



CHAPTER 37

IPv6 ユニキャスト ルーティングの設定

この章では、Cisco ME 3400E イーサネット アクセス 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の詳細については、第 36 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 Access Control List (ACL; アクセス コントロール リスト) の設定の詳細については、第 39 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、スイッチでメトロ IP アクセス イメージが稼動している必要があります。IPv6 ルーティングをイネーブルにするには、スイッチがデュアル IPv4 および 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設定する必要があります。「[デュアル IPv4 および IPv6 プロトコル スタック](#)」(P.37-5) を参照してください。



(注)

この章で使用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。

- 「[IPv6 の概要](#)」(P.37-1)
- 「[IPv6 の設定](#)」(P.37-9)
- 「[IPv6 の表示](#)」(P.37-26)

IPv6 の概要

IPv4 ユーザーが IPv6 に移行すると、エンドツーエンドセキュリティ、QoS (Quality Of Service)、およびグローバルに一意なアドレスなどのサービスを利用できます。IPv6 アドレス スペースにより、プライベート アドレス、およびネットワーク エッジの境界ルータでの Network Address Translation (NAT; ネットワーク アドレス変換) の必要性が減少します。

シスコシステムズの IPv6 実装方法の詳細については、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の詳細については、

- 次の URL から『*Cisco IOS IPv6 Configuration Guide*』にアクセスしてください。
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html
- Cisco.com の [Search] フィールドを使用し、Cisco IOS ソフトウェア マニュアルを特定します。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドに [Implementing Static Routes for IPv6] と入力すると、スタティック ルートに関する複数のマニュアルへのリンクが表示されます。

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

- 「IPv6 アドレス」(P.37-2)
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」(P.37-2)
- 「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.37-8)
- 「制限事項」(P.37-9)

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。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ていません。

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 進数フィールド (n:n:n:n:n:n:n:n 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 進数フィールドを表すことができます。ただし、この短縮形は、各アドレスで一回だけ使用できます。

```
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 の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章の、次のセクションの内容がスイッチに適用できます。

- 「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

スイッチでは、拡張アドレス機能、ヘッダー形式の単純化、拡張子およびオプションのより高度なサポート、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、ホップバイホップの拡張ヘッダー パケットもサポートしており、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、802.1Q トランク ポートによる IPv6 ルーティング (スタティック ルートの場合) 機能、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。等価コスト 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」(P.37-3)
- 「IPv6 の DNS」(P.37-4)
- 「IPv6 ユニキャストのパス MTU ディスカバリ」(P.37-4)

- 「ICMPv6」 (P.37-4)
- 「近隣探索」 (P.37-4)
- 「デフォルト ルータ プリファレンス (DRP)」 (P.37-4)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.37-5)
- 「IPv6 アプリケーション」 (P.37-5)
- 「デュアル IPv4 および IPv6 プロトコル スタック」 (P.37-5)
- 「IPv6 の DHCP アドレス割り当て」 (P.37-6)
- 「IPv6 のスタティック ルート」 (P.37-6)
- 「IPv6 の RIP」 (P.37-6)
- 「IPv6 の OSPF」 (P.37-7)
- 「EIGRP IPv6」 (P.37-7)
- 「IPv6 のマルチプロトコル BGP」 (P.37-7)
- 「IPv6 上の NMP および Syslog」 (P.37-7)
- 「IPv6 上の HTTP」 (P.37-8)

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、集約可能なグローバル ユニキャスト プレフィックスの付いた IPv6 アドレスとなります。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 アドレスの割り当てには、バイナリ値 001 (2000::

- リンク 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、リンクローカルなプレフィックス FE80::

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 アドレスについてのセクションを参照してください。

IPv6 の DNS

IPv6 では、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の DNS レコードタイプがサポートされています。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 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 Maximum Transmission Unit (MTU; システム最大伝送ユニット) の IPv6 ノードへのアダプタイズおよびパス 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 サイズの違いを動的に検出して、サイズに合わせて調整できます。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 Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) 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、近隣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。

近隣探索

スイッチは、IPv6 の NDP (ICMPv6 の最上部で稼動するプロトコル)、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 エントリもサポートします。IPv6 近隣探索プロセスは ICMP メッセージおよび送信要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レイヤアドレスを判別し、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 ビット未満のルートについて、ICMPv6 リダイレクトをサポートします。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 リダイレクトはサポートされません。

近隣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の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 に不要な負荷がかかりません。スイッチがアクティブに解決を試行しているのと同じネイバーをネクストホップとした IPv6 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。ドロップすることにより、CPU に余分な負荷がかかりません。

デフォルト ルータ プリファレンス (DRP)

スイッチは、ルータのアダプタイズメントメッセージの拡張である、IPv6 Default Router Preference (DRP; デフォルト ルータ プリファレンス) 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。その後、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 の NDP では、到達可能性が不明または信用できないルータより、到達可能または到達可能の可能性のあるルータが指定されます。NDP は、到達可能または到達可能の可能性のあるルータとして、常に同じルータを

選択するか、またはルータ リストから順番に選択できます。到達可能または到達不可能の可能性のある 2 台のルータが存在する場合、DRP を使用することにより、IPv6 ホストがどちらか一方を優先するよう設定できます。

IPv6 の DRP の詳細については、Cisco.com の『*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

スイッチはステートレス自動設定を使用して、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します。ホストは、リンクローカルな独自アドレスを自律設定します。起動元ノードはルータに送信要求を送信して、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の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

- Ping、traceroute、Telnet、TFTP、FTP
- 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 AAA の DNS リゾルバ
- IPv6 アドレスの Cisco Discovery Protocol (CDP; シスコ検出プロトコル) サポート

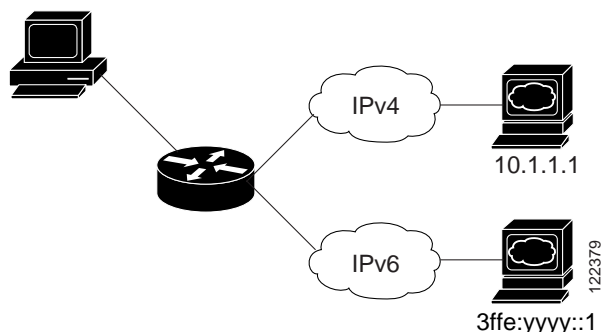
これらのアプリケーションを管理する機能については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4 および IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方でハードウェア メモリの使用を割り当てるには、デュアル IPv4 および IPv6 のテンプレートを使用する必要があります。

図 37-1 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 37-1 インターフェイス上でのデュアル IPv4 および IPv6 のサポート



デュアル IPv4 および IPv6 スイッチ データベース管理 (SDM) テンプレートをを使用して、IPv6 のルーティング デュアル スタック環境 (IPv4 および IPv6 の両方をサポートする) をイネーブルにします。デュアル IPv4 および IPv6 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。

- 最初にデュアル IPv4/IPv6 テンプレートを選択しないで IPv6 を設定しようとする、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 および IPv6 環境のスイッチは、IPv4 および IPv6 パケットを両方ルーティングし、IPv4 の QoS をハードウェアで適用します。
- IPv6 QoS はサポートされません。
- デュアル スタック テンプレートを使用すると、各リソースのハードウェア メモリ容量が少なくなるため、IPv6 を使用する予定がない場合はこのテンプレートを使用しないでください。

IPv4 および IPv6 のプロトコル 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。

IPv6 の DHCP アドレス割り当て

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は、ホストが接続されているネットワークに基づいて、適切なプレフィクスでの重複しないアドレス割り当てを管理します。アドレスは、1 つまたは複数のプレフィクス プールから割り当てられます。デフォルト 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、または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、サーバが自動的に適切なプールを検出できます。

このマニュアルでは、DHCPv6 のアドレスの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、リレー エージェント機能の設定の詳細については、Cisco.com の『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 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 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クスのサポートや、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 の『Cisco IOS IPv6 Configuration Library』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 の OSPF

スイッチは、IP のリンク ステート プロトコルとして IPv6 の Open Shortest Path First (OSPF) をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol (EIGRP; Enhanced IGRP) をサポートします。IPv6 の EIGRP は稼動するインターフェイスで設定されるため、グローバルな IPv6 アドレスは不要です。

EIGRP IPv6 インスタンスでは、実行する前に暗黙的または明示的なルータ ID が必要です。暗黙的なルータ 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動している可能性もあるため、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 の『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 のマルチプロトコル BGP

マルチプロトコル Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) は、IPv6 でサポートされている外部ゲートウェイ プロトコルです。IPv6 用のマルチプロトコル BGP 拡張は、IPv4 BGP と同じ機能をサポートします。IPv6 のマルチプロトコル BGP への拡張には、IPv6 アドレス ファミリーへのサポート、Network Layer Reachability Information (NLRI; ネットワーク レイヤ到着可能性情報)、および IPv6 アドレスを使用するネクストホップ (宛先へのパスの中の次のルータ) のアトリビュートが含まれます。

スイッチは、IPv6 または BGP IPv6 へのマルチキャスト BGP および Non-Stop Forwarding (NSF) をサポートしません。

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

IPv6 上の NMP および Syslog

IPv4 および IPv6 の両方をサポートするには、IPv6 ネットワーク管理で IPv6 および IPv4 両方のトランスポートが必要です。IPv6 上の Syslog では、これら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 の SNMP および Syslog は、次の機能を提供します。

- IPv4 および IPv6 の両方に対するサポート
- SNMP 用の IPv6 トランスポート、および SNMP エージェントを変更し、IPv6 ホストのトラップをサポートするための IPv6 トランスポート
- IPv6 アドレッシングをサポートするための SNMP および Syslog 関連の MIB
- トラップ レシーバーとしての IPv6 ホストの設定

IPv6 上のサポートのため、SNMP は既存の IP トランスポート マッピングが IPv4 と IPv6 を同時にサポートするように変更します。IPv6 トランスポート管理をサポートする SNMP 動作は、次のとおりです。

- User Datagram Protocol (UDP; ユーザ データグラム プロトコル) の SNMP ソケットをデフォルト設定でオープンする

- 新しいトランスポート メカニズム (*SR_IPV6_TRANSPORT*) を提供する
- IPv6 トランスポート上で SNMP 通知を送信する
- IPv6 トランスポート用の SNMP の名前つきアクセス リストをサポートする
- IPv6 トランスポートを使用し SNMP プロキシ転送をサポートする
- SNMP マネージャ機能が IPv6 トランスポートと連動していることを確認する

IPv6 上の SNMP (設定手順を含む) の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

IPv6 上の Syslog (設定手順を含む) の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 上の HTTP

HTTP クライアントは、IPv4 および IPv6 の両方の HTTP サーバに要求を送信し、HTTP サーバは IPv4 および IPv6 両方の HTTP クライアントからの要求に応答します。リテラルな IPv6 アドレスを持つ URL は、コロン区切りの 16 ビット値を使用した 16 進数表記で指定する必要があります。

受信ソケット コールは、IPv4 または IPv6 のアドレス ファミリーを選択します。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になります。リスニング ソケットは、接続を伝える IPv4 信号および IPv6 信号の両方の受信を待機します。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ます。

基本的な TCP/IP スタックはデュアルスタック環境をサポートしています。HTTP は、ネットワークレイヤの相互作用の処理に、TCP/IP スタックおよびソケットを使用します。

HTTP 接続が確立される前に、クライアントとサーバ ホスト間に基本的なネットワーク接続 (ping) が存在している必要があります。

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。

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

- IPv6 ポリシー ベース ルーティング
- IPv6 Virtual Private Network (VPN; バーチャル プライベート ネットワーク) の 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
- Intermediate System-to-Intermediate System (IS-IS) ルーティングのサポート
- サイトローカルなアドレス宛の IPv6 パケット
- IPv4/IPv6 または 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 (RPF)
- IPv6 の一般的なプレフィクス
- IPv6 の HSRP

制限事項

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェアメモリ内の IPv6 圧縮アドレスを使用することによる制限がいくつか発生します。これらのハードウェア制限により、機能の一部が失われたり制限されます。

- IPv6 関連機能で User-Network Interface (UNI; ユーザ ネットワーク インターフェイス) または Enhanced Network Interface (ENI; 拡張ネットワーク インターフェイス) ポートを使用している場合、IPv6 ルーティングを使用していなくても、最初に **ip routing** および **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを入力し、スイッチでの IP ルーティングおよび IPv6 ルーティングをグローバルでイネーブルに設定する必要があります。
- IPv6 ホスト ルート (特定のホストに到達するために使用されるルート) またはマスク長が 64 ビットを越える IPv6 ルートでは、ICMPv6 リダイレクト機能がサポートされません。ホスト ルートまたはマスク長が 64 ビットを越えるルートを介して到達可能な特定の宛先の場合、スイッチは適性のより高い先頭ホップ ルータにホストをリダイレクトできません。
- IPv6 ホスト ルートまたはマスク長が 64 ビットを越える IPv6 ルートの場合、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 バランスはサポートされません。
- スイッチは、SNAP カプセル化 IPv6 パケットを正しく転送できません。



(注) SNAP カプセル化された IPv4 パケットでも同様の制限がありますが、パケットはスイッチで破棄されます。

- 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。
- ホップ単位の拡張ヘッダーを持つ、ブリッジングされた 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通常の SPAN および RSPAN 制限の他に、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 アドレスが間違っている場合があります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスが間違っている場合があります。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 Policy-Based Routing (PBR; 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。

IPv6 の設定

- 「IPv6 のデフォルト設定」 (P.37-10)
- 「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化」 (P.37-10)
- 「デフォルト ルータ プリファレンスの設定」 (P.37-12)
- 「IPv4 および IPv6 プロトコル スタックの設定」 (P.37-13)
- 「IPv6 の DHCP アドレス割り当ての設定」 (P.37-15)

- 「IPv6 ICMP レート制限の設定」(P.37-18)
- 「IPv6 の CEF の設定」(P.37-19)
- 「IPv6 のスタティック ルーティングの設定」(P.37-19)
- 「IPv6 RIP の設定」(P.37-21)
- 「IPv6 OSPF の設定」(P.37-22)
- 「IPv6 の EIGRP の設定」(P.37-24)
- 「IPv6 の BGP の設定」(P.37-24)

IPv6 のデフォルト設定

表 37-1 に、IPv6 のデフォルト設定を示します。

表 37-1 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	ディセーブル (IPv4 CEF 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 は自動的にイネーブル。
IPv6 アドレス	設定なし。

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化

スイッチ上で IPv6 を設定するときは、次の注意事項に従ってください。

- デュアル IPv4 および IPv6 SDM テンプレートを選択してください。
- スイッチでは、この章で説明したすべての機能がサポートされ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.37-8) 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、*ipv6-address* および *ipv6-prefix* の各変数を、16 ビット値を使用したコロン区切りの 16 進数表記でアドレスを指定して入力する必要があります。変数 *prefix-length* (先頭にスラッシュ [/] を付加) は、プレフィクス (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な IPv6 アドレスを設定する必要があります。インターフェイスに IPv6 アドレスを設定すると、リンクローカルなアドレスが自動的に設定され、そのインターフェイスで IPv6 が有効になります。設定されたインターフェイスは、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 (このアドレスは近隣探索プロセスに使用される)
- すべてのノードを含む、リンクローカルなマルチキャストグループ FF02::1
- すべてのルーターを含む、リンク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 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 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 routing 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。 routing : スイッチをルーティング テンプレートに設定して、IPv4 ポリシーベース ルーティングなどの IPv4 および IPv6 ルーティングをサポートします。 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 コンフィギュレーションを最適化します。
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>	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 ビットの Extended Unique 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 プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に算出されます。これにより、インターフェイス上での IPv6 処理がイネーブルになります。 インターフェイスのリンクローカルなアドレスを指定します。このアドレスは、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の代わりに使用します。このコマンドにより、インターフェイス上での IPv6 処理がイネーブルになります。 インターフェイスで IPv6 のリンク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。リンクローカルなアドレスは、同じリンク上のノードと通信する場合にだけ使用されます。
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。

	コマンド	目的
ステップ 13	<code>show ipv6 interface interface-id</code>	設定を確認します。
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** の各インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**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の 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 プレフィクス 2001:0DB8:c18:1::/64 に基づく、リンクローカルなアドレスと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。両方のアドレスの下位 64 ビットでは、EUI-64 インターフェイス ID が使用されます。**show ipv6 interface EXEC** コマンドからの出力は、インターフェイスのリンクローカルなプレフィクス 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 gigabitethernet0/2
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 gigabitethernet0/11
GigabitEthernet0/2 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):
    FE02::1
    FE02::2
    FE02::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.
```

デフォルト ルータ プリファレンスの設定

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 Default Router Preference (DRP; デフォルト ルータ プリファレンス) とともに送信されます。DRP が設定されていない場合、ルータ アドバタイズメント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、等価であってもルーティングが等価コストではない場合、およびポリシーによってホストがいずれかのルータを選択するよう指示されている場合は、DRP が有効です。

インターフェイス上のルータで 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	<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>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、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	<code>ipv6 nd router-preference {high medium low}</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ipv6 interface</code>	設定を確認します。
ステップ 6	<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。

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 の『*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} global` 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、`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	<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 routing 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。 routing : スイッチをルーティング テンプレートに設定して、IPv4 ポリシーベース ルーティングなどの IPv4 および IPv6 ルーティングをサポートします。 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 コンフィギュレーションを最適化します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
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	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	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 7	ipv6 unicast-routing	スイッチ上での IPv6 データ パケットの転送をイネーブルに設定します。
ステップ 8	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 9	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 10	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 11	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 IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に算出されます。 インターフェイスのリンクローカルなアドレスを指定します。このアドレスは、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の代わりに使用します。 インターフェイスで IPv6 のリンク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。リンクローカルなアドレスは、同じリンク上のノードと通信する場合にだけ使用されます。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show 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 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。

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。インターフェイスの IPv4 アドレスを削除する場合は、**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** の各インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**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の 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 gigabitethernet0/2
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 の DHCP アドレス割り当ての設定

- 「DHCPv6 アドレス割り当てのデフォルト設定」 (P.37-15)
- 「DHCPv6 アドレス割り当ての注意事項」 (P.37-15)
- 「DHCPv6 サーバ機能のイネーブル化」 (P.37-16)
- 「DHCPv6 クライアント機能のイネーブル化」 (P.37-18)

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトでは、スイッチに Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 機能は設定されていません。

DHCPv6 アドレス割り当ての注意事項

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

- 以下の手順では、次のレイヤ 3 インターフェイスのうちいずれか 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 インターフェイスでイネーブルに設定する必要があります。
 - SV : **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です。
- DHCPv6 を設定するときは、事前に IPv4 および IPv6 をサポートする SDM (スイッチ データベース管理) テンプレートを選択しておく必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、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、1 つのインターフェイスでは同時に指定できません。

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	<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 dhcp pool <i>poolname</i></code>	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。
ステップ 3	<code>address prefix <i>IPv6-prefix</i> lifetime {<i>t1 t1</i> infinite}</code>	(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 進数にする必要があります。 lifetime <i>t1 t1</i> : IPv6 アドレス プレフィックスが有効ステータスを維持するタイム 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。時間間隔を指定しない場合は 無制限 になります。
ステップ 4	<code>link-address <i>IPv6-prefix</i></code>	(任意) リンクアドレス IPv6 プレフィックスを指定します。 着信インターフェイスのアドレスまたはパケット内のリンクアドレスが指定の IPv6 プレフィックスと一致した場合、サーバは構成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 進数にする必要があります。
ステップ 5	<code>vendor-specific <i>vendor-id</i></code>	(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 民間企業番号です。指定できる範囲は 1 ~ 4294967295 です。
ステップ 6	<code>suboption number {address <i>IPv6-address</i> ascii <i>ASCII-string</i> hex <i>hex-string</i>}</code>	(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 進数の文字列をサブオプション パラメータによって定義されたものとして入力します。
ステップ 7	<code>exit</code>	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	<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 9	<code>interface <i>interface-id</i></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 [<i>poolname</i> automatic] [rapid-commit] [<i>preference value</i>] [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。 <ul style="list-style-type: none"> • poolname : (任意) IPv6 DHCP プールのユーザ定義の名前です。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。 • automatic : (任意) システムはクライアントにアドレスを割り当てる際に使用するプールを自動的に決定できます。 • rapid-commit : (任意) 2 つのメッセージ交換方式を可能にします。 • preference value : (任意) サーバが送信するアドバタイズメッセージの preference オプションで伝送される preference 値。指定できる範囲は 0 ~ 255 です。デフォルトの preference 値は 0 です。 • allow-hint : (任意) サーバが送信請求メッセージでクライアントの提案を考慮するかどうか指定します。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 コンフィギュレーションを確認します。 DHCPv6 サーバ機能がインターフェイスでイネーブルに設定されてい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、DHCP プール コンフィギュレーション モード コマンドの **no** 形式を使用します。インターフェイス上の DHCPv6 サーバ機能をディセーブルに設定するには、**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。

次に、IPv6 アドレス プレフィクスを持つ *engineering* 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 engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 つのリンク アドレスと IPv6 アドレス プレフィクスを持つ *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、ベンダー固有のオプションのある *350* という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	<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>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、設定するインターフェイスを指定します。
ステップ 3	<code>ipv6 address dhcp [rapid-commit]</code>	インターフェイスで、DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 rapid-commit : (任意) アドレス割り当ての 2 つのメッセージ交換方式を可能にします。
ステップ 4	<code>ipv6 dhcp client request [vendor-specific]</code>	(任意) インターフェイスが、ベンダー固有のオプションを要求するように設定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ipv6 dhcp interface</code>	DHCPv6 クライアント機能がインターフェイスでイネーブルに設定されてい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。

次の例では、IPv6 アドレスを取得し、`rapid-commit` オプションをイネーブルにする方法を示します。

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

このマニュアルでは、DHCPv6 のアドレスの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、リレー エージェント機能の設定の詳細については、Cisco.com の『*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に設定されています。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルトのバケット 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 [bucket-size]</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>bucket-size</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>	設定を確認します。
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、パケット転送により多くの CPU 処理能力を割り当てることが可能な、レイヤ 3 IP スイッチング テクノロジーです。デフォルトでは、IPv4 CEF はイネーブル化されています。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ます。また、`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、インターフェイスでの 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 をディセーブルに設定するには、`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 をふたたびイネーブルに設定するには、`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。

CEF の設定の詳細については、Cisco.com の『*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 ルーティングの設定

スタティック IPv6 ルートの設定前には、次の処理を実行する必要があります。

- `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設定します。
- `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設定します。

- 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 IPv6 をレイヤ 3 インターフェイスでイネーブルに設定します。

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 <i>ipv6-prefix/prefix length</i> {<i>ipv6-address</i> <i>interface-id</i> [<i>ipv6-address</i>]} [<i>administrative distance</i>]	<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 ルートが設定されている場合は、ホスト名を設定することもできます。 • <i>/prefix length</i> : IPv6 プレフィックスの長さ。プレフィックスの (アドレスのネットワーク部) の上位連続ビット数を示す 10 進値です。スラッシュ記号を 10 進値の前に付ける必要があります。 • <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 ホップは直接接続する必要はありません。再帰処理が実行されて、直接接続されているネクスト ホップの IPv6 アドレスを検出します。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。 • <i>interface-id</i> : 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は、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、ネクスト ホップの IPv6 アドレスを常に指定するか、または、リンクに対するローカルアドレスをネクスト ホップとして指定し、指定したプレフィックスがリンクに割り当てられるよう設定する必要があります。パケットが送信されるネクスト ホップの IPv6 アドレスを指定することもできます。 <p>(注) リンクに対するローカル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。リンクに対するローカル ネクスト ホップは、隣接ルータに設定する必要があります。</p> <ul style="list-style-type: none"> • <i>administrative distance</i> : (任意) 管理ディスタンス。指定できる範囲は 1 から 254 です。デフォルト値は 1 で、接続されたルートを除くすべてのルートよりもスタティック ルートが優先されます。フローティング スタティック ルートを設定するには、ダイナミックルーティング プロトコルより大きい管理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 <code>show ipv6 static [ipv6-address ipv6-prefix/prefix length] [interface interface-id] [recursive] [detail]</code> または <code>show ipv6 route static [updated]</code>	IPv6 ルーティング テーブルを表示し、エントリを確認します。 <ul style="list-style-type: none"> • 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 ルートだけを表示します。 • recursive (任意) : 再帰スタティック ルートだけを表示します。キーワード recursive は、キーワード interface と相互に排他的です。ただし、コマンド構文に IPv6 プレフィクスが指定されている場合も、指定されていない場合も使用できます。 • 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 セットと最大分解深度。 – 無効なルートの場合、ルートが無効な理由。
ステップ5 <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。

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、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。このルートの管理ディスタンスは 130 です。

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

スタティックな IPv6 ルーティング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 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は、次の処理を実行する必要があります。

- **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設定します。
- **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設定します。
- IPv6 RIP をイネーブルに設定するレイヤ 3 インターフェイス上で IPv6 をイネーブルに設定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 <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 router rip name</code>	IPv6 RIP ルーティング プロセスを設定し、このプロセスのルータ 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 <code>maximum-paths number-paths</code>	(任意) IPv6 RIP がサポート可能な等価コスト ルートの最大数を定義します。指定できる範囲は 1 ~ 64 です。デフォルトは 4 ルートです。
ステップ4 <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5 <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。

コマンド	目的
ステップ 6 <code>ipv6 rip name enable</code>	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設定します。
ステップ 7 <code>ipv6 rip name default-information {only originate}</code>	<p>(任意) IPv6 デフォルト ルート (::/0) を、特定のインターフェイスから送信された RIP ルーティング プロセス アップデートに発信します。</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) を送信した後に、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、このインターフェイスに送信されたアップデートの他のすべてのルートを抑制する場合に選択します。 • originate : このインターフェイスに送信された他のすべてのルートに加え、デフォルト ルートからも送信する場合に選択します。
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 rip [name] [interface interface-id] [database] [next-hops]</code> または <code>show ipv6 route rip [updated]</code>	現在の 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 <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。

RIP ルーティング プロセスをディセーブルに設定するには、**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設定するには、**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、RIP プロセス `cisco` に最大 8 つの等価コスト ルートをイネーブルにし、インターフェイス上でこれをイネーブルに設定する例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 の RIP ルーティング設定の詳細については、Cisco.com の『*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 OSPF をカスタマイズできます。ただし、デフォルト設定でほとんどのカスタマー要件と機能要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルトを変更する場合は注意してください。変更することにより、IPv6 ネットワークの OSPF に悪影響を与える場合があります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、次の処理を実行する必要があります。
 - **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設定します。
 - **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設定します。
 - IPv6 OSPF をイネーブルに設定するレイヤ 3 インターフェイスで **IPv6** をイネーブルに設定します。

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設定します。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設定したとき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 から 65535 まで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 プレフィックスのいずれかで指定できます。 • ipv6-prefix/prefix length : IPv6 ネットワークの宛先、およびプレフィクス (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記号 (/) を付ける必要があります。 • advertise : (任意) Type 3 サマリー Link-State Advertisement (LSA; リンクステートアドバタイズメント) をアドバタイズ、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 : アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 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となります。 • cost cost : (任意) このサマリー ルートのメトリックまたはコスト。宛先への最短パスを決定する 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、同じ宛先への等価コスト ルートの最大数を定義します。指定できる範囲は 1 ~ 64 です。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]	<p>インターフェイスの IPv6 OSPF をイネーブルにします。</p> <ul style="list-style-type: none"> • 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	<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 インターフェイスについて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に設定するには、`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設定するには、`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 ルーティング設定の詳細は、Cisco.com の『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 の EIGRP の設定

デフォルトでは、IPv6 の EIGRP はディセーブルに設定されています。IPv6 の EIGRP は、インターフェイスで設定できます。ルータとインターフェイスを EIGRP 用に設定した後に、`no shutdown` 特権 EXEC コマンドを入力して EIGRP を開始します。



(注)

IPv6 の EIGRP がシャットダウン モードでない場合、EIGRP ルータモード コマンドを入力してルータおよびインターフェイスを設定する前に、EIGRP が稼動を開始する場合があります。

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されたルータ ID を参照してから、`router-id` コマンドを使用します。

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、そ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受動インターフェイスに設定してから、選択したインターフェイスに対して `no passive-interface` コマンドを使用してアクティブに設定します。EIGRP IPv6 を受動インターフェイスとして設定する必要はありません。

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

IPv6 の BGP の設定

マルチプロトコル BGP の IPv6 拡張を設定する場合、BGP ルーティング プロセスの作成、ピアリング関係の設定、および特定のネットワーク向けの BGP のカスタマイズを行う必要があります。IPv6 において、BGP は IPv4 における場合と同様に動作します。IPv6 用に BGP を稼動させるようルータを設定する前に、`ipv6 unicast-routing` コマンドを使用し IPv6 ルーティングをグローバルでイネーブルに設定します。

IPv6 の BGP 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>router bgp as-number</code>	BGP ルーティング プロセスを設定し、自律システム番号を使用して BGP 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	<code>no bgp default ipv4-unicast</code>	前の手順で指定した BGP ルーティング プロセスに対する IPv4 ユニキャスト アドレス ファミリーをディセーブルに設定します。 IPv4 ユニキャスト アドレス ファミリーのルーティング情報は、デフォルトでは各 BGP ルーティング セッションに対してアドバタイズされていますが、 neighbor remote-as コマンドを設定する前にこのコマンドを入力して、変更できます。
ステップ 4	<code>bgp router-id ip-address</code>	(任意) BGP が稼動しているローカル ルータの ID として固定 32 ビット ルータ ID を設定します。デフォルトでは、ルータ ID はルータ ループバック インターフェイスの IPv4 アドレスです。IPv6 だけに対してイネーブルに設定されているルータ (IPv4 アドレスはなし) では、BGP ルータ ID を手動で設定する必要があります。 (注) このコマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションはすべてリセットされます。
ステップ 5	<code>neighbor {ip-address ipv6-address peer-group-name} remote-as as-number</code>	指定された自律システムのネイバーの IPv6 アドレスを、ローカルルータの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。 (注) <code>ipv6-address</code> 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 6	<code>address-family ipv6</code>	IPv6 アドレス ファミリーを指定し、アドレス ファミリー コンフィギュレーション モードを開始します。
ステップ 7	<code>neighbor {ip-address peer-group-name ipv6-address} activate</code>	ローカル ルータとの IPv6 アドレス ファミリーのプレフィックスの交換を、ネイバーでイネーブルに設定します。
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 bgp ipv6</code>	IPv6 BGP コンフィギュレーションの情報を表示します。
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。

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

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html

スイッチは、マルチキャスト IPv6 BGP、IPv6 BGP の Nonstop Forwarding (NSF)、6PE マルチパス (EoMPLS)、および IPv6 VRF はサポートしません。

IPv6 の表示

これら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 コマンドリファレンスを参照してください。

表 37-2 IPv6 のモニタ用コマンド

コマンド	目的
<code>show bgp ipv6</code>	BGP IPv6 コンフィギュレーションおよびルーティング テーブルを表示します。
<code>show ipv6 access-list</code>	IPv6 のアクセス リストを表示します。
<code>show ipv6 cef</code>	IPv6 の Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) 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コンフィギュレーションを表示します。
<code>show ipv6 mtu</code>	宛先キャッシュごとの 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 の OSPF 情報を表示します。
<code>show ipv6 prefix-list</code>	IPv6 プレフィクス リストを表示します。
<code>show ipv6 protocols</code>	スイッチの 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 プロトコルの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。

表 37-3 EIGRP IPv6 情報を表示するためのコマンド

コマンド	目的
<code>show ipv6 eigrp [as-number] interface</code>	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。
<code>show ipv6 eigrp [as-number] neighbor</code>	EIGRP IPv6 で検出されたネイバーを表示します。
<code>show ipv6 eigrp [as-number] traffic</code>	送受信された EIGRP IPv6 パケット数を表示します。
<code>show ipv6 eigrp topology [as-number ipv6-address] [active all-links detail-links pending summary zero-successors]</code>	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 37-4 IPv4 および IPv6 アドレス タイプを表示するためのコマンド

コマンド	目的
<code>show ip http server history</code>	HTTP サーバとの最新の 20 の接続を表示します。表示には、アクセスされた IP アドレスおよび接続がクローズされた時間が含まれます。
<code>show ip http server connection</code>	HTTP サーバとの現在の接続を表示します。表示には、アクセスされたローカル IP アドレスおよびリモート IP アドレスが含まれます。

表 37-4 IPv4 および IPv6 アドレス タイプを表示するためのコマンド (続き)

コマンド	目的
<code>show ip http client connection</code>	HTTP サーバとの HTTP クライアントの接続の設定値を表示します。
<code>show ip http client history</code>	HTTP クライアントからサーバへの最新の 20 の要求を表示します。

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 GigabitEthernet0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to GigabitEthernet0/43
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
  GigabitEthernet0/4
  GigabitEthernet0/11
  GigabitEthernet0/12
  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
  GigabitEthernet0/4
  GigabitEthernet0/11
  GigabitEthernet0/12
  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 Gi0/13

```

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 ::, GigabitEthernet0/11
L    3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C    3FFE:C000:168:1::/64 [0/0]

```

```

    via ::, GigabitEthernet0/4
L  3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
    via ::, GigabitEthernet0/4
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

```

