



IPv6 ユニキャスト ルーティングの設定

この章では、Catalyst 3750 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。



(注)

この章で説明するすべての IPv6 機能を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。IP ベース イメージが稼動しているスイッチでは、IPv6 スタティック ルーティングと IPv6 RIP だけがサポートされます。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、第 40 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 41 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 38 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; スイッチ データベース管理) テンプレートを使用するように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.39-6) 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。

- 「IPv6 の概要」(P.39-1)
- 「IPv6 の設定」(P.39-12)
- 「IPv6 の表示」(P.39-29)

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)、グローバルに一意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。

シスコシステムズの IPv6 の実装方法については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 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
- Cisco IOS ソフトウェア マニュアルを検索する場合は、[検索] 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、[検索] フィールドに *Implementing Static Routes for IPv6* と入力すればスタティック 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

次の項では、スイッチの IPv6 実装について説明しています。

- 「IPv6 アドレス」(P.39-2)
- 「サポート対象の IPv6 ユニキャストルーティング機能」(P.39-3)
- 「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.39-10)
- 「制限事項」(P.39-10)
- 「IPv6 とスイッチ スタック」(P.39-11)

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、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」の章にある次の項の内容は、Catalyst 3750 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.39-3)
- 「IPv6 DNS」 (P.39-4)
- 「IPv6 ユニキャストのパス MTU ディスカバリ」 (P.39-4)
- 「ICMPv6」 (P.39-4)
- 「ネイバー ディスカバリ」 (P.39-4)
- 「デフォルト ルータ プリファレンス」 (P.39-5)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.39-5)
- 「IPv6 アプリケーション」 (P.39-5)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.39-6)
- 「IPv6 DHCP アドレス割り当て」 (P.39-6)
- 「IPv6 のスタティック ルート」 (P.39-7)
- 「IPv6 RIP」 (P.39-7)
- 「IPv6 OSPF」 (P.39-7) (IP サービス イメージを稼動しているスイッチに限り)
- 「OSPFv3 グレースフル リスタート」 (P.39-8) (IP サービス イメージを稼動しているスイッチに限り)
- 「EIGRP IPv6」 (P.39-8) (IP サービス イメージを稼動しているスイッチに限り)
- 「HSRP IPv6」 (P.39-8) (IP サービス イメージを稼動しているスイッチに限り)
- 「IPv6 による SNMP および Syslog」 (P.39-9)
- 「IPv6 による HTTP (S)」 (P.39-9)

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。

スイッチは、ネイティブ イーサネット Inter-Switch Link (ISL) または 802.1Q トランク ポートによる IPv6 ルーティング機能 (スタティック ルートの場合)、IPv6 対応の Routing Information Protocol (RIP)、および Open Shortest Path First (OSPF) バージョン 3 プロトコルを提供します。等価コスト ルートは 16 までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

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。プレフィクスが 2000::/3 (001) ~ E000::/3 (111) のアドレスには、Extended Unique Identifier (EUI; 拡張固有識別子) -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) 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 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。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチは、IPv6 ノードへのシステム Maximum Transmission Unit (MTU; 最大伝送ユニット) のアドバタイズメントおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータパス上のすべてのリンクの MTU サイズを動的に検出して、サイズに合わせて調整することができます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケットサイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャストパケットのパス MTU ディスカバリをサポートしません。

ICMPv6

IPv6 の Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) は、ICMP 宛先到達不能メッセージなどのエラーメッセージを生成して、処理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、ネイバー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。

ネイバー ディスカバリ

スイッチは、IPv6 NDP (ICMPv6 の上位で稼働するプロトコル)、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、ネイバー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。

ネイバー 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、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 ルータの初期設定) 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 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 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、および TFTP
- 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

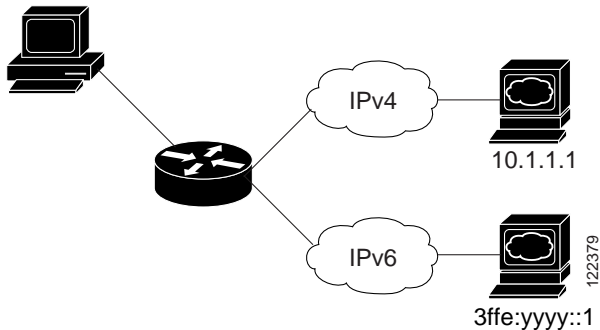
これらのアプリケーションの管理方法に関する詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

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 Ternary Content Addressable Memory (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 39-1 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 39-1 インターフェイス上での IPv4/IPv6 のデュアル サポート



IPv6 ルーティングをイネーブлにするには、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 デスクトップおよびアグリゲータ 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 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境のスイッチは、IPv4 および IPv6 パケットをルーティングし、IPv4 QoS をハードウェアで適用します。
- IPv6 QoS のすべてはサポートされていません。IPv6 QoS trust はサポートされています。
- 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 DHCP アドレス割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能により、ホストが接続されているネットワークに基づいた適切なプレフィクスで重複のないアドレス割り当てが行われます。アドレスは 1 つまたは複数のプレフィクス プールから割り当てることができます。デフォルト ドメインや DNS ネーム サーバアドレスなどのオプションもクライアントに渡すことができます。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で使用されるように割り当てたり、サーバが自動的に適切なプールを選択することもできます。

Cisco IOS Release 12.2(58)SE 以降、IP ベースのフィーチャ セットが稼動しているスイッチは次の機能をサポートします。

- DHCPv6 バルクリース クエリー

DHCPv6 バルクリース クエリーを使用すると、クライアントが DHCPv6 バインディングに関する情報を要求できるようになります。この機能により、新しいクエリー タイプが追加され、TCP を介した DHCPv6 バインディング データのバルク転送が可能になります。DHCPv6 バインディング データのバルク転送は、リレー サーバスイッチがリブートされ、リレー サーバがすべてのバインディング情報を失った場合に役に立ちます。リブート後に、リレー サーバはバルクリース クエリーを生成して DHCP サーバからバインディング情報を取得します。

- DHCPv6 リレー送信元設定

DHCPv6 サーバは DHCP リレー エージェントの送信元アドレスに応答します。一般的に、DHCPv6 リレー エージェントからのメッセージは送信元のインターフェイスの送信元アドレスを示します。DHCPv6 リレー送信元設定機能を使用すると、リレー エージェントからのメッセージの送信元アドレスとして、より安定したアドレス（ループバック インターフェイスなど）を設定できます。送信元アドレスは、スイッチに対してグローバルに設定したり、特定のインターフェイスに対して設定したりできます。インターフェイスに設定されたアドレスは、グローバルで設定されたものよりも優先されます。

これらの機能の詳細と設定方法については、『[Cisco IOS IPv6 Configuration Guide, Release 12.4](#)』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてのみ説明しています。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 にある『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーク デバイス間のルートを示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com 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 RIP

IPv6 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距離ベクトル型プロトコルです。このプロトコルには、IPv6 アドレスおよび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サポートする機能などがあります。

IPv6 RIP の詳細については、Cisco.com にある『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF

IP サービス イメージが稼動するスイッチは IP のリンクステートプロトコルの IPv6 Open Shortest Path First (OSPF) をサポートしています。詳細については、Cisco.com で入手可能な『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing OSPF for IPv6」の章を参照してください。

OSPFv3 グレースフル リスタート

Cisco IOS Release 12.2(58)SE 以降、IP サービス フィーチャ セットが稼動しているスイッチは OSPFv3 のグレースフル リスタート機能をサポートします。この機能を使用すると、OSPFv3 ルーティング プロトコル情報が復元され、既知のルートでノンストップ データ フォワーディングが可能になります。スイッチは、グレースフル リスタートをリスタート モード（グレースフルリスタート対応スイッチの場合）またはヘルパー モード（グレースフルリスタート認識スイッチの場合）のいずれかで使用します。

グレースフル リスタート機能を使用するには、スイッチがハイアベイラビリティ **Stateful Switchover (SSO; ステートフル スイッチオーバー)** モード（デュアル ルート プロセッサ）である必要があります。グレースフル リスタート対応のスイッチは、次の障害が発生したときにグレースフル リスタートを使用します。

- スタンバイ ルート プロセッサにチェンジオーバーするルート プロセッサ障害
- スタンバイ ルート プロセッサへの計画されたルート プロセッサ チェンジオーバー

グレースフル リスタート機能を使用するには、ネイバー スイッチがグレースフルリスタート認識である必要があります。

詳細については、Cisco.com で入手可能な『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

EIGRP IPv6

Switches running the IP サービス イメージが稼動しているスイッチは、IPv6 対応の Enhanced Interior Gateway Routing Protocol (EIGRP) をサポートします。EIGRP IPv6 はこのプロトコルを実行するインターフェイスに設定され、グローバル IPv6 アドレスは必要ありません。



(注)

IP ベース イメージが稼動しているスイッチは、IPv6 EIGRP スタブ ルーティングを含むすべての IPv6 EIGRP 機能をサポートしません。

EIGRP IPv6 のインスタンスを実行するには、明示的または黙示的なルータ ID が必要です。黙示的なルータ ID はローカル IPv4 アドレスから抽出されるため、どの IPv4 ノードにも必ず利用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけのネットワークで実行されていることがあり、利用可能な IPv4 ルータ ID がないこともあります。

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

HSRP IPv6

IP サービス イメージが稼動するスイッチは、IPv6 対応の Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) をサポートします。HSRP は、IPv6 トラフィック ルーティングに冗長性を提供し、1 台のルータのアベイラビリティに依存しないルーティングを可能にします。IPv6 ホストは、IPv6 ネイバー ディスカバリ ルータ アドバタイズメント メッセージを介して利用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされる場合と、ホストによって送信請求される場合があります。

HSRP IPv6 グループは、HSRP グループ番号から抽出される仮想 MAC アドレスと、デフォルトで HSRP 仮想 MAC アドレスから抽出される仮想 IPv6 リンクローカル アドレスを持っています。HSRP グループがアクティブな場合、HSRP 仮想 IPv6 リンクローカル アドレスにメッセージが定期的に送信されます。グループがアクティブでなくなる際に最後のメッセージが送信され、メッセージは停止します。

IPv6 HSRP の設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in 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 User Datagram Protocol (UDP; ユーザ データグラム プロトコル) 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 ファミリーが選択されます。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。

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

スイッチは、次の IPv6 機能をサポートしていません。

- IPv6 ポリシーベース ルーティング
- IPv6 Virtual Private Network (VPN; バーチャル プライベート ネットワーク) Routing And Forwarding (VRF; VPN ルーティングおよび転送) テーブルのサポート
- 次の IPv6 ルーティング プロトコルのサポート：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) および Intermediate System-to-Intermediate System (IS-IS) ルーティング
- サイトローカルなアドレス宛の IPv6 パケット
- IPv4/IPv6 や 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 RPF
- IPv6 の一般的なプレフィクス

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いくつかの制限があります。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。

- IPv6 ホスト ルート (特定のホストに到達するために使用されるルート) またはマスク長が 64 ビットを超える IPv6 ルートでは、ICMPv6 リダイレクト機能がサポートされません。スイッチは、ホスト ルートを介して、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の場合、より適したファースト ホップ ルータにホストをリダイレクトすることができません。
- IPv6 ホスト ルートまたはマスク長が 64 ビットを超える IPv6 ルートには、等価コストおよび不等価コスト ルートを使用するロード バランシングがサポートされません。
- スイッチは、SNAP でカプセル化された IPv6 パケットを転送できません。



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

- スイッチは、IPv6/IPv4 および IPv4/IPv6 パケットをハードウェアでルーティングしますが、スイッチを IPv6/IPv4 または IPv4/IPv6 トンネル エンドポイントにはできません。
- ホップ単位の拡張ヘッダーを持つブリッジング済みの IPv6 パケットは、ソフトウェアで転送されます。IPv4 の場合、これらのパケットはソフトウェアでルーティングされ、ハードウェアでブリッジングされます。
- ソフトウェア コンフィギュレーション ガイドで定義された標準の SPAN および RSPAN 制限のほかに、次のような IPv6 パケット固有の制限事項があります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスに誤りが生じることがあります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスに誤りが生じることがあります。標準トラフィックは影響を受けません。

- スイッチはソースルート IPv6 パケットに関する QoS 分類または PBR 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 とスイッチ スタック

スイッチは、スタック全体への IPv6 フォワーディングとスタック マスター上の IPv6 ホスト機能をサポートしています。スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。Distributed CEF (dCEF; 分散 CEF) を使用して、スタック マスターはルーティング テーブルをスタック メンバー スイッチにダウンロードします。メンバー スイッチはテーブルを受信し、転送用のハードウェア IPv6 ルートを作成します。スタック マスターはすべての IPv6 アプリケーションも実行します。



(注)

IPv6 パケット ルーティングをスタック内で機能させるために、スタック内のすべてのスイッチで IP サービス イメージを実行している必要があります。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。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。スタックの MAC アドレスが変わると、IPv6 アドレスも変わります。 `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; 拡張固有識別子) でスタックの IPv6 アドレスを指定すると、インターフェイス MAC アドレスに基づいたアドレスになります。「[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.39-12) 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 5 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.5-20) を参照してください。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
 - IPv6 ルーティング プロトコルの実行
 - ルーティング テーブルの生成
 - dCEFv6 を使用するスタック メンバーへの CEFv6 ルーティング テーブルの配布
 - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタック メンバー (IP サービス イメージを実行している必要があります)
 - スタック マスターからの CEFv6 ルーティング テーブルの受信
 - ハードウェアへのルートのプログラミング



(注)

IPv6 パケットに例外 (IPv6Option) がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

- マスターの再選択での CEFv6 テーブルのフラッシュ

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.39-12)
- 「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.39-12)
- 「デフォルト ルータ プリファレンスの設定」(P.39-15)
- 「IPv4 および IPv6 プロトコル スタックの設定」(P.39-16)
- 「DHCP 設定による IPv6 アドレス割り当て」(P.39-17)
- 「IPv6 ICMP レート制限の設定」(P.39-21)
- 「IPv6 の CEF および dCEF の設定」(P.39-21)
- 「IPv6 のスタティック ルートの設定」(P.39-22)
- 「IPv6 RIP の設定」(P.39-23)
- 「IPv6 OSPF の設定」(P.39-24)
- 「EIGRP IPv6 の設定」(P.39-26)
- 「IPv6 HSRP の設定」(P.39-26)

IPv6 のデフォルト設定

表 39-1 に IPv6 のデフォルト設定を示します。

表 39-1 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	デフォルトのデスクトップまたはデフォルトのアグリゲータ (Catalyst3750-12S)
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 CEF および dCEF 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
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、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。
- この章に記載されたすべての機能が、IP サービス イメージが稼動している Catalyst 3750 スイッチでサポートされているわけではありません。「サポートされていない IPv6 ユニキャストルーティング機能」(P.39-10) 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 (このアドレスはネイバー 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 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 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} [desktop]	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 <ul style="list-style-type: none"> • default : スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • routing : IPv4 PBR などの IPv4 および IPv6 ルーティングをサポートするため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。 desktop : デスクトップ テンプレートの 1 つをスイッチに設定するために Catalyst 3750-12S アグリゲータ スイッチでのみサポートされます。アグリゲータ スイッチでこの設定が選択されなかった場合、アグリゲータ テンプレートが自動的に選択されます。
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、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 Intertface (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	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/prefix length または ipv6 address ipv6-address link-local または ipv6 enable	IPv6 アドレスの下位 64 ビットの Extended Unique Identifier (EUI; 拡張固有識別子) 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 アドレスを手動で設定します。 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 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 ip routing	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11 ipv6 unicast-routing	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 end	特権 EXEC モードに戻ります。
ステップ 13 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。

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)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/0/1
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 gigabitethernet1/0/1
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):
```

```

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	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。
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、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 gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end

```

IPv6 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。

IPv4 および IPv6 プロトコルスタックの設定

IPv6 ルーティングを設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。まだ設定していない場合、**sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan} [desktop]** 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。新規テンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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	ip routing	スイッチ上でルーティングをイネーブルに設定します。
ステップ 3	ipv6 unicast-routing	スイッチ上で 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 4	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 5	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 6	ip address ip-address mask [secondary]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	グローバル IPv6 アドレスを指定します。ネットワークプレフィクスだけを指定します。最終の 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。 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 ローカルアドレスでなく、インターフェイスで特定のリンク ローカルアドレスを使用するように指定します。 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	end	特権 EXEC モードに戻ります。
ステップ 9	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 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。

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 IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet2/0/1
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 設定による IPv6 アドレス割り当て

ここでは、IPv6 DHCP (DHCPv6) アドレス割り当ての設定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.39-17)
- 「DHCPv6 アドレス割り当て設定の注意事項」 (P.39-17)
- 「DHCPv6 サーバ機能のイネーブル化」 (P.39-18)
- 「DHCPv6 クライアント機能のイネーブル化」 (P.39-20)

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、次の注意事項に従ってください。

- 次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
 - レイヤ 3 インターフェイス上で DHCPv6 IPv6 ルーティングをイネーブルにする必要があります。
 - 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 チャンネル: **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ン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; スイッチ データベース管理) テンプレートを選択する必要があります。
- DHCPv6 クライアント、サーバ、またはリレー エージェントはマスター スイッチ上でのみ稼働します。スタック マスターの再選出が行われると、新しいマスター スイッチが DHCPv6 設定を保持します。ただし、DHCP サーバ データベースのリース情報のローカル RAM コピーは保持されません。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバ機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 dhcp pool <i>poolname</i></code>	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。プール名には、文字列（例：Engineering）または整数（例：0）を使用できます。
ステップ 3	<code>address prefix <i>IPv6-prefix</i> lifetime {<i>t1 t1</i> infinite}</code>	(任意) アドレス割り当てのアドレス 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。 lifetime <i>t1 t1</i> : IPv6 アドレス プレフィックスが有効になっている期間（秒）を指定します。指定できる範囲は 5 ~ 4294967295 秒です。無期限の場合は infinite を指定します。
ステップ 4	<code>link-address <i>IPv6-prefix</i></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上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すると、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。
ステップ 5	<code>vendor-specific <i>vendor-id</i></code>	(任意) ベンダー固有コンフィギュレーション モードを開始し、ベンダー固有の識別番号を入力します。この番号はベンダーの IANA 民間企業番号です。指定できる範囲は 1 ~ 4294967295 です。
ステップ 6	<code>suboption number {address <i>IPv6-address</i> ascii <i>ASCII-string</i> hex <i>hex-string</i>}</code>	(任意) ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ~ 65535 です。サブオプションパラメータの定義に従って IPv6 アドレス、ASCII テキスト、または 16 進形式の文字列を入力します。
ステップ 7	<code>exit</code>	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface <i>interface-id</i></code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

コマンド	目的
ステップ 10 ipv6 dhcp server [<i>poolname</i> automatic] [rapid-commit] [<i>preference value</i>] [allow-hint]	インターフェイスで DHCPv6 サーバ機能をイネーブルにします。 <ul style="list-style-type: none"> • poolname : (任意) IPv6 DHCP プールのユーザ定義名。プール名には、文字列 (例: Engineering) または整数 (例: 0) を使用できます。 • automatic : (任意) クライアントにアドレスを割り当てる際に、使用するプールをシステムが自動的に決定できるようにします。 • rapid-commit : (任意) 2 メッセージ交換方式を許可します。 • preference value : (任意) サーバの送信するアドバタイズ メッセージ内のプリファレンス オプションで伝送されるプリファレンス値。指定できる範囲は 0 ~ 255 です。プリファレンス値のデフォルトは 0 です。 • allow-hint : (任意) サーバが SOLICIT メッセージに含まれたクライアントの提示内容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提示内容を無視します。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show ipv6 dhcp pool または show ipv6 dhcp interface	DHCPv6 プールの設定を確認します。 インターフェイスで DHCPv6 サーバ機能がイネーブルになっていることを確認します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool poolname** グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、DHCP プール コンフィギュレーション モード コマンドの **no** 形式を使用します。インターフェイス上の DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレス プレフィックスを持つ *engineering* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 つのリンクアドレスと 1 つの IPv6 アドレス プレフィックスを持つ *testgroup* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次に、ベンダー固有のオプションを持つ *350* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
```

```
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

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

	コマンド	目的
ステップ 1	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。
ステップ 3	ipv6 address dhcp [rapid-commit]	DHCPv6 サーバから IPv6 アドレスを取得するようにインターフェイスを設定します。 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	ipv6 dhcp client request [vendor-specific]	(任意) ベンダー固有のオプションを要求するようにインターフェイスを設定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ipv6 dhcp interface	インターフェイスで DHCPv6 クライアント機能がイネーブルになっていることを確認します。

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

次に、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例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
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のみ説明しています。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 にある『Cisco IOS IPv6 Configuration Library』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。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 CEF および dCEF の設定

Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) は、ネットワーク パフォーマンスを向上させるレイヤ 3 IP スイッチング技術です。Catalyst 3750 スイッチ スタックでは、ハードウェアはスタックの Distributed CEF (dCEF; 分散 CEF) を使用します。IPv6 CEF および dCEF はデフォルトでディセーブルになっていますが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、最初に `ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケット フォワーディングをグローバルに設定する必要があります。そして、`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 または dCEF をディセーブルにするには、`no ipv6 cef` または `no ipv6 cef distributed` 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 をディセーブルにした後に再びイネーブルにするには、`ipv6 cef` または `ipv6 cef distributed` 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 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 ルートの設定

スタティック IPv6 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、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>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 プレフィックスの長さ。プレフィックス (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。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ッ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	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) 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、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 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 RIP の設定

IPv6 RIP を実行するようにスイッチを設定する前に、**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、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 をイネーブルにする必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須および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。
ステップ 6	<pre>ipv6 rip name enable</pre>	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。

	コマンド	目的
ステップ 7	<code>ipv6 rip name default-information {only originate}</code>	<p>(任意) IPv6 デフォルト ルート (::/0) を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。</p> <p>(注) 任意のインターフェイスから IPv6 デフォルト ルート (::/0) を送信した後に、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。</p> <ul style="list-style-type: none"> • only : デフォルト ルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • originate : デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show ipv6 rip [name] [interface interface-id] [database] [next-hops]</code> または <code>show ipv6 route rip [updated]</code>	IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをディセーブルにするには、**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、*cisco* という RIP ルーティング プロセスを最大等価コスト ルート数 8 で設定し、それをインターフェイス上でイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 RIP 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 RIP for IPv6」の章を参照してください。

IPv6 OSPF の設定

使用するネットワークに合わせて IPv6 OSPF をカスタマイズできます。ただし、IPv6 OSPF のデフォルト設定は、ほとんどのユーザおよび機能の要件を満たすように設定されています。

次の注意事項に従ってください。

- スイッチで IP サービス イメージが稼動している必要があります。
- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、**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、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 をイネーブルにする必要があります。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須および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。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ~ 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]	(任意) エリア境界でルートを統合し、サマライズします。 <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 プレフィクスのどちらかを指定できます。 • 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。10 進値の前にスラッシュ (/) を付加する必要があります。 • 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。Type3 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 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。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	ipv6 ospf process-id area area-id [instance instance-id]	インターフェイス上で IPv6 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	end	特権 EXEC モードに戻ります。
ステップ 9	show ipv6 ospf [process-id] [area-id] interface [interface-id] または show ipv6 ospf [process-id] [area-id]	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	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。

OSPF ルーティング プロセスをディセーブルするには、**no ipv6 router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して OSPF ルーティング プロセスをディセーブルにするには、**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 OSPF 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 OSPF for IPv6」の章を参照してください。

EIGRP IPv6 の設定

インターフェイスで **ipv6 router eigrp as-number** コマンドと **ipv6 eigrp as-number** コマンドを設定する場合、IPv6 対応 EIGRP はイネーブルになります。

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、**eigrp router-id ip-address** コマンドを使用します。

スイッチで IP サービス イメージが稼動している必要があります。

EIGRP IPv4 の場合と同じように、EIGRP IPv6 でも EIGRP IPv4 インターフェイスを指定してからその一部を受動インターフェイスとして選択できます。その場合は **passive-interface default** コマンドを使用してすべてのインターフェイスを受動にしてから、アクティブにするインターフェイスを指定して **no passive-interface** コマンドを使用します。受動インターフェイス上に 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 IOS IPv6 Configuration Guide』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 HSRP の設定

Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) IPv6 は、IPv6 トラフィックのルーティングに冗長性を提供し、1 台のルータの可用性に依存しないルーティングを可能にします。

スイッチで IPv6 HSRP がイネーブルの場合、IPv6 ホストは IPv6 ネイバー ディスカバリ ルータ アドバタイズメント メッセージを介して利用可能な IPv6 ルータを学習します。HSRP の IPv6 グループは、HSRP グループ番号から抽出される仮想 MAC アドレスを持っています。また、このグループは仮想 IPv6 リンクローカルアドレスを持っています。このアドレスはデフォルトで HSRP 仮想 MAC アドレスから抽出されます。HSRP グループがアクティブな場合、HSRP 仮想 IPv6 リンクローカルアドレスにメッセージが定期的送信されます。

スイッチで IP サービス イメージが稼動している必要があります。

IPv6 HSRP を設定する場合は、インターフェイス上で HSRP バージョン 2 (HSRPv2) をイネーブルにする必要があります。

HSRPv1 および HSRPv2 を使用する IPv6 HSRP を設定する際の設定上の注意事項については、「[HSRP 設定時の注意事項](#)」(P.42-6) および「[HSRP のトラブルシューティング](#)」(P.42-13) を参照してください。

IPv6 HSRP および HSRPv2 の詳細については、[第 42 章「HSRP および VRRP の設定」](#)を参照してください。



(注)

IPv6 HSRP グループを設定する前に、**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 パケットの転送をイネーブルにし、IPv6 HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにします。

HSRP バージョン 2 のイネーブル化

レイヤ 3 インターフェイス上で HSRP バージョン 2 をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	<code>standby version {1 2}</code>	2 を入力して HSRP バージョンを変更します。デフォルト値は 1 です。
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 standby</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。

HSRP IPv6 グループのイネーブル化

レイヤ 3 インターフェイス上で IPv6 HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、IPv6 HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	<code>standby [group-number] ipv6 {link-local-address autoconfig}</code>	IPv6 HSRP グループを作成 (またはイネーブルに) します。 <ul style="list-style-type: none"> (任意) <i>group-number</i> : HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 4095 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 ホットスタンバイ ルータ インターフェイスのリンクローカルアドレスを入力するか、または、リンクローカルプレフィクスと変更済み EUI-64 フォーマットのインターフェイス識別情報からリンクローカルアドレスが自動的に生成されるように設定にします。EUI-64 インターフェイス識別情報は、関連する HSRP 仮想 MAC アドレスから作成されます。

	コマンド	目的
ステップ 4	<code>standby [group-number] preempt [delay {minimum seconds reload seconds sync seconds}]</code>	<p>ルータを preempt に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。</p> <ul style="list-style-type: none"> （任意） group-number : コマンドが適用されるグループ番号です。 （任意） delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒です（1 時間）。デフォルトは 0 です（遅延なしで引き継ぎます）。 （任意） reload : リロード後のプリエンプト遅延を秒数で設定します。この遅延時間は、ルータのリロード後初めてインターフェイスがアップになる際にのみ適用されます。 （任意） sync : IP 冗長クライアントの最大同期化時間を秒数で設定します。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 5	<code>standby [group-number] priority priority</code>	<p>アクティブ ルータを選択するときに使用される priority 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルトのプライオリティは 100 です。最大の値が、最高のプライオリティを表します。</p> <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show standby [interface-id [group-number]]</code>	設定を確認します。
ステップ 8	<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 HSRP をディセーブルにするには、**no standby [group-number] ipv6** 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、ポートのグループ 1 で IPv6 HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、IPv6 HSRP を使用して学習されます。



(注)

これは、IPv6 HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

IPv6 HSRP の設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 の表示

コマンドの構文と使い方については『Cisco IOS Command Reference』を参照してください。

表 39-2 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 39-2 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 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 39-3 に、EIGRP IPv6 情報を表示するための特権 EXEC コマンドを示します。

表 39-3 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 が検出し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 39-4 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 39-4 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。

表 39-4 IPv4 および IPV6 アドレス タイプを表示するコマンド (続き)

コマンド	目的
<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 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
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
  None
```

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

```
Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
  Administrative distance is 120.Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
    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
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```