



## IPv6 ホスト機能の設定



(注) IPv6 ホスト機能を使用するには、スイッチで LAN ベース イメージが稼動している必要があります。

この章では、Catalyst 2960 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) スヌーピングの設定については、[第 34 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。

デュアル スタック環境 (IPv4 および IPv6 の両方をサポート) をイネーブルにするには、デュアル IPv4 および IPv6 Switch Database Management (SDM; スイッチング データベース管理) 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」\(P.33-5\)](#)を参照してください。



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

この章で説明する内容は、次のとおりです。

- [「IPv6 の概要」\(P.33-2\)](#)
- [「IPv6 の設定」\(P.33-7\)](#)
- [「IPv6 の表示」\(P.33-14\)](#)

## IPv6 の概要

IPv4 ユーザは IPv6 に移行して、エンドツーエンドセキュリティ、Quality Of Service (QoS; サービス品質)、グローバルに一意的なアドレスなどのサービスを利用することができます。IPv6 のアドレス空間の使用により、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 Network Address Translation (NAT; ネットワーク アドレス変換) 処理を使用する必要性が削減されます。

シスコシステムズ製の 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](http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html)

この章に記載されている IPv6 およびその他の機能の詳細については、次の情報を参照してください。

- 次の URL にある『*Cisco IOS IPv6 Configuration Library*』を参照してください。  
[http://www.cisco.com/en/US/docs/ios/12\\_2t/ipv6/ipv6\\_vgf.html](http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html)
- Cisco IOS ソフトウェア マニュアルを検索する場合は、[Search] フィールドを使用してください。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、[Search] フィールドに *Implementing Static Routes for IPv6* と入力するとスタティック ルートに関する次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](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.33-2)
- 「サポート対象の IPv6 ホスト機能」(P.33-3)

## 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、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ません。

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

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

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

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

2 つのコロン (::) を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、次のように各アドレス内で 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 にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章にある以下のセクションの内容は、Catalyst 2960 スイッチに適用されます。

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

## サポート対象の IPv6 ホスト機能

ここでは、スイッチでサポートされている IPv6 プロトコルの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.33-3)
- 「IPv6 DNS」 (P.33-4)
- 「ICMPv6」 (P.33-4)
- 「近接ディスカバリ」 (P.33-4)
- 「デフォルト ルータ プリファレンス」 (P.33-4)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.33-5)
- 「IPv6 アプリケーション」 (P.33-5)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.33-5)
- 「IPv6 による SNMP および Syslog」 (P.33-6)
- 「IPv6 による HTTP (S)」 (P.33-7)

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

### 128 ビット幅のユニキャスト アドレス

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

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

これらのアドレスはグローバルルーティングプレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバルユニキャストアドレス割り当てには、バイナリ値 001 (2000::/3) で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 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。Neighbor Discovery Protocol (NDP; 近接ディスカバリ プロトコル) およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカルリンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章で、IPv6 ユニキャストアドレスに関するセクションを参照してください。

## IPv6 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における 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ており、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; 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、処理やその他の診断機能の実行時のエラーを報告します。IPv6 では、近接ディスカバリ プロトコルおよびパス MTU ディスカバリにも ICMP パケットが使用されます。

## 近接ディスカバリ

スイッチは、IPv6 NDP (ICMPv6 の上位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なネイバー エントリもサポートします。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対する 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。スイッチがアクティブに解決を試みているネイバーと、後続の IPv6 パケットのネクスト ホップが同じ場合、その IPv6 パケットはドロップされます。これにより CPU の余分な負荷を避けられます。

## デフォルト ルータ プリファレンス

スイッチは、ルータのアドバタイズメント 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) をサポートしています。DRP により、適切なルータを選択するホストの機能が向上します。これはホストがマルチホーミングされており、ルータが異なるリンク上にある場合に特に有効です。スイッチでは RFC 4191 の Route Information Option はサポートされていません。

IPv6 ホストはデフォルト ルータ リストを管理し、このリストを使用してオフリンク宛先向けのトラフィックに対応するルータを選択します。宛先に対応するルータを選択すると、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。到達可能であるルータまたは到達可能性の高いルータの場合、NDP は同じルータを毎回選択することもルータ リスト内から順番に選択することもできます。DRP を使用することで、2 台のルータが到達可能である場合または到達可能性が高い場合には、どちらか一方のルータを優先するように IPv6 ホストを設定できます。

IPv6 DRP の詳細については、Cisco.com の『Cisco IOS IPv6 Configuration Library』にある「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

スイッチではステートレス自動設定が使用されるため、ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。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用のアドバタイズメントを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 にある『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 File Transfer Protocol (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; シスコ検出プロトコル) サポート

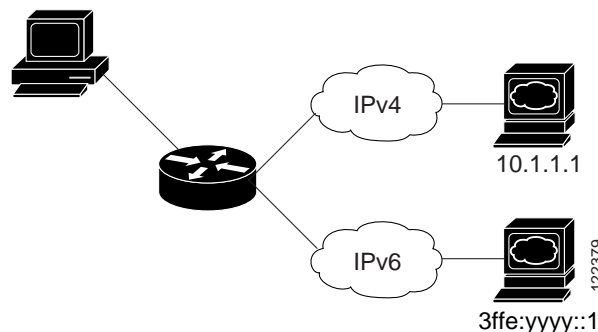
これらのアプリケーションの管理方法に関する詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

## デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方に 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 33-1 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 33-1 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 スタック環境 (IPv4 と IPv6 の両方をサポートする) をイネーブルにするには、デュアル IPv4 および IPv6 スイッチング データベース管理 (SDM) テンプレートを使用します。デュアル IPv4/IPv6 SDM テンプレートの詳細については、第 7 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します。

- 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 QoS および ACL はサポートされていません。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4 および IPv6 のプロトコル スタックの詳細については、Cisco.com にある『*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明示的に定義します。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 にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

## IPv6 による SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 ネットワークの管理に 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 で提供される機能は、次のとおりです。

- IPv4 と IPv6 両方のサポート
- SNMP 用の IPv6 トランスポート、および IPv6 ホストのトラップをサポートするための SNMP エージェントの変更
- IPv6 アドレッシングをサポートする SNMP 関連 MIB および Syslog 関連 MIB
- IPv6 ホストをトラップの受信側にする設定

IPv6 によるサポートの場合、SNMP は既存の IP トランスポート マッピングを変更して IPv4 と IPv6 を同時にサポートします。次の SNMP 処理は、IPv6 トランスポート管理をサポートしています。

- デフォルト設定での UDP SNMP ソケットのオープン
- 新しいトランスポート メカニズム (*SR\_IPV6\_TRANSPORT*) の提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポート対応の SNMP 名前付きアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能が IPv6 トランスポートで動作することの確認

設定手順を含めた IPv6 による SNMP に関する詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含めた IPv6 による Syslog の詳細については、Cisco.com にある『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 および IPv6 HTTP サーバの両方に要求を送信し、HTTP サーバは IPv4 および IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを使用する 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。

アクセプト ソケット コールによって、IPv4 または IPv6 のアドレス ファミリが選択されます。アクセプト ソケットは IPv4 ソケットか IPv6 ソケットのどちらかです。リスニング ソケットは、接続を知らせる IPv4 信号と IPv6 信号の両方を待ち受けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされます。

TCP/IP の基本スタックはデュアル スタック環境をサポートします。HTTP は、ネットワークレイヤの相互作用の処理に TCP/IP スタックとソケットを使用します。

HTTP 接続が可能になるには、クライアントとサーバの間で基本的なネットワーク接続 (ping) が確立している必要があります。

詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」の章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.33-7)
- 「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.33-8)
- 「デフォルト ルータ プリファレンス (DRF) の設定」(P.33-10)
- 「IPv6 ICMP レート制限の設定」(P.33-11)
- 「IPv6 のスタティック ルートの設定」(P.33-12)

## IPv6 のデフォルト設定

表 33-1 に IPv6 のデフォルト設定を示します。

表 33-1 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、スイッチ上で IPv6 トラフィックをグローバルに転送する手順について説明します。

スイッチに IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル Ipv4/IPv6 SDM テンプレートを選択してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドの *ipv6-address* および *ipv6-prefix* 変数は、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで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。

インターフェイス上で 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 にある『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	<b>configure terminal</b>	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	<b>sdm prefer dual-ipv4-and-ipv6 default }</b>	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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>reload</b>	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	<b>configure terminal</b>	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	<b>interface interface-id</b>	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 7	<b>ipv6 address ipv6-prefix/prefix length eui-64</b>  または <b>ipv6 address ipv6-address link-local</b>  または <b>ipv6 enable</b>	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。  インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。  インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合に限定されます。
ステップ 8	<b>exit</b>	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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	<b>show ipv6 interface interface-id</b>	設定を確認します。
ステップ 11	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。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 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。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) を付加する方法を示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# interface fastethernet0/11
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface fastethernet0/11
FastEthernet0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
    Global unicast address(es):
      2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1: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 (DRP) 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 コマンドで設定されたデフォルト ルータ プリファレンス (DRP) と共に送信されます。DRP が設定されていない場合、RA は **medium** プリファレンスで送信されます。

DRP が有効なのは、リンク上の 2 つのルータが同等であっても等コスト ルーティングを提供していない場合で、ポリシーが 2 台のルータのどちらかを優先するように指定しているような場合です。

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	<b>configure terminal</b>	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	<b>interface interface-id</b>	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	<b>ipv6 nd router-preference {high   medium   low}</b>	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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ipv6 interface</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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、ルータの DRP を *high* にしてインターフェイスに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 DRP の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』にある「Implementing IPv6 Addresses 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 [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"> <li><i>interval</i> : 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。</li> <li><i>bucket-size</i> : (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。</li> </ul>
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。

デフォルトの設定に戻すには、`no ipv6 icmp error-interval` グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

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

## IPv6 のスタティック ルートの設定

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

	コマンド	目的
ステップ 1	<b>configure terminal</b>	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	<b>ipv6 route</b> <i>ipv6-prefix/prefix length</i> { <i>ipv6-address</i>   <i>interface-id</i> [ <i>ipv6-address</i> ]} [ <i>administrative distance</i> ]	スタティック IPv6 ルートを設定します。 <ul style="list-style-type: none"> <li>• <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。</li> <li>• <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。</li> <li>• <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。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。</li> <li>• <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、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、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。</li> </ul> <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"> <li>• <i>administrative distance</i> : (任意) 管理ディスタンス。指定できる範囲は 1 ~ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きな管理ディスタンスを使用します。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<p><b>show ipv6 static</b> [<i>ipv6-address</i>   <i>ipv6-prefix/prefix length</i>] [<b>interface</b> <i>interface-id</i>] [<b>recursive</b>] [<b>detail</b>]</p> <p>または</p> <p><b>show ipv6 route static</b> [<i>updated</i>]</p>	<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"> <li>• <b>interface</b> <i>interface-id</i> : (任意) 出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートだけを表示します。</li> <li>• <b>recursive</b> : (任意) 再帰スタティック ルートだけを表示します。<b>recursive</b> キーワードは <b>interface</b> 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。</li> <li>• <b>detail</b> : (任意) 次に示す追加情報を表示します。 <ul style="list-style-type: none"> <li>– 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</li> <li>– 無効なルートの場合、ルートが無効な理由</li> </ul> </li> </ul>
ステップ 5	<b>copy running-config startup-config</b>	(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、管理ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

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

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

## IPv6 の表示

コマンドの構文および使用方法の詳細については、『IOS Command Reference』を参照してください。

表 33-2 に、スイッチ上で IPv6 をモニタリングする特権 EXEC コマンドを示します。

表 33-2 IPv6 のモニタリング 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 <i>interface-id</i></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 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 33-3 に、IPv4 および IPv6 アドレス タイプに関する情報を表示するための特権 EXEC コマンドを示します。

表 33-3 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
<code>show ip http server history</code>	HTTP サーバに対する過去 20 件の接続を表示します。アクセスした IP アドレスおよび接続を終了した時刻が含まれます。
<code>show ip http server connection</code>	HTTP サーバに対する現在の接続を表示します。ローカル IP アドレスおよびアクセスしているリモート IP アドレスが含まれます。
<code>show ip http client connection</code>	HTTP サーバに対する HTTP クライアント接続の設定値を表示します。
<code>show ip http client history</code>	HTTP クライアントがサーバに対して行った最後の 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 protocols** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
    FastEthernet0/4
    FastEthernet0/11
    FastEthernet0/12
Redistribution:
  None
```

次に、**show ipv6 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
  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
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
```