



IPv6 ホスト機能の設定

この章では、Catalyst 2975 スイッチに IPv6 ホスト機能を設定する方法について説明します。

IPv6 Multicast Listener Discovery (MLD) スヌーピングについては、[第 35 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。

(IPv4 と IPv6 の両方をサポートする) デュアル スタック環境をイネーブルにするには、デュアル IPv4/IPv6 スイッチ データベース管理 (SDM) テンプレートを使用するように、スイッチを設定する必要があります。[「デュアル IPv4/IPv6 プロトコル スタック」\(P.34-4\)](#)を参照してください。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「IPv6 の概要」(P.34-1)
- 「IPv6 の設定」(P.34-7)
- 「IPv6 の表示」(P.34-11)

IPv6 の概要

IPv4 ユーザは IPv6 に移行することで、エンドツーエンドのセキュリティ、Quality of Service (QoS; サービス品質)、およびグローバルに一意なアドレスなどのサービスを受けることができます。IPv6 アドレス空間により、プライベート アドレスとネットワーク エッジ上の境界ルータでの Network Address Translation (NAT; ネットワーク アドレス変換) 処理の必要性が少なくなります。

シスコシステムズの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

この章の IPv6 とその他の機能については、

- 次の URL の『Cisco IOS IPv6 Configuration Library』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- [Search] フィールドを使用して、Cisco IOS ソフトウェアのドキュメントを見つけます。たとえば、スタティック ルートに関する情報が必要な場合は、検索フィールドに「*Implementing Static Routes for IPv6*」と入力して、スタティック ルートに関する次のドキュメントを取得します。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ここでは、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.34-2)
- 「サポートされる IPv6 ホスト機能」 (P.34-2)
- 「IPv6 とスイッチ スタック」 (P.34-6)

IPv6 アドレス

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

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

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

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

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

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

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

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

「Implementing Addressing and Basic Connectivity」の章で、次のセクションの内容が Catalyst 2975 スイッチに当てはまります。

- 「IPv6 Address Formats」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポートされる IPv6 ホスト機能

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

- 「128 ビット幅のユニキャスト アドレス」 (P.34-3)
- 「IPv6 用 DNS」 (P.34-3)
- 「ICMPv6」 (P.34-3)
- 「近接ディスカバリ」 (P.34-4)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.34-4)
- 「IPv6 アプリケーション」 (P.34-4)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.34-4)
- 「IPv6 による SNMP と Syslog」 (P.34-5)

- 「IPv6 による HTTP (S)」 (P.34-6)

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

128 ビット幅のユニキャスト アドレス

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

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

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

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

詳細については、Cisco.com の『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の 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 用 DNS

IPv6 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 タイプをサポートしています。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 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

ICMPv6

IPv6 の Internet Control Message Protocol (ICMP) は ICMP 宛先到達不能メッセージなどのエラーメッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、近接ディスカバリ 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。

近接ディスカバリ

スイッチは IPv6 対応の 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 エントリをサポートします。IPv6 NDP は ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカルリンク）上のネイバのリンクレイヤ アドレスを判別し、ネイバ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対して ICMPv6 リダイレクトをサポートしていません。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

近接ディスカバリ スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバである場合、そのようなパケットが追加されると、スイッチは廃棄を実行します。この廃棄を実行することで、CPU にそれ以上負荷がかからないようになります。

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することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をア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 の『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、traceroute、Telnet、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル)、および FTP (ファイル転送プロトコル)
- IPv6 トランスポートによる Secure Shell (SSH ; セキュア シェル)
- IPv6 トランスポートによる HTTP サーバアクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol (CDP) サポート

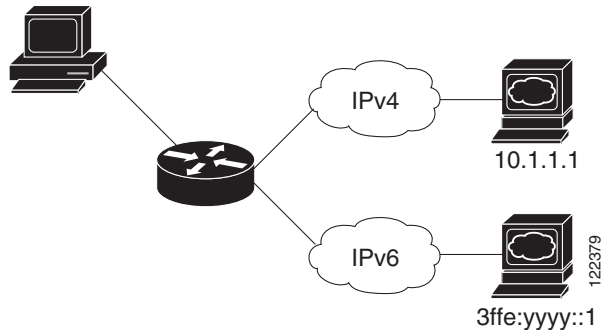
これらのアプリケーションの管理の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」と「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方で Ternary CAM (TCAM) の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 34-1 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 34-1 インターフェイス上での IPv4/IPv6 のデュアル サポート



デュアル IPv4/IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートを使用して、(IPv4 と IPv6 の両方をサポートする) デュアル スタック環境をイネーブルにします。デュアル IPv4/IPv6 SDM テンプレートの詳細については、[第 8 章「SDM テンプレートの設定」](#)を参照してください。

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

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

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

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを示的に定義します。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 による SNMP と Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で、IPv6 と IPv4 の両方のトランスポートが必要です。IPv6 による Syslog 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ています。

IPv6 による SNMP および syslog は次の機能を提供します。

- IPv4 と IPv6 の両方のサポート
- SNMP 用および SNMP エージェントを変更して 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 アドレス指定をサポートする SNMP および syslog 関連 MIB
- トラップ レシーバとしての IPv6 ホストの設定

IPv6 によるサポートでは、IPv4 と IPv6 を同時にサポートするように、SNMP により既存の IP トランスポートのマッピングが変更されます。次の SNMP の操作では、IPv6 トランスポートの管理をサポートしています。

- デフォルトの設定で、UDP SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供する
- IPv6 トランスポートによる SNMP 通知を送信する
- IPv6 トランスポートによる SNMP 名前付きアクセス リストをサポートする
- IPv6 トランスポートを使用した 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携することを確認する

設定手順を含む IPv6 による SNMP 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。

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

IPv6 による HTTP (S)

HTTP クライアントは IPv4 と IPv6 の両方の HTTP サーバに要求を送信し、これらのサーバは IPv4 と IPv6 の両方の HTTP クライアントの要求に応答します。文字による IPv6 アドレスを含む URL は 16 ビット値を使用したコロン区切りの 16 進形式で指定する必要があります。

`accept` ソケット コールは IPv4 または IPv6 アドレス ファミリを選択します。`accept` ソケットは IPv4 ソケットか IPv6 ソケットです。リスニング ソケットは、接続を示す IPv4 信号と IPv6 信号の両方をリスンし続けます。IPv6 リスニング ソケットは IPv6 ワイルドカードアドレスとバインドされています。

下位の 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 TCP/IP スタックおよびソケットに依存して、ネットワークレイヤの相互作用を処理します。

HTTP 接続を確立する前に、クライアントとサーバ ホスト間に基本のネットワーク接続 (**ping**) が存在する必要があります。

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

IPv6 とスイッチ スタック

スイッチは スタック全体の IPv6 転送とスタック マスター上の IPv6 ホスト機能をサポートします。スタック マスターは IPv6 ホスト機能と IPv6 アプリケーションを実行します。

新しいスタック マスターが選択されてリセットする間、スイッチ スタックは IPv6 パケットを転送しません。スタック MAC アドレスが変更され、IPv6 アドレスも変更されます。**ipv6 address ipv6-prefix/prefix length eui-64** インターフェイス コンフィギュレーション コマンドを使用して、extended unique identifier (EUI) を含むスタック IPv6 アドレスを指定すると、そのアドレスはイン

ターフェイス MAC アドレスに基づきます。「IPv6 アドレッシングの設定および IPv6 ホスト のイネーブル化」(P.34-7) を参照してください。

固定 MAC アドレス機能をスタックに設定してスタック マスターを変更した場合、スタック MAC アドレスは約 4 分間変更されません。詳細については、第 6 章「スイッチ スタックの管理」の「固定 MAC アドレスのイネーブル化」(P.6-18) を参照してください。

IPv6 の設定

ここでは、次の IPv6 転送の設定情報について説明します。

- 「IPv6 のデフォルト設定」(P.34-7)
- 「IPv6 アドレッシングの設定および IPv6 ホスト のイネーブル化」(P.34-7)
- 「IPv6 ICMP レート制限の設定」(P.34-9)
- 「IPv6 のスタティック ルーティングの設定」(P.34-10)

IPv6 のデフォルト設定

表 34-1 に IPv6 のデフォルト設定を示します。

表 34-1 IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 アドレス	未設定

IPv6 アドレッシングの設定および IPv6 ホスト のイネーブル化

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

スイッチに IPv6 を設定する前に、次の注意事項に従ってください。

- デュアル IPv4/IPv6 SDM テンプレートを選択してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、*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 進形式でアドレスを指定して入力する必要があります。*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 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、リンクに対して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、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（このアドレスは近接ディスカバリ プロセスに使用される）
- すべてのノードを含む、リンクに対してローカルな マルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルな マルチキャスト グループ FF02::2

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	sdm prefer dual-ipv4-and-ipv6 default	<ul style="list-style-type: none"> IPv4 および IPv6 をサポートする SDM テンプレートを選択します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	OS (オペレーティング システム) をリロードします。
ステップ 5	configure terminal	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	<p>IPv6 アドレスの下位 64 ビットの 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。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。</p> <p>インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。</p> <p>インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合に限定されます。</p>
ステップ 8	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show ipv6 interface interface-id	設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** 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 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 に基づいた、リンクに対して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 コマンドの出力には、インターフェイスのリンクに対してローカルなプレフィクス FE80::/64 にインターフェイス ID (20B:46FF:FE2F:D940) を付加する方法が示されます。


```

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/1
GigabitEthernet1/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    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.
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 Addressing and Basic Connectivity」の章を参照してください。

IPv6 ICMP レート制限の設定

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 icmp error-interval interval [bucketsize]</code>	IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定します。 <ul style="list-style-type: none"> <code>interval</code> : バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 <code>bucketsize</code> : （任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 interface [interface-id]</code>	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 のスタティック ルーティングの設定

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 route ipv6-prefix/prefix length {ipv6-address interface-id [ipv6-address]} [administrative distance]</code>	<p>スタティック IPv6 ルートを設定します。</p> <ul style="list-style-type: none"> • <i>ipv6-prefix</i> : スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • <i>/prefix length</i> : IPv6 プレフィクスの長さ。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。10 進値の前にスラッシュを付加する必要があります。 • <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 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは 16 ビット値を使用したコロン区切りの 16 進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、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィクスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 <p>(注) リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、<i>interface-id</i> を指定する必要があります (リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります)。</p> <ul style="list-style-type: none"> • <i>administrative distance</i> : (任意) 管理距離。指定できる範囲は 1 ~ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルートタイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きな管理距離を使用します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 4 <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 テーブルの内容を表示して、設定を確認します。 <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。recursive キーワードは interface キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィクスが指定されているかどうかに関係なく、使用することができます。 • detail : (任意) 次に示す追加情報を表示します。 <ul style="list-style-type: none"> – 有効な再帰ルートの場合、出力パス セットおよび最大分解深度 – 無効なルートの場合、ルートが無効な理由
ステップ 5 <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、管理距離が 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

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

IPv6 の表示

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

表 34-2 に、スイッチ上で IPv6 をモニタするための特権 EXEC コマンドを示します。

表 34-2 IPv6 のモニタ用コマンド

コマンド	目的
<code>show ipv6 access-list</code>	アクセス リストのサマリーを表示します。
<code>show ipv6 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 キャッシュ エントリを表示します。
<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 route</code>	IPv6 ルート テーブル エントリを表示します。
<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 34-3 に、IPv4 および IPv6 アドレス タイプに関する情報を表示する特権 EXEC コマンドを示します。

表 34-3 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
show ip http server history	アクセスされた IP アドレスと接続が閉じられた時間を含む、HTTP サーバへの以前の 20 接続について表示します。
show ip http server connection	アクセスされているローカルおよびリモート IP アドレスを含む HTTP サーバへの現在の接続について表示します。
show ip http client connection	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
show ip http client history	HTTP クライアントからサーバに対して行われた最後の 20 要求のリストを表示します。

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

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

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

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
    GigabitEthernet2/0/4
    GigabitEthernet2/0/
    GigabitEthernet1/0/12
  Redistribution:
    None
```

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

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

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

```
Switch# show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
3FFE:C000:0:7::777                         - 0007.0007.0007 REACH 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
```

