



CHAPTER 37

IPv6 ユニキャスト ルーティングの設定

この章では、Catalyst 3750 Metro 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。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、第 38 章「IPv6 MLD スヌーピングの設定」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) の設定については、第 39 章「IPv6 ACL の設定」を参照してください。IPv4 ユニキャスト ルーティングの設定については、第 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 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートの使用をスイッチに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.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、次の URL にある『Cisco IOS IPv6 Command Reference』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

この章で説明する内容は、次のとおりです。

- 「IPv6 の概要」(P.37-1)
- 「IPv6 の設定」(P.37-10)
- 「IPv6 の表示」(P.37-27)

IPv6 の概要

IPv4 ユーザは IPv6 に移行すると、エンドツーエンドのセキュリティ、Quality Of Service (QoS)、グローバルに一意なアドレスなどのサービスを利用できます。IPv6 では、アドレスレンジが広いこと、プライベートアドレスや、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) 処理の必要性が削減されます。

IPv6 およびこの章で説明するその他の機能については、次を参照してください。

- 次の URL にある『Cisco IOS IPv6 Configuration Guide』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
- [Search] フィールドを使用して、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] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについてのマニュアルを入手できます。
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

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 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.37-9)
- 「制限事項」 (P.37-9)

IPv6 アドレス

スイッチでは、IPv6 ユニキャストアドレスだけがサポートされています。サイトローカルなユニキャストアドレス、エニーキャストアドレス、またはマルチキャストアドレスはサポートされていません。

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。次に、先行ゼロを省略した同じアドレスを示します。

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

また、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 回だけです。

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

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

「Implementing Addressing and Basic Connectivity」の章の次の項の内容がスイッチに適用されます。

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

サポート対象の IPv6 ユニキャストルーティング機能

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

- 「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)
- 「Default Router Preference (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/IPv6 プロトコル スタック」 (P.37-5)
- 「DHCP for IPv6 アドレスの割り当て」 (P.37-6)
- 「IPv6 のスタティック ルート」 (P.37-7)
- 「IPv6 の RIP」 (P.37-7)
- 「IPv6 の OSPF」 (P.37-7)
- 「IPv6 の EIGRP」 (P.37-7)
- 「IPv6 のマルチプロトコル BGP」 (P.37-7)
- 「IPv6 上の SNMP および syslog」 (P.37-8)
- 「IPv6 上の HTTP(S)」 (P.37-8)

スイッチでは、拡張アドレス機能、ヘッダー形式の単純化、拡張子とオプションのサポートの改善、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。ホップバイホップの拡張ヘッダー パケットもサポートされており、これらのパケットはソフトウェアでルーティングまたはブリッジングされます。

スイッチは、ネイティブ イーサネット Inter-Switch Link (ISL; スイッチ間リンク) または 802.1Q トランク ポート (スタティック ルートの場合) による IPv6 ルーティング機能を備えており、IPv6 対応 Routing Information Protocol (RIP) および Open Shortest Path First (OSPF) バージョン 3 プロトコルに対応しています。最大 16 個の等価コスト ルートがサポートされており、IPv4 および IPv6 のフレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチでは、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 アドレスがサポートされています。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) で始ま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 形式の 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::/10 (1111 1110 10) およびインターフェイス ID を使用します。Neighbor Discovery Protocol (NDP; 近隣探索プロトコル) およびステートレス自動設定プロセスでは、リンクローカルなアドレスを使用します。ローカル リンク上のノードはリンクローカルなアドレスを使用するため、通信時にグローバルに一意的なアドレスは必要ありません。IPv6 ルータは、リンクローカルな送信元または宛先のアドレスを持つパケットを他のリンクに転送しません。

詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide』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 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 レコードタイプでは IPv6 アドレスがサポートされており、IPv4 の A アドレス レコードと同等です。スイッチでは、IPv4 および IPv6 の DNS 解決がサポートされています。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチでは、システム Maximum Transmission Unit (MTU; 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 ディスカバリがサポートされています。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズにあ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。スイッチでは、マルチキャストパケットのパス MTU ディスカバリがサポートされていません。

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) では、ICMP 宛先到達不能メッセージなどのエラーメッセージが生成され、処理中に発生したエラーやその他の診断機能のエラーがレポートされます。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

スイッチでは、IPv6 対応の NDP (ICMPv6 の最上部で動作するプロトコル)、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 エントリがサポートされています。IPv6 近隣探索プロセスでは、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、ネイバーの到達可能性を確認して近接ルータを追跡します。

スイッチでは、マスク長が 64 ビット未満のルートに対して ICMPv6 リダイレクトがサポートされています。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の取得プロセス中に、スイッチ CPU に余分な負荷がかからなくなります。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が試行されているネイバーと同じである場合、スイッチに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 への余分な負荷がかからなくなります。

Default Router Preference (DRP)

スイッチでは、ルータのアダプタイズメッセージの拡張である IPv6 Default Router Preference (DRP) がサポートされています。DRP では、特にホストがマルチホーム構成になっており、ルータが異なるリンク上にある場合に、ホストで適切なルータを選択する機能が向上します。スイッチでは、Route Information Option (RFC 4191) はサポートされていません。

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 リストを保持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 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見込みの高いルータが指定されます。NDP は、到達可能または到達可能見込みの高いルータとして、常に同じルータを選択

するか、またはルータ リストの中のルータを繰り返して使用できます。DRP を使用することにより、2 台のルータが到達可能または到達可能見込みが高い場合に、IPv6 ホストがこれらのルータを差別化するように設定できます。

IPv6 の DRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』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の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ダプタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』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

スイッチでは、次のアプリケーションで IPv6 がサポートされています。

- ping、traceroute、Telnet、Trivial File Transfer Protocol (TFTP)、および File Transfer Protocol (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 AAAA 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

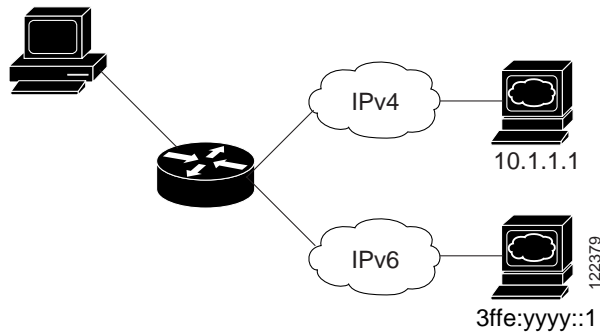
これらのアプリケーションを管理する場合の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 と IPv6 の両方のプロトコルで Ternary Content Addressable Memory (TCAM; Ternary CAM) 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 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/IPv6 サポート



デュアル IPv4/IPv6 SDM テンプレートを使用して、IPv6 ルーティングをイネーブルにします。デュアル IPv4/IPv6 SDM テンプレートの詳細については、第 6 章「SDM テンプレートの設定」を参照してください。

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

- デュアル IPv4/IPv6 テンプレートを最初に選択せずに 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ていません。
- デュアル IPv4/IPv6 環境のスイッチは、IPv4 と IPv6 の両方のパケットをルーティングし、ハードウェアで IPv4 QoS を適用します。
- IPv6 QoS は完全に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 プロトコル スタックの詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 により、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。このアドレス割り当て機能により、ホストが接続したネットワークに基づいて、適切なプレフィックスの重複しないアドレス割り当てが管理されます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てられます。デフォルトのドメインや DNS ネーム サーバ アドレスなどの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や複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide』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し、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タイプのトラフィックにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』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 アドレスとプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

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

IPv6 の OSPF

スイッチでは、IPv6 の Open Shortest Path First (OSPF) (IP のリンクステート プロトコル) がサポートされています。詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 の EIGRP

スイッチでは、IPv6 の Enhanced Interior Gateway Routing Protocol (EIGRP; 拡張 IGRP) がサポートされています。IPv6 の EIGRP は動作するインターフェイス上で設定されるため、グローバル IPv6 アドレスを必要としません。

EIGRP IPv6 インスタンスでは、実行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 ノードには使用可能なルータ ID が必ず設定されます。ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで動作するため、使用可能な IPv4 ルータ ID がない場合があります。

IPv6 の EIGRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Guide*』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 Exterior Gateway Protocol (EGP; 外部ゲートウェイ プロトコル) です。IPv6 のマルチプロトコル BGP 拡張では、IPv4 BGP と同じ機能がサポートされています。マルチプロトコル BGP に対する IPv6 機能拡張では、IPv6 アドレス ファミリーと 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 (パス内の宛先に向かう次のルータ) アトリビュートがサポートされています。

スイッチでは、IPv6 または BGP IPv6 のマルチキャスト BGP や Non-stop Forwarding (NSF) がサポートされていません。

IPv6 の BGP の設定については、Cisco.com で『*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 SNMP および syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 ネットワーク管理で IPv6 と IPv4 の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 タイプがサポートされています。

IPv6 上の Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) および syslog には、次の機能が用意されています。

- IPv4 および IPv6 のサポート
- 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 Management Information Base (MIB; 管理情報ベース)
- トラップ レシーバとしての IPv6 ホストの設定

IPv6 上でのサポートのために、SNMP は IPv4 および IPv6 を同時にサポートするように既存の IP トランスポート マッピングを変更します。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。

- デフォルト設定を持つ User Datagram Protocol (UDP; ユーザ データグラム プロトコル) SNMP ソケットをオープンします。
- 新しいトランスポート メカニズム (*SR_IPV6_TRANSPORT*) を提供します。
- IPv6 トランスポート上で SNMP 通知を送信します。
- IPv6 トランスポート用の SNMP 名前付きアクセス リストをサポートします。
- IPv6 トランスポートを使用する SNMP プロキシ転送をサポートします。
- 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します。

IPv6 上の SNMP (設定手順を含む) については、Cisco.com で『*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) については、Cisco.com で『*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(S)

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 の両方の HTTP クライアントからの要求に応答します。リテラル IPv6 アドレスを使用する URL は、コロンで区切られた 16 ビット値を使用した 16 進数形式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 ファミリを選択します。受信ソケットは、IPv4 または IPv6 の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 および IPv6 の両方の信号を継続して受信します。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 スタックでは、デュアルスタック環境がサポートされています。HTTP は、ネットワーク レイヤの相互作用を処理するのに TCP/IP スタックおよびソケットを使用します。

HTTP 接続が確立する前に、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 で『*Cisco IOS IPv6 Configuration Guide*』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 Policy-Based Routing (PBR; 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) Routing/Forwarding (VRF; VPN ルーティング/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 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 (uRPF; ユニキャスト RPF)
- IPv6 の一般的なプレフィクス
- IPv6 Hot Standby Router Protocol (HSRP; ホット スタンバイ ルータ プロトコル)



(注)

スイッチでは、MPLS、EoMPLS、QinQ 信頼、階層型 QoS などの特定の ES ポート固有の機能を含む IPv6 関連の機能はサポートされていません。

制限事項

IPv6 はスイッチのハードウェアに実装されるため、TCAM 内の IPv6 圧縮アドレスによる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て制限されます。

機能の制限は次のとおりです。

- ICMPv6 リダイレクト機能は、IPv6 ホスト ルート（特定のホストに到達するのに使用されるルート）またはマスク長が 64 ビットを超える IPv6 ルートではサポートされません。スイッチは、ホスト ルートまたはマスク長が 64 ビットを超えるルートを介して到達可能な、特定の宛先へのより最適な先頭ホップ 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 ビットを超える IPv6 ルートでは、等価コスト ルー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、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) でカプセル化された IPv6 パケットを転送できません。



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

- スイッチは IPv6/IPv4 および IPv4/IPv6 の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 のトンネル エンドポイントにすることはできません。
- ホップバイホップの拡張ヘッダーを持つブリッジド IPv6 パケットは、ソフトウェアで転送されません。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ますが、ブリッジングはハードウェアで行われます。

- 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 Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN; リモート SPAN) 制限に加えて、次のような IPv6 パケット固有の制限事項があります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスが不正である可能性があります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスが不正である可能性があります。通常の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。

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および IPv6 ルーティングのイネーブル化」(P.37-11)
- 「DRP の設定」(P.37-13)
- 「IPv4 および IPv6 プロトコル スタックの設定」(P.37-14)
- 「DHCP for IPv6 の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.37-19)
- 「IPv6 の CEF の設定」(P.37-20)
- 「IPv6 のスタティック ルートの設定」(P.37-20)
- 「IPv6 の RIP の設定」(P.37-22)
- 「IPv6 の OSPF の設定」(P.37-23)
- 「IPv6 の EIGRP の設定」(P.37-25)
- 「IPv6 の BGP の設定」(P.37-26)

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 または dCEFv6	ディセーブル (IPv4 Cisco Express Forwarding (CEF; シスコ エクスプレッス フォワーディング) および distributed CEF (dCEF; 分散 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 および dCEF6 は自動的にイネーブルになります。
IPv6 アドレス	未設定。

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバルに転送する手順について説明します。

スイッチ上で IPv6 を設定する場合は、次の注意事項を確認してください。

- デュアル IPv4/IPv6 SDM テンプレートを選択する必要があります。
- サポートされていない IPv6 機能について、「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.37-9) 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、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定して、*ipv6-address* および *ipv6-prefix* 変数を入力します。*prefix-length* 変数 (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 進値です。

インターフェイスで IPv6 トラフィックを転送するには、そのインターフェイスにグローバルな 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。設定が済んだ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請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ます)
- 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 で『Cisco IOS IPv6 Configuration Guide』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	sdm prefer dual-ipv4-and-ipv6 {default routing vlan}	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 <ul style="list-style-type: none"> • default : システム リソースを均衡化するようにスイッチをデフォルト テンプレートに設定します。 • routing : IPv4 ポリシーベース ルーティングを含む、IPv4 および IPv6 ルーティングをサポートするようにスイッチをルーティング テンプレートに設定します。 • vlan : ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	オペレーティング システムをリロードします。
ステップ 5	configure terminal	スイッチのリロード後にグローバル コンフィギュレーション モードを開始します。

	コマンド	目的
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 cui-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。指定するのはネットワーク プレフィクスだけです。残りの 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ローカルアドレスの代わりに、インターフェイスで使用するリンクローカルアドレスを指定します。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 リンクローカル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。このリンクローカル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 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 cui-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。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 アドレスが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 プレフィクス `2001:0DB8:c18:1::/64` に基づくリンクローカル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方法の例を示します。いずれのアドレスの下位 64 ビットにも 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プレフィクス `FE80::/64` にインターフェイス ID (`20B:46FF:FE2F:D940`) がどのように付加されるかを示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
```

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/1/1
GigabitEthernet1/1/1 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.
```

DRP の設定

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

DRP が有効となるのは、リンク上の 2 台のルータが等価ではあっても等価コストではないルーティングを行う可能性がある場合、およびホストがいずれかのルータを選択するようにポリシーで指示された場合です。

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

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

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

次に、インターフェイスにルータの DRP を **high** で設定する方法の例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 の DRP の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide』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。まだ設定が済んでいない場合は、**sdm prefer dual-ipv4-and-ipv6 {default | routing | 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、**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 の両方をサポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	sdm prefer dual-ipv4-and-ipv6 {default routing vlan}	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 <ul style="list-style-type: none"> • default : システム リソースを均衡化するようにスイッチをデフォルト テンプレートに設定します。 • routing : IPv4 ポリシーベース ルーティングを含む、IPv4 および IPv6 ルーティングをサポートするようにスイッチをルーティング テンプレートに設定します。 • vlan : ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	オペレーティング システムをリロードします。
ステップ 5	configure terminal	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	スイッチで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 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。

	コマンド	目的
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。指定するのはネットワークプレフィクスだけです。残りの 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルアドレスの代わりに、インターフェイスで使用するリンクローカルアドレスを指定します。 インターフェイスに IPv6 リンクローカル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。このリンクローカル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 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。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 アドレスが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方法の例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

DHCP for IPv6 のアドレス割り当ての設定

ここでは、Dynamic Host Configuration Protocol for IPv6 (DHCPv6) のアドレス割り当てを設定する方法について説明します。

- 「DHCPv6 アドレス割り当てのデフォルト設定」(P.37-16)
- 「DHCPv6 アドレス割り当て設定時の注意事項」(P.37-16)
- 「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 DHCPv6 機能は設定されていません。

DHCPv6 アドレス割り当て設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項を確認してください。

- この手順では、次に示すレイヤ 3 インターフェイスのいずれかを指定する必要があります。
 - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
 - SVI : **interface vlan *vlan_id*** コマンドを使用して作成された VLAN インターフェイスです。
 - レイヤ 3 モードの EtherChannel ポート チャネル : **interface port-channel *port-channel-number*** コマンドを使用して作成されたポートチャネル論理インターフェイスです。
- DHCPv6 を設定する前に、IPv4 および IPv6 をサポートする Switch Database Management (SDM) 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、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、1 つのインターフェイスで同時に指定することはできません。

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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 dhcp pool <i>poolname</i>	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。
ステップ 3	address prefix <i>IPv6-prefix</i> lifetime {<i>tl tl</i> infinite}	(任意) アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。 lifetime <i>tl tl</i> : IPv6 アドレス プレフィックスが有効な状態を維持する時間間隔 (秒単位) 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。

	コマンド	目的
ステップ 4	<code>link-address IPv6-prefix</code>	(任意) リンクアドレスの IPv6 プレフィックスを指定します。 着信インターフェイス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 vendor-id</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 IPv6-address ascii ASCII-string hex hex-string}</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 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 10	<code>ipv6 dhcp server [poolname automatic] [rapid-commit] [preference value] [allow-hint]</code>	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 プール用にユーザが定義した名前。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) クライアントにアドレスを割り当てるときに使用するプールがシステムで自動的に決定されます。 • rapid-commit : (任意) 2 メッセージ交換方式を許可します。 • 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 SOLICIT メッセージでクライアントの提案を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	show ipv6 dhcp pool または show ipv6 dhcp interface	DHCPv6 プール設定を確認します。 DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool poolname** グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、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するには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、*engineering with an IPv6 address prefix* 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 engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次の例では、3 つのリンクアドレスおよび 1 つの IPv6 アドレス プレフィクスを持つ *testgroup* 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 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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
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) アドレス割り当てに 2 メッセージ交換方式を許可します。
ステップ 4	<code>ipv6 dhcp client request [vendor-specific]</code>	(任意) インターフェイスでベンダー固有のオプションを要求できるようにします。
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上でイネーブルであることを確認します。

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

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

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

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

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、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"> 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	<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、パケット サイズを 20 トークンに設定する方法の例を示します。

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

IPv6 の CEF の設定

Cisco Express Forwarding (CEF) は、ネットワーク パフォーマンスを改善するためのレイヤ 3 IP スイッチング テクノロジーです。IPv6 CEF はデフォルトでディセーブルですが、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。**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

IPv6 CEF をディセーブルにするには、**no ipv6 cef** グローバル コンフィギュレーション コマンドを使用します。IPv6 CEF または dCEF がディセーブルになっている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。

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

IPv6 のスタティック ルートの設定

IPv6 スタティック 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てから、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 をイネーブルにしておく必要があります。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 route <i>ipv6-prefix/prefix length</i> {<i>ipv6-address</i> <i>interface-id</i> [<i>ipv6-address</i>]} [<i>administrative distance</i>]	<p>IPv6 スタティック 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 プレフィクスの長さ。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。ネクストホップの IPv6 アドレス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、コロンで区切られた 16 ビット値を使用した 16 進数形式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、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、または指定したプレフィクスをリンクに割り当てて、リンクローカル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 アドレスを任意で指定することもできます。 <p>(注) リンク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があります)。</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、この場合は接続されたルートを除く他のどのルート 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	<pre>show ipv6 static [ipv6-address ipv6-prefix/prefix length] [interface interface-id] [recursive] [detail]</pre> <p>または</p> <pre>show ipv6 route static [updated]</pre>	<p>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。</p> <ul style="list-style-type: none"> • interface interface-id : (任意) 指定されたインターフェイスを出力インターフェイスとして含むスタティック 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。 recursive キーワードは interface キーワードと相互に排他的ですが、コマンド構文での IPv6 プレフィックスの指定の有無には関係なく使用できます。 • 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	<pre>copy running-config startup-config</pre>	(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方法の例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet1/1/1 130
```

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

IPv6 の RIP の設定

IPv6 RIP を実行する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から、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 をイネーブルにしておく必要があります。

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	<pre>configure terminal</pre>	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	<pre>ipv6 router rip name</pre>	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	<pre>maximum-paths number-paths</pre>	(任意) IPv6 RIP がサポートできる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、デフォルトは 4 ルートです。
ステップ 4	<pre>exit</pre>	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	<pre>interface interface-id</pre>	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>	指定した 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	<code>ipv6 rip name default-information {only originate}</code>	(任意) IPv6 デフォルト ルート (::/0) を RIP ルーティング プロセスのアップデートに生成し、指定したインターフェイスから送信します。 (注) 任意のインターフェイスから IPv6 デフォルト ルート (::/0) が送信され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。 <ul style="list-style-type: none"> • only : デフォルト ルートが生成されますが、このインターフェイスで送信されるアップデート内の他のすべてのルートが抑制されます。 • originate : デフォルト ルート、およびこのインターフェイスで送信されるアップデート内の他のすべてのルートが送信されます。
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>	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するには、`no ipv6 router rip name` グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して RIP ルーティング プロセスをディセーブルにするには、`no ipv6 rip name` インターフェイス コンフィギュレーション コマンドを使用します。

次に、最大 8 の等価コスト ルートで RIP ルーティング プロセス `cisco` をイネーブルにし、インターフェイス上でこのプロセスをイネーブルにする方法の例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitEthernet1/1/1
Switch(config-if)# ipv6 rip cisco enable
```

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

IPv6 の OSPF の設定

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

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意が必要です。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、次の操作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します。
 - 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します。このプロセス ID は、IPv6 ルーティング プロセスの OSPF 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。この番号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 プレフィクスのいずれかを指定できます。 • 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。スラッシュ記号 (/) を 10 進値の前に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。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 Shortest Path First (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、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。

	コマンド	目的
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。
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 の OSPF をイネーブルにします。 instance instance-id : (任意) インスタンス ID
ステップ 8	<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にするには、**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の OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf process-id area area-id** インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Guide』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 はディセーブルです。IPv6 の EIGRP はインターフェイスに設定できます。EIGRP 用にルータおよびインターフェイスを設定したあとで、**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 が実行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済みのルータ ID を確認してから、**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、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface default** コマンドを使用してすべてのインターフェイスをパッシブに設定してから、選択されたインターフェイス上で **no passive-interface** コマンドを使用し、これらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要はありません。

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

IPv6 の BGP の設定

IPv6 のマルチプロトコル BGP 拡張を設定する場合は、BGP ルーティング プロセスを作成し、ピアリング関係を設定して特定ネットワークの BGP をカスタマイズする必要があります。IPv6 の BGP 機能は IPv4 の BGP 機能と同じです。IPv6 の BGP を実行するようにルータを設定する前に、**ipv6 unicast-routing** コマンドを使用して、グローバルに IPv6 ルーティングをイネーブルにしておく必要があります。

IPv6 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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router bgp as-number	BGP ルーティング プロセスを設定し、指定した自律システム番号に対して 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	no bgp default ipv4-unicast	前の手順で指定した BGP ルーティング プロセスの IPv4 ユニキャスト アドレス ファミリをディセーブルにします。 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いないかぎり、デフォルトでは IPv4 ユニキャスト アドレス ファミリのルーティング情報が各 BGP ルーティング セッションにアドバタイズされます。
ステップ 4	bgp router-id ip-address	(任意) BGP を実行するローカル ルータの ID として 32 ビット固定のルータ ID を設定します。デフォルトのルータ 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 だけがイネーブルな (IPv4 アドレスのない) ルータでは、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 セッションがすべてリセットされます。
ステップ 5	neighbor {ip-address ipv6-address[%] interface-type interface-number peer-group-name} remote-as as-number	指定した自律システム内のネイバーの 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) <i>ipv6-address</i> は、コロンで区切られた 16 ビット値を使用した 16 進数形式にする必要があります。
ステップ 6	address-family ipv6	IPv6 アドレス ファミリを指定して、アドレス ファミリ 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	neighbor {ip-address peer-group-name ipv6-address} activate	IPv6 アドレス ファミリのプレフィクスをネイバーがローカル ルータと交換できるようにします。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show bgp ipv6	IPv6 BGP 設定の情報を表示します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定手順の詳細については、Cisco.com で『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

スイッチでは、マルチキャスト IPv6 BGP、IPv6 BGP の Nonstop Forwarding (NSF)、6PE マルチパス (EoMPLS)、または IPv6 VRF がサポートされていません。

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 設定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>	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。

表 37-3 EIGRP IPv6 情報を表示するコマンド

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 タイプを表示するコマンド

コマンド	目的
<code>show ip http server history</code>	HTTP サーバとの接続を最新 20 個まで表示します (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を含む)。
<code>show ip http server connection</code>	HTTP サーバへの現在の接続を表示します (アクセスされているローカル IP アドレスおよびリモート IP アドレスを含む)。
<code>show ip http client connection</code>	HTTP サーバへの HTTP クライアント接続数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要求を最新 20 個まで表示します。

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
    GigabitEthernet1/1/1
    GigabitEthernet1/1/2
Redistribution:
  None
```

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

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

  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
  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 V17
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
```