク上の他のノードと通信できます。また、リンクローカルアドレスを使用して、ノードをさらに設定することもできます。手動設定を行ったり、DHCP サーバなどのサーバを利用したりしなくても、ノードをネットワークに接続して、グローバルな IPv6 アドレスを自動的に生成することができます。IPv6 の場合、リンク上のルータはルータ アドバタイズメント メッセージを使用して、グローバルプレフィックス、およびリンクのデフォルト ルータとして動作するための機能をアドバタイズします。リンク上のノードがグローバル IPv6 アドレスの自動設定できるようにするには、ルータ アドバタイズメント メッセージ内のプレフィックス (64 ビット) にインターフェイス ID (64 ビット) を付加します。

ノードによって設定された 128 ビット IPv6 アドレスには、リンク上で一意であることを確認するための重複アドレス検出 (RFC 2462) が実行されます。アドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスはグローバルに一意であることが保証されます。システムが起動すると、ホストから、ICMP パケット ヘッダーの Type フィールド値が 133 であるルータ送信請求メッセージが送信されます。これにより、スケジューリングされた次のルータ アドバタイズメント メッセージを待機しなくても、ホストを即座に自動設定することができます。IPv6 重複アドレス検出は、ユニキャストアドレスがインターフェイスに割り当てられる前に実行されます。自動生成された、サイトに対してローカルな IPv6 アドレスは、スイッチではサポートされません。

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、TFTP、および FTP
- 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

Cisco IOS を使用したこれらのアプリケーションの管理の詳細については、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/ipv6_c/sa_mgev6.htm

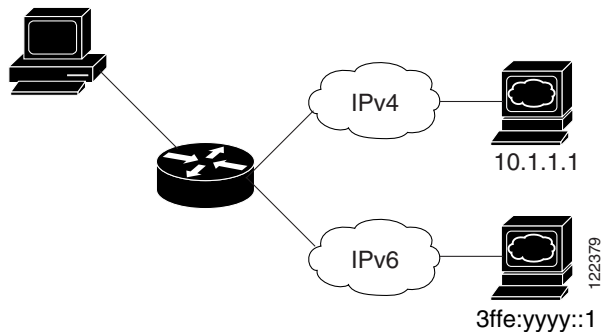
IPv4 と IPv6 の二重プロトコル スタック

IPv6 に移行する方法の 1 つは、デュアル IPv4/IPv6 プロトコル スタックを使用することです。デュアル スタックを使用すると、ノードで稼働中のアプリケーションに緩やかな段階的アップグレードを行うことができます。IPv6 にアップグレードされたアプリケーションは、IPv6 プロトコル スタックを使用します。アップグレードされていない、IPv4 のみをサポートするアプリケーションと、アップグレード済みアプリケーションを、同じノード上で共存させることができます。新規のアップグレード済みアプリケーションは、IPv4 と IPv6 の両方のプロトコル スタックを使用できます。

Cisco IOS ソフトウェアは、デュアル IPv4/IPv6 プロトコル スタック方式をサポートしています。IPv4 および IPv6 ルーティングがイネーブル化されていて、インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、インターフェイスは IPv4 と IPv6 の両方のトラフィックを転送します。

図 35-1 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 35-1 インターフェイス上での IPv4/IPv6 のデュアル サポート



スイッチは Ternary CAM (TCAM) を使用して、ユニキャスト ルート、MAC (メディア アクセス コントロール) アドレス、アクセス コントロール リスト (ACL)、およびその他の機能を格納します。また、スイッチの使用方法に応じてメモリ リソースを割り当てるための Switching Database Manager (SDM; スイッチング データベース マネージャ) テンプレートを備えています。IPv4 および IPv6 プロトコルの両方で 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。「SDM テンプレート」(P.35-8) 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

このリリースでは、次の IPv6 機能はサポートされていません。

- IPv6 ポリシーベース ルーティング
- IPv6 パーチャル 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
- IPv6 経由の Web Cache Communication Protocol (WCCP)
- マルチプロトコル ボーダー ゲートウェイ プロトコル (BGP)、Intermediate System-to-Intermediate System (IS-IS) ルーティング、Enhanced Interior Gateway Routing Protocol (EIGRP) の各 IPv6 ルーティング プロトコルのサポート
- IPv6 トランスポート経由の簡易ネットワーク管理プロトコル (SNMP)
- Cisco Discovery Protocol (CDP) IPv6 アドレス ファミリのサポート
- IPv6 ホットスタンバイ ルータ プロトコル (HSRP)

- DHCPv6
- サイトローカルなアドレス宛での 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 はスイッチ内のハードウェアで実装されるため、TCAM での IPv6 圧縮アドレスの使用によるいくつかの制限が発生します。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 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 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 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 パケットを正常に転送できません。これらのパケットは、転送（ブリッジまたはルーティング）される前に破損し、破損したパケットとしてネットワークに到達します。



(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、これらのパケットはスイッチでドロップされ、破損したパケットとしては転送されません。

- 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。
- 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すると、SPAN 出力パケット内の送信元 MAC アドレスが破損する場合があります。
 - RSPAN IPv6 ルーテッドパケットを送信すると、宛先 MAC アドレスが破損する場合があります。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 分類またはポリシーベース ルーティング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。

SDM テンプレート

Catalyst 3560 スイッチには、ユニキャストルート、MAC アドレス、ACL、および他の機能を格納するための TCAM が 1 つあります。TCAM リソースをさまざまな用途に割り当てるために、スイッチ SDM テンプレートはシステム リソースにプライオリティを設定して、特定の機能のサポートを最適化します。スイッチ環境に最適なテンプレートを選択するには、**sdm prefer** グローバル コンフィギュレーション コマンドを入力します。SDM テンプレートの詳細については、第 7 章「SDM テンプレートの設定」を参照してください。

スイッチで拡張 IP サービス イメージを実行している場合、SDM テンプレートを選択して IP バージョン 6 (IPv6) をサポートすることができます。IPv4/IPv6 テンプレートを使用することにより、(IPv4 と IPv6 の両方をサポートする) 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。



(注) 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、警告メッセージが生成されます。

- 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 環境では、スイッチは IPv4 パケットと IPv6 パケットの両方をルーティングし、IPv4 QoS と ACL をハードウェアで適用します。このリリースでは、IPv6 の QoS および ACL はサポートされていません。



(注) デュアル スタック テンプレートを使用すると、リソースごとに使用可能な TCAM 容量が少なくなるため、IPv4 トラフィックだけを転送する場合は、このテンプレートを使用しないでください。

デュアル IPv4/IPv6 SDM テンプレート

次に示す SDM テンプレートは、IPv4 および IPv6 環境をサポートしています。



(注) このリリースでは、IPv6 のマルチキャスト、QoS、または ACL はサポートされていません。

- デュアル IPv4/IPv6 デフォルト テンプレート：スイッチ上で IPv4 のレイヤ 2、マルチキャスト、ルーティング、QoS、ACL、および IPv6 のレイヤ 2 とルーティングをサポートします。
- デュアル IPv4/IPv6 VLAN テンプレート：スイッチ上で IPv4 のベーシック レイヤ 2、マルチキャスト、QoS、ACL、および IPv6 のベーシック レイヤ 2 をサポートします。



(注) IPv4 ルートに必要なのは、1 つの TCAM エントリだけです。IPv6 ではハードウェア圧縮方式が使用されるため、IPv6 ルートは複数の TCAM エントリを使用することができ、ハードウェアで転送されるエントリ数が削減されます。たとえば、IPv6 によって直接接続された IP アドレスの場合、デスクトップテンプレートで使用可能なエントリ数は 2000 未満になります。

表 35-1 は、新しいテンプレートごとに割り当てられる機能リソースの概算をまとめたものです。この各テンプレートについての概数は、8 つのルーテッドインターフェイスと約 1000 の VLAN を持つスイッチに基づいて計算されています。



(注) 現在のソフトウェア リリースでは、IPv6 の QoS または ACL はサポートされていません。

表 35-1 デュアル IPv4/IPv6 テンプレートによって許容される機能リソースの概算

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 の VLAN
ユニキャスト MAC アドレス	2 K	8 K
IPv4 IGMP グループおよびマルチキャスト ルート	1 K	1 K
IPv4 ユニキャスト ルートの合計 :	3 K	0
• IPv4 ホストに直接接続	2 K	0
• 間接 IPv4 ルート	1 K	0
IPv6 マルチキャスト グループ	1 K	1 K
IPv6 ユニキャスト ルートの合計 :	3 K	0
• 直接接続された IPv6 アドレス	2 K	0
• 間接 IPv6 ユニキャスト ルート	1 K	0
IPv4 ポリシー ベース ルーティング ACE	0	0
IPv4 または MAC QoS ACE (合計)	512	512
IPv4 または MAC セキュリティの ACE (合計)	1 K	1 K
IPv6 ポリシー ベース ルーティング ACE	0	0
IPv6 QoS ACE	510	510
IPv6 セキュリティの ACE	510	510

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」(P.35-10)
- 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」(P.35-10)
- 「IPv4 および IPv6 プロトコル スタックの設定」(P.35-12)
- 「IPv6 ICMP レート制限の設定」(P.35-14)
- 「IPv6 の CEF の設定」(P.35-14)
- 「IPv6 のスタティック ルーティングの設定」(P.35-15)
- 「IPv6 RIP の設定」(P.35-17)
- 「IPv6 OSPF の設定」(P.35-19)

IPv6 のデフォルト設定

表 35-2 に IPv6 のデフォルト設定を示します。

表 35-2 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と IPv6 ルーティングのイネーブル

ここでは、個々のレイヤ 3 インターフェイスに IPv6 アドレスを割り当て、IPv6 トラフィックの転送をスイッチ上でグローバルにイネーブルにする方法について説明します。



(注)

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、*ipv6-address* および *ipv6-prefix* 変数を RFC 2373 に記載されている形式 (アドレスがコロン区切りの 16 ビット値を使用した 16 進形式で指定される) で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。

IPv6 トラフィックを転送するインターフェイスの場合は、そのインターフェイス上で IPv6 アドレスを設定する必要があります。インターフェイス上でグローバル IPv6 アドレスを設定すると、リンクローカルアドレスが自動的に設定され、そのインターフェイスに対して IPv6 がアクティブになります。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 FF02:0:0:0:1: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



(注)

スイッチ上で IPv6 を設定する前に、デュアル IPv4/IPv6 SDM テンプレートを選択するようにしてください。

IPv6 ルーティングの設定の詳細については、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing Basis Connectivity for IPv6」の章を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm



(注)

この章に記載されたすべての機能が 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.35-6) 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	<code>configure terminal</code>	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	<code>sdm prefer dual-ipv4-and-ipv6 {default vlan}</code>	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。 <ul style="list-style-type: none"> 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。 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>reload</code>	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	<code>configure terminal</code>	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 (スイッチのリロード後)。
ステップ 6	<code>interface interface-id</code>	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 Interface (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	<code>no switchport</code>	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	<code>ipv6 address ipv6-prefix/prefix length eui-64</code> または <code>ipv6 address ipv6-address link-local</code> または <code>ipv6 enable</code>	IPv6 アドレスの下位 64 ビットに Extended Universal Identifier (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	<code>exit</code>	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	<code>ip routing</code>	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。
ステップ 11	<code>ipv6 unicast-routing</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip v6 interface interface-id</code>	入力内容を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(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すために追加されています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface fastethernet0/11
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 fastethernet0/11
FastEthernet0/11 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:FE2F: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.
```

IPv4 および IPv6 プロトコル スタックの設定

インターフェイスに IPv4 と IPv6 の両方のアドレスを設定すると、そのインターフェイスは IPv4 と IPv6 の両方のトラフィックを転送し、さらに IPv4 と IPv6 の両方のネットワーク上でデータを送受信できます。

IPv4 と IPv6 の両方をサポートし、IPv6 ルーティングをイネーブルにするようにレイヤ 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。



(注)

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 | vlan}** 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。新しいテンプレートを選択する場合は、そのテンプレートを有効にするために、**reload** 特権 EXEC コマンドを使用してスイッチをリロードする必要があります。

	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 IPv4 ルーティングをイネーブルにします。
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	IPv6 アドレスの下位 64 ビットにインターフェイス ID 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	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 ip v6 interface interface-id	入力内容を確認します。
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 fastethernet0/11
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
```

IPv6 ICMP レート制限の設定

IPv6 ICMP レート制限ではトークンバケットアルゴリズムを使用して、IPv6 ICMP エラーメッセージをネットワークに送信する場合のレートを制限します。エラーメッセージの間隔は、タイムインターバルおよびバケットサイズで指定します。traceroute など一部のアプリケーションでは、一連の要求に対する応答を迅速かつ連続的に送信しなければならない場合があるため、エラーメッセージ間隔のみを指定した場合は、アプリケーションに障害が発生することがあります。トークンバケットを使用すると、エラーメッセージの送信能力をそれぞれ表す複数のトークンを仮想バケットに格納できます。メッセージを送信するたびに、バケットからトークンが 1 つ削除されます。一連のエラーメッセージが生成された場合は、バケットが空になるまでエラーメッセージを送信できます。バケットが空の場合は、新規トークンがバケットに格納されるまで、IPv6 ICMP エラーメッセージは送信されません。この方法ではレート制限間隔の平均値が大きくなり、間隔が固定されている場合よりも柔軟性が高まります。

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	<code>configure terminal</code>	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	<code>ipv6 icmp error-interval interval [bucketsize]</code>	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。 <ul style="list-style-type: none"> <code>interval</code> : 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。 <code>bucketsize</code> : (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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 interface [interface-id]</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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に使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチングルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。IPv4 CEF は、デフォルトでイネーブルに

設定されています。IPv6 CEF はデフォルトではディセーブルに設定されていますが、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 パケットの転送をグローバルに設定してから、**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、特定の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 がディセーブルになっていた場合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 ステータスを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

IPv6 のスタティック ルーティングの設定

スタティック ルートは手動で設定され、2 つのネットワーク デバイス間のルートを示的に定義します。スタティック ルートの利点は、セキュリティが高まり、リソースが効率化されることです。スタティック ルートではルートの計算や通信が不要であるため、ダイナミック ルーティング プロトコルよりも使用帯域幅が減少します。スタティック ルートの主な欠点は、ダイナミック ルーティングと異なり、自動的に更新されず、ネットワーク トポロジが変更された場合に手動再設定が必要なことです。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 ルートのタイプは、次のとおりです。

- 直接接続されたスタティック ルート：宛先は現在のインターフェイスに直接接続されていると想定されるため、出力インターフェイスのみを指定します。パケットの宛先は、ネクスト ホップ アドレスとして使用されます。直接接続されたスタティック ルートが有効なのは、指定したインターフェイスが IPv6 に対応していて、起動している場合のみです。
- 再帰スタティック ルート：ネクスト ホップのみを指定し、出力インターフェイスはネクスト ホップから取得します。再帰スタティック ルートが有効なのは、指定したネクスト ホップが有効な IPv6 出力インターフェイスであり、ルートが自己再帰型でなく、再帰深度が IPv6 転送の最大再帰深度を超えていない場合のみです。
- 完全指定のスタティック ルート：出力インターフェイスとネクスト ホップを両方とも指定します。ネクスト ホップは、指定した出力インターフェイスに直接接続されていると想定されます。完全指定のスタティック ルートが有効なのは、指定した IPv6 インターフェイスが IPv6 に対応していて、起動している場合のみです。
- フローティング スタティック ルート：上記の 3 つのスタティック ルートタイプはいずれも、フローティング スタティック ルートに設定できます。このルートは、設定済みのルーティング プロトコルを介して取得されたダイナミック ルートのバックアップに使用されます。フローティング スタティック ルートに設定されたアドミニストレーティブ ディスタンスは、バックアップしているルーティング プロトコルよりも非効率的です。したがって、トラフィックのルーティングには常に、フローティング スタティック ルートでなくダイナミック ルートが使用されます。ダイナミック ルートが失われた場合は、フローティング スタティック ルートが代わりに使用されます。



(注)

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 <code>configure terminal</code>	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 <code>ipv6 route ipv6-prefix/prefix length {ipv6-address interface-id [ipv6-address]} [administrative distance]</code>	<p>スタティック IPv6 ルートを設定します。</p> <ul style="list-style-type: none"> • <i>ipv6-prefix</i> : 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。 • <i>/prefix length</i> : 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。 • <i>ipv6-address</i> : 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 RFC 2373 に記載された形式 (16 ビット値を使用したコロン区切りの 16 進表記で指定) で設定する必要があります。 • <i>interface-id</i> : 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。 <p>(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、<i>interface-id</i> 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)。</p> <ul style="list-style-type: none"> • <i>administrative distance</i> : (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 <code>end</code>	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 [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>] [interface <i>interface-id</i>] [recursive] [detail] または show ipv6 route [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>]	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。 <ul style="list-style-type: none"> • interface <i>interface-id</i> : (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。 <ul style="list-style-type: none"> – 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、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing Static Routes for IPv6」の章を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

IPv6 RIP の設定

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 RIP は、IPv4 の RIP と同様に機能し、同じ利点を提供します。IPv6 RIP 拡張には、IPv6 アドレスとプレフィックスのサポート、および RIP アップデート メッセージの宛先アドレスとして、すべての RIP ルータのマルチキャスト グループ アドレス FF02::9 を使用することが含まれています。

各 IPv6 RIP プロセスでは、すべての隣接ネットワーク キング デバイスから学習された一連の最適コスト IPv6 ルートを格納する、Routing Information Database (RIB) と呼ばれるローカル ルーティング テーブルが保持されます。IPv6 RIP が 2 つの異なるネイバーから同じルートを学習し、それぞれのルートのコストが異なる場合、コストが最小のルートだけがローカル RIB に格納されます。RIB にはまた、RIP プロセスが RIP を実行中のネイバーにアドバタイズしている期限切れのルートもすべて格納されます。同じルートが別のルーティング プロトコルから学習されており、そのルートのアドミニストレーティブ ディスタンスが IPv6 RIP よりも優れている場合、その RIP ルートは IPv6 RIB には追加されませんが、IPv6 RIP RIB にはそのまま残ります。



(注) 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 ~ 64 であり、デフォルトは 4 パスです。
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。
ステップ 7	ipv6 rip name default-information {only originate}	<p>(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。</p> <p>(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。</p> <ul style="list-style-type: none"> • 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] [interface interface-id] [database] [next-hops] または show ipv6 route [ipv6-address ipv6-prefix/prefix length protocol]	<p>IPv6 RIP プロセスに関する情報を表示します。</p> <p>IPv6 ルーティング テーブルの現在の内容を表示します。</p>
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。

This example shows how to enable the RIP routing process `cisco`, with a maximum of eight equal-cost routes and enable it on an interface:

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet0/11
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、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing RIP for IPv6」の章を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

IPv6 OSPF の設定

Open Shortest Path First (OSPF) は、IP のリンクステート プロトコルです。つまり、ルーティングの決定は、送信元デバイスと宛先デバイスを接続するリンクのステートに基づいて行われます。リンクステートは、インターフェイスと、その隣接ネットワーク デバイスとの関係を説明するものです。リンクステート アドバタイズメント (LSA) で伝播されるインターフェイス情報には、インターフェイスの IPv6 プレフィックス、ネットワーク マスク、接続先のネットワークのタイプ、そのネットワークに接続されているルータなどが含まれています。LSA データは、OSPF ルーティング テーブルを作成するために使用されるリンクステート データベースに格納されます。このデータベースには raw データの集合が格納されるに対して、ルーティング テーブルには、特定のレイヤ 3 ポートを使用する既知の宛先への最短パスのリストが格納されます。OSPF バージョン 2 (RFC 2740) は IPv6 をサポートしています。

IPv6 OSPF は OSPF バージョン 2 (IPv4) とほぼ同じであり、IPv6 ルーティング プレフィックスと、よりサイズの大きい IPv6 アドレスのサポートを提供するように拡張されています。ただし、次の違いがあります。

- インターフェイス上で IPv6 OSPF をイネーブルにすると、ルーティング プロセスとそれに関連する設定が自動的に作成されるため、IPv4 の場合のようにルーティング プロセスを明示的に作成する必要はありません。
- IPv6 OSPF では、インターフェイス コンフィギュレーション モードでコマンドを使用して、各インターフェイスで OSPF をイネーブルにする必要があります。OSPF バージョン 2 では、インターフェイスは、ルータ コンフィギュレーション モードを使用して間接的にイネーブルになります。
- IPv6 では、1 つのインターフェイス上で多数のアドレス プレフィックスを設定できます。デフォルトでは、インターフェイス上で設定されたすべてのアドレス プレフィックスが含まれます。アドレス プレフィックスのサブセットを選択してインポートすることはできません。
- OSPF バージョン 2 とは異なり、1 つのリンクで IPv6 の複数のインスタンスを実行できます。
- OSPF バージョン 2 は、ルータ ID として使用する IPv4 アドレスを選択するために、インターフェイス上で設定された 32 ビット IPv4 アドレスを使用します。インターフェイス上で IPv6 OSPF をイネーブルにすると、そのインターフェイス上で IPv4 アドレスが設定されている場合は、その IP アドレスが IPv6 ルータ ID として使用されます。そのインターフェイス上で IPv4 アドレスが設定されていない場合は、OSFP プロセスが開始される前に、**router-id** ルータ コンフィギュレーション コマンドを使用してルータ ID を設定する必要があります。

OSPF は、ループバック インターフェイスを他のインターフェイスより優先して自動的に選択し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。ループバック インターフェイスが存在しない場合、OSPF はルータ内で最大の IP アドレスを選択します。いずれかの特定のインターフェイスを使用するように OSPF を設定することはできません。

ネットワークで IPv6 OSPF をカスタマイズすることはできますが、その必要はほとんどありません。IPv6 での OSPF のデフォルトは、ほとんどのカスタマーおよび機能の要件を満たすように設定されています。



(注)

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。



(注)

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]	<p>(任意) エリア境界でルートを統合し、サマライズします。</p> <ul style="list-style-type: none"> 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 リンクステート アドバタイズメント (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。

	コマンド	目的
ステップ7	<code>ipv6 ospf process-id area area-id [instance instance-id]</code>	インターフェイス上で IPv6 OSPF をイネーブルにします。 <ul style="list-style-type: none"> instance instance-id : (任意) インスタンス ID
ステップ8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ9	<code>show ipv6 ospf [process-id] [area-id] interface [interface-id]</code> または <code>show ipv6 ospf [process-id] [area-id]</code>	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	<code>copy running-config startup-config</code>	(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、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

IPv6 の表示

表 35-3 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 35-3 IPv6 のモニタリング用コマンド

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

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
  FastEthernet0/4
  FastEthernet0/11
  FastEthernet0/12
Redistribution:
  None

```

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 V17
3FFE:C101:113:1::33                       - 0000.0000.0033 REACH Fa1/0/13

```

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 route** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 route
IPv6 Routing Table - 21 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    ::/0 [1/0]
     via 3FFE:C000:0:7::777
C    3FFE:C000:0:1::/64 [0/0]
     via ::, Vlan1
L    3FFE:C000:0:1:20B:46FF:FE2F:D940/128 [0/0]
     via ::, Vlan1
C    3FFE:C000:0:7::/64 [0/0]
     via ::, Vlan7
L    3FFE:C000:0:7:20B:46FF:FE2F:D97F/128 [0/0]
     via ::, Vlan7
C    3FFE:C000:111:1::/64 [0/0]
     via ::, FastEthernet0/11
L    3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C    3FFE:C000:168:1::/64 [0/0]
     via ::, FastEthernet0/4
L    3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
     via ::, FastEthernet0/4
C    3FFE:C000:16A:1::/64 [0/0]
     via ::, Loopback10
L    3FFE:C000:16A:1:20B:46FF:FE2F:D900/128 [0/0]
     via ::, Loopback10

```

<output truncated>

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
      unreachable: 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
      unreachable: 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
```