



IPv6 ユニキャスト ルーティングの設定

この章では、IE 3000 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)

この章のすべての IPv6 機能を使用するには、スイッチスタックで IP サービス イメージを実行している必要があります。IP ベース イメージを実行するスイッチは、IPv6 スタティック ルーティングおよび IPv6 用の RIP だけをサポートしています。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、[第 43 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; アクセス制御リスト) の設定については、[第 44 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 41 章「IP ユニキャスト ルーティングの設定」](#)を参照してください。

IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを使用するように、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」\(P.42-5\)](#)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」\(P.42-2\)](#)
- [「IPv6 の設定」\(P.42-10\)](#)
- [「IPv6 の表示」\(P.42-27\)](#)

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できます。IPv6 では、アドレスレンジが広いこと、プライベートアドレスや、ネットワークエッジの境界ルータでの Network Address Translation (NAT; ネットワークアドレス変換) 処理の必要性が削減されます。

シスコシステムズ製の IPv6 実装については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

この章での IPv6 およびその他の機能についての情報

- 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/ipv6/configuration/guide/12_4t/ipv6_12_4t.html
- [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを探してください。たとえば、スタティックルートについての情報が必要な場合は、[Search] フィールドに「Implementing Static Routes for IPv6」と入力し、スタティックルートについての次のマニュアルを見つけることができます。
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ここでは、スイッチでの IPv6 の実装について説明します。

- 「IPv6 アドレス」(P.42-2)
- 「IPv6 ユニキャストルーティングのサポートされる機能」(P.42-3)
- 「IPv6 ユニキャストルーティングのサポートされない機能」(P.42-9)
- 「制限事項」(P.42-9)

IPv6 アドレス

スイッチは IPv6 ユニキャストアドレスだけをサポートします。サイトローカル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しません。

IPv6 の 128 ビットアドレスは、コロンで区切られた 8 個の 16 ビットの 16 進数フィールドで表されます。n:n:n:n:n:n:n:n という形式です。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、各フィールドの先行ゼロは省略可能です。上記のアドレスの先行ゼロをのぞいた表現を次に示します。

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

2 つのコロン (::) でゼロが連続する 16 進数フィールドを表すこともできますが、この短縮バージョンを使用できるのは各アドレスの中で 1 回だけです。

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

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

「Implementing Addressing and Basic Connectivity」では、次の項が IE 3000 スイッチに該当します。

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

IPv6 ユニキャスト ルーティングのサポートされる機能

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

- 「128 ビット幅ユニキャスト アドレス」 (P.42-3)
- 「IPv6 用の DNS」 (P.42-4)
- 「IPv6 ユニキャストのパス MTU 検出」 (P.42-4)
- 「ICMPv6」 (P.42-4)
- 「ネイバー探索」 (P.42-4)
- 「デフォルト ルータ プリファレンス」 (P.42-5)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.42-5)
- 「IPv6 アプリケーション」 (P.42-5)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.42-5)
- 「IPv6 アドレス割り当てのための DHCP」 (P.42-6)
- 「IPv6 用のスタティック ルート」 (P.42-7)
- 「IPv6 用の RIP」 (P.42-7)
- 「IPv6 用の OSPF」 (P.42-7)
- 「IPv6 用の EIGRP」 (P.42-7)
- 「IPv6 用の HSRP」 (P.42-7)
- 「IPv6 での SNMP と Syslog」 (P.42-8)
- 「IPv6 での HTTP (S)」 (P.42-8)

スイッチは、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のサポートの向上、拡張ヘッダーのハードウェア解析などをサポートします。また、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 パケットをサポートします。

スイッチが IPv6 ルーティング機能を提供する対象としては、ネイティブ イーサネットの Inter-Switch Link (ISL; スイッチ間リンク) またはスタティック ルートの 802.1Q トランク ポート、IPv6 用の Routing Information Protocol (RIP)、Open Shortest Path First (OSPF) バージョン 3 プロトコルなどがあります。スイッチは最大で 16 の等価コスト ルートをサポートし、IPv4 と IPv6 のフレームを同時にラインレートで転送できます。

128 ビット幅ユニキャスト 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ローカル ユニキャスト アドレスをサポートします。サイトローカル ユニキャスト アドレスはサポートしません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能なグローバル ユニキャスト プレフィクスからの IPv6 アドレスです。このアドレス構造により、ルーティング プレフィクスの厳密な集約が可能になり、グローバル ルーティング テーブルのルーティング テーブル エントリの数が制限されます。これらのアドレスは、組織を通して集約され、最終的にはインターネット サービス プロバイダーに集約されるリンクで使用されます。

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 アドレスの割り当てでは、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。プレフィクスが 2000::/3 (001) から E000::/3 (111) までのアドレスは、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。

- リンクローカルプレフィクス FE80::/10 (1111 1110 10) および変更された EUI 形式のインターフェイス ID を使用することで、任意のインターフェイスにリンクローカルユニキャストアドレスを自動的に生成できます。Neighbor Discovery Protocol (NDP; ネイバー探索プロトコル) およびステートレス自動設定プロセスでは、リンク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ローカルアドレスを使用するため、グローバルに一意のアドレスを必要としません。IPv6 ルータは、発信元または宛先がリンクローカルアドレスであるパケットを、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」で IPv6 ユニキャストアドレスに関する項を参照してください。

IPv6 用の DNS

IPv6 は、Domain Name System (DNS; ドメインネームシステム) の名前からアドレスおよびアドレスから名前の検索処理で、DNS レコードタイプをサポートします。DNS AAAA リソースレコードタイプは IPv6 アドレスをサポートし、IPv4 の A アドレスレコードと同等です。スイッチは、IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU 検出

スイッチは、IPv6 ノードに対するシステムの Maximum Transmission Unit (MTU; 最大伝送ユニット) のアドバタイズと、パス MTU 検出をサポートします。パス MTU 検出を使用すると、ホストは特定のデータパスに沿ったすべてのリンクの MTU サイズの違いをダイナミックに検出して、調整できます。IPv6 では、パスに沿ったリンクがパケットサイズに十分な大きさでない場合は、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 検出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中にエラーを通知します。IPv6 では、ICMP パケットはネイバー探索プロトコルおよびパス MTU 検出でも使用されます。

ネイバー探索

スイッチは、ICMPv6 上で動作するプロトコルである NDP を IPv6 に対してサポートします。また、NDP をサポートしない IPv6 ステーションのスタティックネイバーエントリもサポートします。IPv6 ネイバー探索プロセスは、ICMP メッセージと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）のネイバーのリンクレイヤアドレスを特定し、ネイバーの到達可能性を確認して、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。ICMP リダイレクトは、ホストルートまたはマスク長が 64 ビットより長い集約ルートについてはサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためのネクストホップ転送情報を取得する処理の間に、スイッチの CPU の負荷が必要以上に大きくならないことが保証されます。スイッチは、アクティブに解決しようとしているものと同じネイバーがネクストホップとして指定されている追加の IPv6 パケットを廃棄します。この廃棄により、CPU の負荷の増大を防ぎます。

デフォルト ルータ プリファレンス

スイッチは、ルータ アドバタイズメント メッセージの拡張機能である IPv6 Default Router Preference (DRP; デフォルト ルータ プリファレンス) をサポートします。DRP を使用すると、ホストはより適切なルータを選択できます。特に、ホストがマルチホームで、ルータが異なるリンク上にある場合に有効です。スイッチは、RFC 4191 のルート情報オプションはサポートしません。

IPv6 ホストは、オフリンクの宛先へのトラフィックに対するルータを選択するためにデフォルト ルータ リストを保持しています。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、到達可能性が不明または信用できないルータより、到達可能または到達可能の可能性があるルータが指定されます。到達可能ルータまたは到達可能性が高いルータについて、NDP は毎回同じルータを選択することも、リストのルータを順番に使用することもできます。DRP を使用すると、どちらも到達可能である、または到達可能性が高い 2 つのルータの間で一方を他方より優先するように、IPv6 ホストを設定できます。

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

IPv6 のステートレス自動設定および重複アドレス検出

スイッチは、ステートレス自動設定を使用して、ホストとモバイルの IP アドレスの管理など、リンク、サブネット、サイト アドレッシングの変更を管理します。ホストは自立的に独自のリンクローカル アドレスを設定し、起動ノードはルータ送信請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 アドバタイズを要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 アプリケーション

スイッチは以下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、TFTP、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

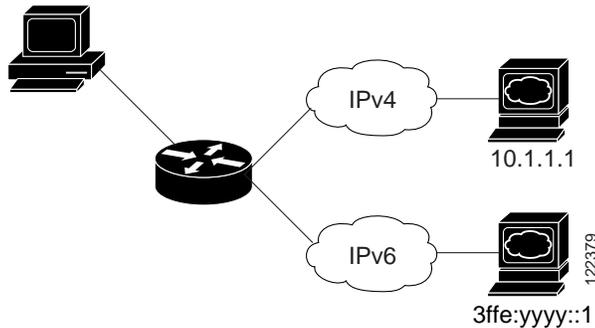
これらのアプリケーションの管理の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

デュアル IPv4/IPv6 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 42-1 は、IP パケットと宛先アドレスに基づいて、IPv4 と IPv6 の両方のトラフィックを同じインターフェイスで転送するルータを示しています。

図 42-1 インターフェイス上でのデュアル IPv4/IPv6 のサポート



IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを 사용합니다。デュアル IPv4/IPv6 SDM テンプレートの詳細については、[第 10 章「SDM テンプレートの設定」](#)を参照してください。

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

- 先にデュアル IPv4/IPv6 テンプレートを選択しないで 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 だけの環境では、スイッチは IPv4 パケットをルーティングし、ハードウェアで IPv4 QoS と ACL を適用します。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 と IPv6 の両方のパケットをルーティングし、ハードウェアで IPv4 QoS を適用します。
- IPv6 QoS はサポートされません。
- 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、各リソースに対する TCAM の容量が少なくなります。

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 で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 アドレス割り当てのための DHCP

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は、ホストが接続されているネットワークに基づく正しいプレフィクスでの重複しないアドレス割り当てを管理します。1 つまたは複数のプレフィクス プールからアドレスを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 アドレスなどの追加オプションを、クライアントに返すことができます。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するためにアドレス プールを割り当てることも、サーバで適切なプールを自動的に検出することもできます。

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

IPv6 用のスタティック 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装置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の場合や、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便利です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」を参照してください。

IPv6 用の RIP

IPv6 用の Routing Information Protocol (RIP) は、ルーティング メトリックとしてホップ カウントを使用する距離ベクトル プロトコルです。IPv6 のアドレスとプレフィクス、および RIP 更新メッセージの宛先アドレスとしての全 RIP ルータ マルチキャスト グループ アドレス FF02::9 をサポートしています。

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

IPv6 用の OSPF

IP サービス イメージを実行するスイッチは、IPv6 の Open Shortest Path First (OSPF) (IP のリンクステート プロトコル) をサポートします。詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 用の EIGRP

IP サービス イメージを実行するスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol (EIGRP) をサポートします。EIGRP は実行しているインターフェイスに設定され、グローバル IPv6 アドレスを必要としません。

実行する前に、EIGRP IPv6 のインスタンスには暗黙的または明示的なルータ ID が必要です。暗黙的なルータ ID はローカル IPv4 アドレスから取得されるので、すべての IPv4 ノードは常に使用可能なルータ ID を持っています。ただし、EIGRP IPv6 は IPv6 ノードだけのネットワークで実行する場合があるため、使用可能な IPv4 ルータ ID がいない可能性があります。

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

IPv6 用の HSRP

IP サービス イメージを実行するスイッチは、IPv6 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、単一のルータの可用性に依存しない冗長なルーティングを IPv6 のトラフィックに提供します。IPv6 ホストは、IPv6 のネイバー探索 ルータ アドバタイズメント メッセージを通して使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か、ホストにより送信請求されます。

HSRP の IPv6 グループは、HSRP グループ番号から取得される仮想 MAC アドレスと、デフォルトでは HSRP の仮想 MAC アドレスから取得される仮想 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になると、HSRP の仮想 IPv6 リンクローカル アドレスに定期的にメッセージが送信されます。このメッセージは、グループがアクティブ状態ではなくなって、最後のメッセージが送信された後で停止します。

IPv6 用の HSRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」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、IPv6 のネットワーク管理には 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用のアドレス データ タイプをサポートします。

IPv6 での SNMP と Syslog は、次の機能を提供します。

- IPv4 と IPv6 の両方のサポート
- SNMP 用の IPv6 トランスポート、および IPv6 ホスト用のトラップをサポートするために SNMP エージェントを変更するための IPv6 トランスポート
- IPv6 アドレッシングをサポートするための SNMP 関連および Syslog 関連の MIB
- トラップ レシーバーとしての IPv6 ホストの設定

IPv6 でのサポートの場合、SNMP は IPv4 と IPv6 を同時にサポートするために既存の IP トランスポート マッピングを変更します。次の SNMP 処理は IPv6 のトランスポート管理をサポートします。

- デフォルト設定で User Datagram Protocol (UDP; ユーザ データグラム プロトコル) SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供する
- IPv6 トランスポートで SNMP 通知を送信する
- IPv6 トランスポート用に SNMP 名前付きアクセス リストをサポートする
- IPv6 トランスポートを使用する SNMP プロキシ転送をサポートする
- IPv6 トランスポートでの SNMP マネージャ機能の動作を確認する

設定手順など、IPv6 での SNMP の詳細については、Cisco.com で『*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 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

IPv6 での HTTP (S)

HTTP クライアントは IPv4 と IPv6 の両方の HTTP サーバに要求を送信し、HTTP 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。コロンで区切られた 16 ビット値を使用した 16 進数形式で、リテラル IPv6 アドレスの URL を指定する必要があります。

受け付けソケット呼び出しは、IPv4 または IPv6 のアドレス ファミリを選択します。受け付けソケットは、IPv4 または IPv6 ソケットです。リスニングソケットは、接続を示す IPv4 と IPv6 の両方の信号を引き続き待ち受けます。IPv6 リスニングソケットは、IPv6 のワイルドカードアドレスにバインドされます。

基になっている TCP/IP 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 TCP/IP スタックとソケットに依存して、ネットワーク層の相互作用を処理します。

HTTP 接続を確立するには、クライアントとサーバホストの間に基本的なネットワーク接続 (ping) が存在している必要があります。

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

IPv6 ユニキャスト ルーティングのサポートされない機能

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 の Virtual Private Network (VPN; 仮想私設網) Routing and Forwarding (VRF; VPN ルーティング/転送) テーブルのサポート
- 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 アドレス宛の IPv6 パケット
- IPv4-to-IPv6 や IPv6-to-IPv4 などのトンネリング プロトコル
- IPv4-to-IPv6 または IPv6-to-IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse Path Forwarding (RPF)
- IPv6 の汎用プレフィクス

制限事項

IPv6 はスイッチのハードウェアで実装されるので、TCAM での IPv6 圧縮アドレスのために制限事項がいくつか発生します。ハードウェアに関するこれらの制限事項により、失われたり制限されたりする機能があります。

制限される機能は次のとおりです。

- ICMPv6 リダイレクト機能は、IPv6 ホスト ルート (特定のホストに到達するために使用されるルート) またはマスクが 64 ビットより大きい IPv6 ルートについてはサポートされません。スイッチは、ホスト ルートまたはマスクが 64 ビットより大きいルートを通して到達可能な特定の宛先に対するより優れ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はできません。
- 等価コスト ルートまたは不等価コスト ルートを使用するロード バランシングは、IPv6 ホスト ルートまたはマスクが 64 ビットより大きい IPv6 ルートについては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 の 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廃棄されて転送されません。

- スイッチは IPv6-to-IPv4 および IPv4-to-IPv6 パケットをハードウェアでルーティングしますが、スイッチは IPv6-to-IPv4 トンネルまたは IPv4-to-IPv6 トンネルのエンドポイントになることはできません。
- ホップバイホップ拡張ヘッダーを含む IPv6 ブリッジド パケットは、ソフトウェアで転送されます。IPv4 では、このようなパケットに対するルーティングはソフトウェアで行われますが、ブリッジングはハードウェアで行われます。
- ソフトウェア コンフィギュレーション ガイドで定義されている通常の SPAN および RSPAN の制限事項に加えて、IPv6 パケットに固有の次の制限事項があります。
 - IPv6 でルーティングされる RSPAN パケットを送信するとき、SPAN 出力パケットの送信元 MAC アドレスが正しくない場合がある。
 - IPv6 でルーティングされる RSPAN パケットを送信するとき、宛先 MAC アドレスが正しくない場合がある (通常のトラフィックには影響なし)。

- スイッチは、ソースルート IPv6 パケットに対してハードウェアで QoS 分類またはポリシーベースルーティングを適用できません。
- スイッチは、マルチキャスト パケットに対して ICMPv6 のパケット サイズ超過メッセージを生成できません。

IPv6 の設定

ここでは、IPv6 フォワーディングの次の設定情報について説明します。

- 「IPv6 のデフォルト設定」(P.42-10)
- 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化」(P.42-11)
- 「デフォルト ルータ プリファレンスの設定」(P.42-13)
- 「IPv4 および IPv6 プロトコル スタックの設定」(P.42-14)
- 「IPv6 アドレス割り当てのための DHCP の設定」(P.42-15)
- 「IPv6 ICMP レート制限の設定」(P.42-19)
- 「IPv6 に対する CEF の設定」(P.42-19)
- 「IPv6 に対するスタティック ルートの設定」(P.42-20)
- 「IPv6 用の RIP の設定」(P.42-21)
- 「IPv6 用の OSPF の設定」(P.42-22)
- 「IPv6 用の EIGRP の設定」(P.42-24)
- 「IPv6 用の HSRP の設定」(P.42-24)

IPv6 のデフォルト設定

表 42-1 に、IPv6 のデフォルト設定を示します。

表 42-1 IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト。
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル。
CEFv6 または dCEFv6	ディセーブル (IPv4 CEF および dCEF はデフォルトでイネーブル)。 (注) IPv6 ルーティングをイネーブルにすると、CEFv6 および dCEF6 は自動的にイネーブルになります。
IPv6 アドレス	設定なし。

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化

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

スイッチで IPv6 を設定する場合は、次の注意事項を考慮してください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- この章で説明されている機能の中には、IP サービス イメージを実行する IE 3000 スイッチでサポートされていないものがあります。「IPv6 ユニキャスト ルーティングのサポートされない機能」(P.42-9) を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドの *ipv6-address* および *ipv6-prefix* 変数には、コロンで区切られた 16 ビット値の 16 進数形式で指定したアドレスを入力する必要があります。 *prefix-length* 変数 (先頭にスラッシュ (/) が付加された値) は、アドレスの上位何ビットがプレフィクス (アドレスのネットワーク部) であるかを示す 10 進値です。

インターフェイスで IPv6 トラフィックを転送するには、そのインターフェイスにグローバル IPv6 アドレスを設定する必要があります。インターフェイスに IPv6 アドレスを設定すると、自動的にリンクローカルアドレスが設定され、そのインターフェイスで IPv6 がアクティブになります。設定されたインターフェイスは、次の必要なマルチキャスト グループをそのリンクに自動的に追加します。

- インターフェイスに割り当てられている各ユニキャスト アドレスに対する送信請求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104 (このアドレスは、ネイバー探索プロセスで使用されます)
- 全ノード リンクローカル マルチキャスト グループ FF02::1
- 全ルータ リンクローカル マルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com で『Cisco IPv6 DHCPv6 Configuration Library』の「Implementing Addressing and Basic Connectivity for IPv6」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 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}	IPv4 と 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 リソースのバランスを取ります。 • routing : スイッチをルーティング テンプレートに設定して、IPv4 および IPv6 のルーティングをサポートします (IPv4 のポリシーベース ルーティングを含む)。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	オペレーティング システムをリロードします。
ステップ 5	configure terminal	スイッチのリロード後にグローバル コンフィギュレーション モードを開始します。
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)、またはレイヤ 3 EtherChannel のいずれでもかまいません。

	コマンド	目的
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)。
ステップ 8	ipv6 address <i>ipv6-prefix/prefix length eui-64</i> または ipv6 address <i>ipv6-address link-local</i> または ipv6 enable	IPv6 アドレスの下位 64 ビットに、Extended Unique Identifier (EUI) を設定したグローバル 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、インターフェイス上で IPv6 の処理がイネーブルになります。 インターフェイスで IPv6 をイネーブルにすると自動的に設定されるリンクローカルアドレスの代わりに使用するリンクローカルアドレスをインターフェイスに指定します。このコマンドにより、インターフェイス上で IPv6 の処理がイネーブルになります。 インターフェイスで IPv6 リンクローカルアドレスを自動的に設定し、IPv6 処理用にインターフェイスをイネーブルにします。リンクローカルアドレスは、同じリンク上のノードと通信するためにだけ使用できます。
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	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 <i>interface-id</i>	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

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、引数を指定せずに **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の IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づいて、リンクローカルアドレスとグローバルアドレスの両方で IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID は、両方のアドレスの下位 64 ビットで使用されています。**show ipv6 interface EXEC** コマンドの出力では、インターフェイス ID (20B:46FF:FE2F:D940) がインターフェイスのリンクローカル プレフィクス FE80::/64 にどのように追加されているかが示されます。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/1
GigabitEthernet1/1 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るデフォルト ルータ プリファレンス (DRP) の内容とともに送信されます。DRP が設定されていない場合、送信される RA のプリファレンス値は **medium** になります。

DRP は、リンク上の 2 つのルータが同等であっても、等価コスト ルーティングではなく、ポリシーではホストが一方のルータを優先するように示されている場合に使用すると便利です。

インターフェイス上でルータの 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 インターフェイスでルータに 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) 設定をコンフィギュレーション ファイルに保存します。

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、インターフェイスでルータにハイの DRP を設定する例を示します。

```

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end

```

IPv6 に DRP を設定する方法の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」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 と 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は、**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。新しいテンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 と IPv6 の両方をサポートするようにレイヤ 3 インターフェイスを設定し、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	ip routing	スイッチ上でルーティングをイネーブルにします。
ステップ 3	ipv6 unicast-routing	スイッチでの 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 cui-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 プレフィッ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。 インターフェイスで IPv6 をイネーブルにすると自動的に設定されるリンクローカルアドレスの代わりに使用するリンクローカルアドレスをインターフェイスに指定します。 インターフェイスで IPv6 リンクローカルアドレスを自動的に設定し、IPv6 処理用にインターフェイスをイネーブルにします。リンクローカルアドレスは、同じリンク上のノードと通信するためにだけ使用できます。
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) 設定をコンフィギュレーション ファイルに保存します。

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 cui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、引数を指定せずに **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の 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 gigabitethernet1/1
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
```

IPv6 アドレス割り当てのための DHCP の設定

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

- 「デフォルトの DHCPv6 アドレス割り当ての設定」 (P.42-15)
- 「DHCPv6 アドレス割り当て設定時の注意事項」 (P.42-15)
- 「DHCPv6 サーバ機能のイネーブル化」 (P.42-16)
- 「DHCPv6 クライアント機能のイネーブル化」 (P.42-18)

デフォルトの DHCPv6 アドレス割り当ての設定

デフォルトでは、DHCPv6 機能はスイッチに設定されません。

DHCPv6 アドレス割り当て設定時の注意事項

DHCPv6 アドレス割り当ての設定時は、次の注意事項を考慮してください。

- 手順では、次のレイヤ 3 インターフェイスのいずれかを指定する必要があります。
 - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイスで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。
 - レイヤ 3 モードでの 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。
- DHCPv6 を設定するには、IPv4 と IPv6 をサポートする Switch Database Management (SDM) テンプレートを選択する必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、1 つのインターフェイスでは同時に指定できません。

DHCPv6 サーバ機能のイネーブル化

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

	コマンド	目的
ステップ 1	<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。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。
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 ビット値をコロンで区切った 16 進数に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な状態を維持する時間 (秒単位) を指定します。指定できる範囲は 5 ~ 4294967295 秒です。時間間隔を指定しない場合は、 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 IPv6 プレフィックスを指定します。 着信インターフェイスのアドレスまたはパケット内のリンクアドレスが指定の IPv6 プレフィックスと一致した場合、サーバは構成情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数にする必要があります。
ステップ 5	<code>vendor-specific <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 ID 番号を入力します。この番号はベンダーの IANA 民間企業番号です。指定できる範囲は 1 ~ 4294967295 です。
ステップ 6	<code>suboption number {address <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。IPv6 アドレス、ASCII テキスト、または 16 進数の文字列をサブオプションパラメータによって定義されたものとして入力します。
ステップ 7	<code>exit</code>	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface <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] [<i>rapid-commit</i>] [<i>preference value</i>] [<i>allow-hint</i>]	<p>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。</p> <ul style="list-style-type: none"> • poolname : (任意) IPv6 DHCP プール用にユーザ定義された名前。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。 • automatic : (任意) クライアントにアドレスを割り当てる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 つのメッセージ交換方式を可能にします。 • preference value : (任意) サーバが送信するアドバタイズメッセージの preference オプションで伝送される preference 値。指定できる範囲は 0 ~ 255 です。デフォルトの preference 値は 0 です。 • allow-hint : (任意) サーバが送信請求メッセージでクライアントの提案を考慮するかどうか指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11 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	<p>DHCPv6 プールの設定を確認します。</p> <p>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。</p>
ステップ 13 copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

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。インターフェイスでの DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、*engineering with an IPv6 address prefix* というプールを設定する方法を示します。

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

次に、3 つのリンクアドレスと IPv6 のアドレス プレフィクスで *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
```

次の例では、ベンダー固有のオプションのある *350* というプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
```

```
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで 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]	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 rapid-commit : (任意) アドレス割り当ての 2 つのメッセージ交換方式を可能にします。
ステップ 4	ipv6 dhcp client request [vendor-specific]	(任意) インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	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 gigabitethernet1/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

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

IPv6 ICMP レート制限の設定

デフォルトでは、ICMP レート制限はイネーブルになっています。エラー メッセージ間のデフォルトの間隔は 100 ミリ秒、バケット サイズ（バケットに格納されるトークンの最大数）は 10 です。

ICMP の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"> <code>interval</code> : バケットにトークンが追加される間隔（ミリ秒単位）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 <code>bucketsize</code> : (任意) バケットに格納されるバケットの最大数。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) 設定をコンフィギュレーション ファイルに保存します。

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 のエラー メッセージの間隔を 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 に対する CEF の設定

Cisco Express Forwarding (CEF) 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 テクノロジーです。IPv6 CEF はデフォルトではディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、まず `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 パケット転送をグローバルに設定する必要があります。 `ipv6 address` インターフェイス コンフィギュレーション コマンドを使用して、IPv6 アドレスと IPv6 処理をインターフェイスに設定する必要があります。

IPv6 CEF をディセーブルにするには、`no ipv6 cef` グローバル コンフィギュレーション コマンドを使用します。ディセーブルにした IPv6 CEF または dCEF を再びイネーブルにするには、`ipv6 cef` グローバル コンフィギュレーション コマンドを使用します。 `show ipv6 cef` 特権 EXEC コマンドを入力すると、IPv6 ステータスを確認できます。

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

IPv6 に対するスタティック ルートの設定

スタティック IPv6 ルートを設定するには、**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 インターフェイスに IPv6 アドレスを設定して 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 ルートの宛先である IPv6 ネットワーク。スタティック ホスト ルートの設定では、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。アドレスの上位何ビットがプレフィックス (アドレスのネットワーク部) であるかを示す 10 進値です。スラッシュ記号を 10 進値の前に付ける必要があります。 <i>ipv6-address</i> : 指定されたネットワークに到達するため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されている必要はありません。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、再帰処理が行われます。このアドレスは、コロンで区切られた 16 ビット値を使用した 16 進数形式で指定する必要があります。 <i>interface-id</i> : ポイントツーポイント インターフェイスおよびブロードキャスト インターフェイスから直接スタティック 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はありません。ブロードキャスト インターフェイスでは、ネクストホップの IPv6 アドレスを常に指定するか、指定されたプレフィックスをリンクに割り当ててリンクローカルアドレスをネクストホップとして指定する必要があります。必要に応じて、パケットの送信先であるネクストホップの IPv6 アドレスを指定できます。 <p>(注) ネクストホップとしてリンクローカル アドレスを使用する場合は (リンクローカル ネクストホップは、隣接ルータでもある必要があります)、<i>interface-id</i> を指定する必要があります。</p> <ul style="list-style-type: none"> <i>administrative distance</i> : (任意) 管理ディスタンスです。指定できる範囲は 1 ~ 254 です。デフォルト値は 1 で、接続されたルートを除く他のすべてのルート タイプより優先されるスタティック ルートを指定します。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 プロトコルの管理ディスタンスよりも大きい管理ディスタンスを使用します。
ステップ 3	end	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 4 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使用するスタティック 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することはできませんが、IPv6 プレフィクスとは同時に指定することもできます。 • detail : (任意) 次の追加情報を表示します。 <ul style="list-style-type: none"> – 有効な再帰ルートの場合、出力パス セット、および解決の最大深さ。 – 無効なルートの場合、そのルートが無効である理由。
ステップ 5 copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

設定されているスタティック 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 であるフローティング 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 で『Cisco IOS IPv6 Configuration Library』の「Implementing Static Routes for IPv6」を参照してください。

IPv6 用の RIP の設定

IPv6 RIP を実行するようにスイッチを設定するには、**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 RIP をイネーブルにするすべてのレイヤ 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 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 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 rip name	IPv6 RIP ルーティング プロセスを設定し、プロセスのルータ 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 maximum-paths number-paths	(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 です。デフォルト値は 4 ルートです。
ステップ 4 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 5 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 6 ipv6 rip name enable	インターフェイスで指定した IPv6 RIP ルーティング プロセスを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、指定したインターフェイスから送信します。</p> <p>(注) IPv6 デフォルト ルート (::/0) を任意のインターフェイスから送信したあとにルーティング ループが発生しないようにするために、ルーティング プロセスはインターフェイスで受信するデフォルト ルートをすべて無視します。</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る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 ルートに加えて、現在のインターフェイスで送信される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 テーブルの内容を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

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。インターフェイスの RIP ルーティング プロセスをディセーブルにするには、**no ipv6 rip name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、最大 8 つの等価コスト ルートで RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイスでそれを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 用の RIP ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing RIP for IPv6」を参照してください。

IPv6 用の OSPF の設定

IPv6 用の OSPF は、各ネットワーク用にカスタマイズできます。ただし、IPv6 での OSPF に対するデフォルトは、ほとんどのユーザと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。

- スイッチは、IP サービス イメージを実行している必要があります。
- IPv6 コマンドのデフォルトを変更する場合は注意が必要です。デフォルトを変更すると、IPv6 ネットワーク用の OSPF に悪影響を及ぼす可能性があります。

- インターフェイスで IPv6 OSPF をイネーブルにするには、**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	プロセスの 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 ルーティング プロセスの OSPF をイネーブルにするときに管理用に割り当てた番号です。プロセス ID はローカルに割り当てられており、1 ~ 65535 の範囲の正の整数です。
ステップ 3	area area-id range {ipv6-prefix/prefix length} [advertise not-advertise] [cost cost]	<p>(任意) エリアの境界でルートを統合および集約します。</p> <ul style="list-style-type: none"> • area-id : ルートを集約するエリアの ID。10 進値または IPv6 プレフィクスとして指定できます。 • ipv6-prefix/prefix length : 宛先 IPv6 ネットワーク、およびアドレスの上位何ビットがプレフィクス (アドレスのネットワーク部) であるかを示す 10 進値です。スラッシュ記号 (/) を 10 進値の前に付ける必要があります。 • advertise : (任意) Type 3 サマリー Link-State Advertisement (LSA; サマリー リンクステート アドバタイズ) をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • not-advertise : (任意) アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠されたままになります。 • 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。宛先までの最短のパスを判別する場合に、OSPF SPF 計算で使用されます。指定できる値の範囲は、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 です。デフォルト値は 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]	IPv6 用の OSPF をインターフェイスで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。

	コマンド	目的
ステップ 9	<code>show ipv6 ospf [process-id] [area-id] interface [interface-id]</code> または <code>show ipv6 ospf [process-id] [area-id]</code>	OSPF インターフェイスに関する情報を表示します。 OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

OSPF ルーティング プロセスをディセーブルにするには、**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。インターフェイスの OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf process-id area area-id** インターフェイス コンフィギュレーション コマンドを使用します。

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

IPv6 用の EIGRP の設定

デフォルトでは、IPv6 用の EIGRP はディセーブルになっています。インターフェイスで IPv6 用の EIGRP を設定できます。EIGRP 用にルータとインターフェイスを設定してから、**no shutdown** 特権 EXEC コマンドを入力して EIGRP を開始します。



(注)

IPv6 用の EIGRP がシャットダウン モードではない場合、EIGRP の **router-mode** コマンドを入力してルータとインターフェイスを設定する前に、EIGRP が実行を開始する場合があります。

スイッチは、IP サービス イメージを実行している必要があります。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定されているルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 と同様に、EIGRPv6 を使用して EIGRP IPv4 インターフェイスを指定し、そのサブセットを受動インターフェイスとして選択できます。すべてのインターフェイスをパッシブにするには、**passive-interface default** コマンドを使用します。すべてのインターフェイスをアクティブにするには、選択したインターフェイスで **no passive-interface** コマンドを使用します。受動インターフェイスでは EIGRP IPv6 を設定する必要はありません。

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

IPv6 用の HSRP の設定

Hot Standby Router Protocol (HSRP) は、単一のルータのアベイラビリティに依存しない冗長なルーティングを IPv6 のトラフィックに提供します。

IPv6 用の HSRP をスイッチでイネーブルにすると、IPv6 ホストは IPv6 のネイバー探索ルータ アドバタイズメント メッセージを通して使用可能な IPv6 ルータを学習します。HSRP IPv6 グループは、HSRP グループ番号から取得される仮想 MAC アドレスを持っています。また、デフォルトで、HSRP の仮想 MAC アドレスから取得される仮想 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になると、HSRP の仮想 IPv6 リンクローカル アドレスに定期的にメッセージが送信されます。

スイッチは、IP サービス イメージを実行している必要があります。

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

HSRPv1 および HSRPv2 で IPv6 用の HSRP を設定する場合の注意事項については、「[HSRP 設定時の注意事項](#)」(P.45-5) および「[HSRP のトラブルシューティング](#)」(P.45-12) を参照してください。

IPv6 用の HSRP および HSRPv2 の詳細については、[第 45 章「HSRP の設定」](#) を参照してください。



(注) IPv6 グループ用の HSRP を設定するには、**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 グループ用の HSRP を設定する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。

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	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、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	standby version {1 2}	2 を入力して HSRP のバージョンを変更します。デフォルトは 1 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show standby	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) 設定をコンフィギュレーションファイルに保存します。

IPv6 用の HSRP グループのイネーブル化

レイヤ 3 インターフェイスで IPv6 用の HSRP を作成または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、IPv6 用の 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。

	コマンド	目的
ステップ 3	<code>standby [group-number] ipv6 {link-local-address autoconfig}</code>	IPv6 グループ用の HSRP 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です。指定できる範囲は 0 ~ 4095 です。デフォルト値は 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、リンクローカル プレフィクスと変更された EUI-64 形式のインターフェイス ID からのリンクローカル アドレスの自動生成をイネーブルにします。EUI-64 形式のインターフェイス ID は、関連する HSRP 仮想 MAC アドレスから作成されます。
ステップ 4	<code>standby [group-number] preempt [delay {minimum seconds reload seconds sync seconds}]</code>	ルータを preempt に設定します。これは、ローカル ルータのプライオリティがアクティブ ルータより高い場合は、そのローカル ルータがアクティブ ルータとして制御を行うことを意味します。 <ul style="list-style-type: none"> (任意) <i>group-number</i> : 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 (1 時間) です。デフォルト値は 0 です (引き継ぎ前の遅延なし)。 (任意) reload : リロード後のプリエンプション遅延を設定します (秒単位)。遅延は、ルータがリロードしたあとの最初の interface-up イベントに対してだけ適用されます。 (任意) sync : IP 冗長クライアントに対する最大同期期間を設定します (秒単位)。 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。
ステップ 5	<code>standby [group-number] priority priority</code>	アクティブ ルータを選択するとき使用される 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。値が大きいほど、高いプライオリティを表します。 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。
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) 設定をコンフィギュレーション ファイルに保存します。

IPv6 用の 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 用の HSRP をアクティブにする例を示します。ホットスタンバイ グループが使用する IP アドレスは、IPv6 用の HSRP を使用して学習されます。



(注)

この手順は、IPv6 用の HSRP をイネーブルにするために必要な最低限の数のステップです。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

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

IPv6 の表示

次の各コマンドの構文と使用方法の詳細については、Cisco IOS のコマンドリファレンスを参照してください。

表 42-2 に、スイッチで IPv6 をモニタするための特権 EXEC コマンドを示します。

表 42-2 IPv6 をモニタするためのコマンド

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 cef	IPv6 用の Cisco Express Forwarding を表示します。
show ipv6 interface <i>interface-id</i>	IPv6 インターフェイスの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 キャッシュのエントリを表示します。
show ipv6 ospf	IPv6 OSPF の情報を表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 protocols	スイッチでの IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコルのステータスを表示します。
show ipv6 route	IPv6 ルート テーブルのエントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
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 42-3 に、EIGRP IPv6 の情報を表示するための特権 EXEC コマンドを示します。

表 42-3 EIGRP IPv6 の情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [<i>as-number</i>] <i>interface</i>	EIGRP IPv6 用に設定されているインターフェイスに関する情報を表示します。
show ipv6 eigrp [<i>as-number</i>] <i>neighbor</i>	EIGRP IPv6 によって検出されたネイバーを表示します。
show ipv6 eigrp [<i>as-number</i>] <i>traffic</i>	送受信された EIGRP IPv6 パケットの数を表示します。
show ipv6 eigrp topology [<i>as-number</i> <i>ipv6-address</i>] [<i>active</i> <i>all-links</i> <i>detail-links</i> <i>pending</i> <i>summary</i> <i>zero-successors</i>]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 42-4 に、IPv4 および IPv6 のアドレス 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 42-4 IPv4 および IPv6 のアドレス タイプを表示するためのコマンド

コマンド	目的
<code>show ip http server history</code>	最近の HTTP サーバへの接続を 20 個表示します。アクセスされた IP アドレスと、接続終了時刻も表示されます。
<code>show ip http server connection</code>	HTTP サーバへの現在の接続を表示します。アクセスされているローカルおよびリモートの IP アドレスも表示されます。
<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要求のリスト（最近の 20 個）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

```

<テキスト出力は省略>

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
    FastEthernet1/4
    FastEthernet1/6
    FastEthernet1/7
  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
```