



IPv6 ホスト機能の設定

この章では、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。

IPv4 ユニキャストルーティングの設定方法については、第 35 章「IPv4 ユニキャストルーティングの設定」を参照してください。IPv6 Multicast Listener Discovery (MLD) スヌーピングについては、第 37 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 と IPv6 の両方をサポートしている環境) を使用するには、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを使用するようスイッチを設定する必要があります。「IPv4/IPv6 デュアルプロトコルスタック」(P.36-5) を参照してください。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。



(注)

この章で使用しているコマンドの完全な構文と使用方法については、手順の中で参照している 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.36-1)
- 「IPv6 の設定」(P.36-7)
- 「IPv6 の表示」(P.36-12)

IPv6 の概要

IPv4 ユーザは、IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service (QoS)、グローバルに一意的なアドレスなどのサービスを利用できます。IPv6 では、アドレスレンジが広いため、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。

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

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

IPv6 と、この章で説明しているその他の機能については、次のドキュメント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_c.html
- Cisco IOS ソフトウェアのマニュアルを検索するには、[Search] フィールドを使用します。たとえば、スタティックルートに関する情報を知りたい場合は、検索フィールドに「Implementing Static Routes for IPv6」と入力することにより、スタティックルートに関する次のマニュアルが見つかります。
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/SA_Stat6.html

ここでは、スイッチでの 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.36-2)
- 「サポートされる IPv6 ユニキャスト ホスト機能」 (P.36-2)

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、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、n:n:n:n:n:n という形式で、コロンで区切った 8 個の 16 ビット 16 進数フィールドとして表現します。次に示すのは IPv6 アドレスの例です。

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

より実装しやすくするように、各フィールドの先行するゼロは省略可能です。先行するゼロがないアドレスは次のようになります。

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

また、2 つのコロン (::) を使用して、連続するゼロの 16 進数フィールドを表すこともできますが、この短縮形は各アドレスで 1 回だけ使用できます。

```
2031:0:130F::09C0:80F:130B
```

IPv6 のアドレス形式、アドレスの種類、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」の章で、次のセクションの内容がスイッチに適用されます。

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

サポートされる IPv6 ユニキャスト ホスト機能

以降のセクションでは、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 ワイド ユニキャスト アドレス」 (P.36-3)
- 「IPv6 の DNS」 (P.36-3)
- 「ICMPv6」 (P.36-3)
- 「近接ディスカバリ」 (P.36-4)
- 「Default Router Preference」 (P.36-4)
- 「IPv6 ステートレス自動設定および重複アドレス検出」 (P.36-4)
- 「IPv6 アプリケーション」 (P.36-4)
- 「IPv4/IPv6 デュアルプロトコルスタック」 (P.36-5)
- 「IPv6 のスタティックルート」 (P.36-6)
- 「IPv6 での SNMP と Syslog」 (P.36-6)
- 「IPv6 での HTTP (HTTPS)」 (P.36-6)

スイッチでのサポートには、拡張アドレス機能、ヘッダー形式の単純化、拡張機能およびオプションに対するサポート改善、および拡張ヘッダーのハードウェア解析が含まれています。スイッチでは、ソフトウェアでルーティングまたはブリッジングされるホップバイホップ拡張ヘッダー パケットがサポートされています。

128 ビット ワイド ユニキャスト アドレス

スイッチでは、集約可能グローバル ユニキャスト アドレスおよびリンクローカル 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 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 プレフィクスによる IPv6 アドレスです。このアドレス構造は、ルーティング プレフィクスの厳密な集約を可能にするため、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 エントリ数を制限します。これらのアドレスは、組織を通じて集約され、最終的にインターネット サービス プロバイダーで集約されるリンクに使用されます。

これらアドレスは、グローバル ルーティング プレフィクス、サブネット ID、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 アドレス割り当てでは、バイナリ値 001 (2000::/3) で始まるアドレスの範囲が使用されます。2000::/3 (001) ~ E000::/3 (111) のプレフィクスを持つアドレスは、Extended Unique Identifier (EUI) 64 形式の 64 ビット インターフェイス ID を持つ必要があります。

- リンクローカル ユニキャスト アドレスは、リンクローカル プレフィクス FE80::/10 (1111 1110 10) および修正 EUI 形式のインターフェイス ID を使用して、インターフェイス上に自動的に設定できます。リンクローカルアドレスは、近接ディスカバリ プロトコルとステートレス自動設定プロセスで使用されます。ローカルリンク上のノードは通信にリンクローカルアドレスを使用し、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクローカルな送信元アドレスまたは宛先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 にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章の、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 の DNS

IPv6 では、Domain Name System (DNS; ドメイン ネーム システム) レコードタイプが、DNS の名前からアドレス、アドレスから名前の検索プロセスでサポートされています。DNS AAAA リソースのレコードタイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等のものです。スイッチは、IPv4 と 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、処理や他の診断機能でのエラーをレポートします。IPv6 でも、ICMP パケットは近接ディスカバリ プロトコルおよび Path MTU Discovery で使用されます。

近接ディスカバリ

またスイッチは、ICMPv6 上で動作するプロトコルである IPv6 の NDP と、NDP をサポートしていない IPv6 ステーション用のスタティック ネイバー エントリをサポートします。IPv6 近接ディスカバリ プロセスでは、ICMP メッセージと送信要求ノードの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の判別、ネイバーの到達可能性の検証、および近接ルータのトラッキングを行います。

スイッチは、マスク長が 64 ビット未満のルートの ICMPv6 リダイレクトをサポートします。64 ビット以上のマスク長を持つホスト ルートおよび要約ルートに対する ICMP リダイレクトはサポートされていません。

近接ディスカバリ スロットリングを使用すると、IPv6 パケットをルーティングするためのネクスト ホップ フォワーディング情報を取得する際に、スイッチの CPU が無駄に消費されるのを防ぐことができます。スイッチは、スイッチが頻繁に解決しようとしているネイバーと同じネクスト ホップ宛ての余分な IPv6 パケットをドロップします。これにより、CPU に対する無駄な負荷を減らすことができます。

Default Router Preference

スイッチは、ルータ アドバタイズメント メッセージ中の拡張機能である、IPv6 Default Router Preference (DRP) をサポートしています。DRP を使用することで、特にホストがマルチホーミングされている場合や、ルータが異なるリンク上にある場合に、ホストがより適切なルータを選択できるようになります。スイッチでは、RFC 4191 で規定されている 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 ルート リストを保持しており、そこからオフリンク宛先へのトラフィックのためのルートを選択します。宛先に対して選択されたルータは、宛先キャッシュにキャッシュされます。IPv6 の NDP では、到達可能か到達可能である可能性が高いルータは、到達可能性が不明か疑わしいルータよりも優先されることが規定されています。到達可能か到達可能である可能性が高いルータに対して、NDP は毎回同じルータを選択するか、ルータ リストから順番に選択します。DRP を使用することで、到達可能か到達可能である可能性が高い複数のルータに対して、あるルータを他のルータよりも優先させるように IPv6 ホストを設定できます。

IPv6 の DRP の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 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、ホストおよびモバイル IP アドレスの管理など、リンク、サブネット、サイトのアドレッシングの変更を管理します。ホストは自身のリンクローカルアドレスを自立的に設定します。ブートしようとするノードは、ルータ送信要求を送信して、インターフェイスを設定するためのルータ アドバタイズメントを要求します。

自動設定と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 をサポートしています。

- ping、traceroute、Telnet、TFTP、および FTP
- IPv6 トランスポートでの Secure Shell (SSH; セキュア シェル)
- IPv6 トランスポートでの HTTP サーバアクセス

- IPv4 トランスポートでの AAAA 用 DNS リゾルバ
- IPv6 アドレスに対する Cisco Discovery Protocol (CDP; シスコ検出プロトコル) のサポート

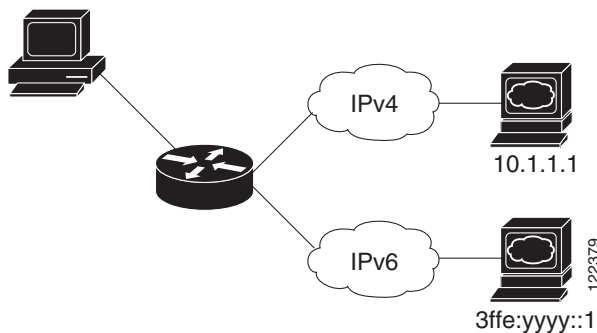
これらのアプリケーションの管理の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv4/IPv6 デュアル プロトコル スタック

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

図 36-1 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 トラフィックおよび IPv6 トラフィックの両方を転送するルータを示します。

図 36-1 インターフェイス上での IPv4 と IPv6 のデュアル サポート



デュアル スタック環境 (IPv4 と IPv6 の両方をサポートしている環境) 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 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ます。

- デュアル IPv4/IPv6 テンプレートを選択せずに 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 のみの環境では、スイッチは IPv4 QoS と ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境では、スイッチは IPv4 QoS と 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。
- IPv6 を使用する予定がない場合は、デュアル スタック テンプレートを使用しないでください。このテンプレートを使用すると、各リソースの TCAM キャパシティが少なくなります。

IPv4 および IPv6 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 台のネットワーク デバイス間の明示的なルートを定義します。スタティック ルートは、外部ネットワークへのパスが 1 つしかない小規模なネットワークや、大規模なネットワークで特定の種類のトラフィックにセキュリティを提供する場合に有効です。

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 での SNMP と Syslog

IPv4 と IPv6 の両方をサポートするために、IPv6 ネットワーク管理では、IPv6 と IPv4 の両方のトランスポートが必要です。IPv6 での Syslog は、これらのトランスポートに対するアドレス データ タイプをサポートしています。

IPv6 での SNMP と Syslog は、次の機能を提供しています。

- IPv4 と IPv6 の両方のサポート
- SNMP の IPv6 トランスポートと IPv6 ホストのトラップをサポートするための SNMP エージェントに対する修正
- IPv6 アドレッシングをサポートするための SNMP と Syslog 関連の MIB
- IPv6 ホストのトラップ受信者としての設定

SNMP では、IPv6 でのサポートのため、既存の IP トランスポート マッピングが、IPv4 と IPv6 を同時にサポートするように変更されています。次の SNMP アクションが IPv6 トランスポート管理をサポートしています。

- User Datagram Protocol (UDP; ユーザ データグラム プロトコル) SNMP ソケットをデフォルトの設定でオープンする。
- `SR_IPV6_TRANSPORT` と呼ばれる新しいトランスポート メカニズムの提供
- IPv6 トランスポート上で SNMP 通知の送信
- IPv6 トランスポート用の 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 フォワーディングのサポート
- 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

設定手順など、IPv6 での SNMP 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。

設定手順など、IPv6 での Syslog 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 での HTTP (HTTPS)

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ます。これらのサーバは、IPv4 と 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 アドレスを使用した URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケットの呼び出しでは、IPv4 または IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットか IPv6 ソケットのいずれかです。リスン中のソケットは、接続を示す IPv4 シグナルと IPv6 シグナルの両方を引き続きリスンします。IPv6 のリスン中のソケットは、IPv6 ワイルドカードアドレスに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 スタックとソケットを使用してネットワーク レイヤの通信を処理します。

HTTP 接続を行う前に、基本的なネットワーク接続性 (**ping**) が、クライアントとサーバ ホストの間に存在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

次のセクションでは、この IPv6 の転送の設定について説明します。

- 「IPv6 のデフォルト設定」(P.36-7)
- 「IPv6 アドレッシングの設定と IPv6 ホストのイネーブル化」(P.36-7)
- 「Default Router Preference の設定」(P.36-9)
- 「IPv6 ICMP レート制限の設定」(P.36-10)
- 「IPv6 のスタティック ルートの設定」(P.36-11)



(注)

スイッチで IPv6 を設定するまえに、`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 コマンドを入力し、スイッチをリロードしてデュアル テンプレートを設定します。

IPv6 のデフォルト設定

表 36-1 に、IPv6 のデフォルト設定を示します。

表 36-1 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	設定なし

IPv6 アドレッシングの設定と IPv6 ホストのイネーブル化

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

スイッチで IPv6 を設定する前に、次の点に注意してください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択します。

- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、*ipv6-address* および *ipv6-prefix* 変数を入力する必要があります。アドレスは、コロンで区切られた 16 ビット値を使用して 16 進数で指定します。スラッシュ [/] が前に付いている *prefix-length* 変数は、10 進数値で、アドレスの上位連続ビットのうち何ビットでプレフィクス（アドレスのネットワーク部分）を構成しているかを示します。

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上にグローバル 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、自動的にリンクローカルアドレスが設定されて、インターフェイスで IPv6 がアクティブ化されます。設定されたインターフェイスは、次のような、その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に対する、送信要求ノード マルチキャスト グループ FF02:0:0:0:1:ff00::/104（このアドレスは近接ディスカバリ プロセスで使用されます）
- 全ノードのリンクローカル マルチキャスト グループ FF02::1
- 全ルータのリンクローカル 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。

IPv6 アドレスをレイヤ 3 インターフェイスに割り当てて 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	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ためにスイッチをデフォルトのテンプレートに設定します。 • routing : IPv4 および IPv6 トラフィックをサポートするため、スイッチをルーティング テンプレートに設定します。 • vlan : スイッチでの VLAN 設定を最大化します。
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	スイッチがリロードされた後にグローバル コンフィギュレーション モードを開始します。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。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)、レイヤ 3 EtherChannel のうちいずれかを指定できます。
ステップ 7	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）。

コマンド	目的
ステップ 8 ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	IPv6 アドレスの下位 64 ビットで Extended Unique Identifier (EUI) 形式のグローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最後の 64 ビットはスイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイスでの IPv6 処理がイネーブルになります。 インターフェイスで IPv6 をイネーブルにしたときに自動的に設定されるリンクローカルアドレスではなく、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、インターフェイスでの IPv6 処理がイネーブルになります。 インターフェイスで自動的に IPv6 リンクローカルアドレスを設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクローカルアドレスは、同一リンク内のノードとの通信だけに使用できます。
ステップ 9 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 10 end	特権 EXEC モードに戻ります。
ステップ 11 show ipv6 interface interface-id	設定を確認します。
ステップ 12 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** 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。次に、インターフェイス上で IPv6 ホストをイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/11
Switch(config-if)# no switchport
Switch(config-if)# ipv6 enable
Switch(config-if)# exit
```

Default Router Preference 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 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 は中程度の優先度で送信されます。

DRP は、リンク上の 2 台のルータによって、同等の、しかし等コストでないルーティングが提供され、ホストでいずれかのルータを優先するようにポリシーで指定されている場合に有効です。

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

コマンド	目的
ステップ 1 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、DRP を指定するレイヤ 3 インターフェイスを入力します。

	コマンド	目的
ステップ 3	<code>ipv6 nd router-preference {high medium low}</code>	スイッチ インターフェイス上のルータに対して DRP を指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ipv6 interface</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、インターフェイス上のルータに対して、DRP に *high* を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 の DRP の設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「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になっています。デフォルトのエラー メッセージ間隔は 100 ミリ秒、バケット サイズ (バケットに格納できる最大トークン数) 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 メッセージの間隔とバケット サイズを設定します。 <ul style="list-style-type: none"> <i>interval</i> : トークンがバケットに追加される間隔 (ミリ秒単位)。指定できる範囲は 0 ~ 2147483647 ミリ秒です。 <i>bucketsize</i> : (任意) バケットに格納されるトークンの最大数。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 ミリ秒でバケット サイズを 20 トークンにする例を示します。

```
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、少なくとも 1 つのレイヤ 3 インターフェイスで IPv6 アドレスを設定することで IPv6 をイネーブルにする必要があります。

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

	コマンド	目的
ステップ 1	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 ルートの宛先である IPv6 ネットワーク。スタティック ホストルートが設定されている場合はホスト名を指定することもできます。 <i>/prefix length</i> : IPv6 プレフィックスの長さ。アドレスの上位連続ビットのうち何ビットでプレフィックス (アドレスのネットワーク部分) を構成しているかを示す 10 進数値。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> : 指定されたネットワークへの到達に使用できるネクストホップの IPv6 アドレス。ネクストホップの IPv6 アドレスは直接接続が不要で、直接接続されているネクストホップの IPv6 アドレスを検索するために再帰が実行されます。アドレスは、RFC 2373 に規定された形式である必要があり、16 ビットの値をコロンで区切った 16 進数で指定されます。 <i>interface-id</i> : ポイントツーポイントおよびブロードキャストインターフェイスからの直接スタティック 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では、ネクストホップの IPv6 アドレスを指定する必要がありません。ブロードキャストインターフェイスでは、常にネクストホップ用の IPv6 アドレスを指定するか、指定したプレフィックスがリンクに割り当てられ、ネクストホップとしてリンクローカルアドレスを指定していることを確認する必要があります。必要に応じてパケットの送信先となるネクストホップの IPv6 アドレスを指定できます。 <p>(注) リンクローカルアドレスをネクストホップとして使用する場合、<i>interface-id</i> を指定しなければなりません (リンクローカルネクストホップは隣接ルータでなければなりません)。</p> <ul style="list-style-type: none"> <i>administrative distance</i> : (任意) 管理距離。範囲は 1 ~ 254 で、デフォルト値は 1 です。この場合、接続されているルートを除く他のタイプのルートよりも、スタティックルートが優先されます。フローティングスタティックルートを設定するには、ダイナミックルーティングプロトコルよりも大きい管理距離を指定します。
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 show ipv6 static [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>] [interface <i>interface-id</i>] [recursive] [detail] または show ipv6 route static [<i>updated</i>]	IPv6 ルーティング テーブルの内容を表示して設定を確認します。 <ul style="list-style-type: none"> • interface <i>interface-id</i> : (任意) 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いるスタティック ルートだけを表示します。 • recursive : (任意) 再帰的なスタティック ルートだけを表示します。recursive キーワードは、interface キーワードと同時に指定できませんが、コマンド構文に含まれる IPv6 プレフィクス付きでもプレフィクスなしでも使用できます。 • detail : (任意) 次の追加情報を表示します。 <ul style="list-style-type: none"> – 有効な再帰的ルートの場合、出力パス セット、および最大解決深度 – 無効なルートの場合、ルートが無効である理由
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定したスタティック 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 gigabitethernet0/1 130
```

IPv6 スタティック 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

これらのコマンドの完全な構文と使用方法については、Cisco IOS コマンド リファレンスを参照してください。

表 36-2 に、スイッチで IPv6 をモニタリングするための特権 EXEC コマンドを示します。

表 36-2 IPv6 のモニタリング用コマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 interface <i>interface-id</i>	IPv6 インターフェイス ステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとの IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 36-3 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 36-3 IPv4 および IPv6 アドレス タイプを表示するためのコマンド

コマンド	目的
show ip http server history	HTTP サーバへの最近の 20 件の接続を表示します。アクセスした IP アドレスと接続を閉じた時間が含まれます。
show ip http server connection	HTTP サーバへの現在の接続を表示します。アクセス中のローカルおよびリモートの IP アドレスが含まれます。
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実行された最近の 20 件の要求の一覧を表示します。

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
    GigabitEthernet0/4
    GigabitEthernet0/11
    GigabitEthernet0/12
  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 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

```