IPv6 ユニキャスト ルーティングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

IPv6 ユニキャスト ルーティングの設定について

この章では、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。

IPv6 の概要

IPv4 ユーザーは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

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

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

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。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] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

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のみです。サイトローカルユニキャスト アドレスおよびマルチキャスト 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 回のみです。

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 で『*Cisco IOS IPv6 Configuration Library*』の http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3e/ip6b-xe-3e-book.html を参照してください。

「Implementing Addressing and Basic Connectivity」の章では、次の項の内容が Catalyst 2960、2960-S、2960-C、2960-X、2960-CX、3560-CX スイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：マルチキャスト
- Ipv6 アドレス 出力表示
- 簡易 IPv6 パケット ヘッダー

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

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されていません。

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

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

- リンク ローカル 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 ローカル プレフィックス FE80::/10（1111 1110 10）およびインターフェイスID を使用します。ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクローカル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、リンクローカルの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 で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある 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 の DNS

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。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 ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス 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 パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合せて調整できます。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。

ICMPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索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。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部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 ネイバー エントリをサポートします。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層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。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 リダイレクトが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にネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

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 メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、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。NDP は、到達可能または到達できる可能性の高いルータとして、常に同じルータを選択するか、またはルータ リストを循環して選択できます。DRP を使用することにより、両方ともが到達可能または到達できる可能性の高い 2 台のルータの一方を他方に対して優先させるよう IPv6 ホストを設定することができます。

DRP for IPv6 の設定については、「*DRP* の設定」を参照してください。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』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ているため、ホストやモバイル IP アドレスの管理のような、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。ホストは独自のリンクローカルアドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*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、および Telnet
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバー アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバーは 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。このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよびDNS ネーム サーバー アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバーが自動的に適切なプールを検出できます。

DHCP for IPv6 の設定については、「*DHCP for IPv6* アドレス割り当ての設定」のセクションを参照してください。

DHCPv6 クライアント、サーバー、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*』を参照してください。

IPv6 のスタティック ルート

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

IPv6 のスタティック ルーティングの設定（CLI）

IPv6 用のスタティックルートの設定については、「*IPv6* 用のスタティックルーティングの設定」を参照してください。

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」の章を参照してください。

RIP for IPv6

IPv6 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ディスタンスベクトル プロトコルです。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使用する機能などがあります。

IPv6 の RIP の設定については、「*IPv6 の RIP の設定*」を参照してください。

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

OSPF for IPv6

フィーチャ セットを実行しているスイッチは、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*』を参照してください。

OSPFv3 グレースフル リスタート

OSPFv3 機能により、OSPFv3 ルーティング プロトコル情報が復元されている間も、既知のルート上でノンストップのデータの転送が可能になります。スイッチでは、グレースフル リスタートがリスタート モード（グレースフル リスタート対応スイッチの場合）とヘルパー モード（グレースフル リスタート認識スイッチの場合）のいずれかで使用されます。

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 ステートフル スイッチオーバー（SSO）モードである必要があります（デュアル ルート プロセッサ）。グレースフル リスタートに対応したスイッチでは、次の障害が発生した際にグレースフル リスタートが使用されます。

- スタンバイ ルート プロセッサへの切り替えが起こるルート プロセッサ障害
- 計画されたスタンバイ ルート プロセッサへのルート プロセッサの切り替え

グレースフル リスタート機能では、隣接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『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSFP for IPv6」の章を参照してください。

高速コンバージェンス：LSA および SPF スロットリング

OSPFv3 リンク ステート アドバタイズメント（LSA）および Shortest Path First（SPF）スロットリング機能は、ネットワークが不安定なときに、OSPFv3 でのリンク ステート アドバタイズメントの更新の速度を低下させる動的な方法ダイナミック方式を提供します。またこの機能を使用すると、LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮が可能になります。

OSPFv3 では以前はレート制限 SPF 計算および LSA 生成にスタティック タイマーを使用しました。これらのタイマーを設定することもできますが、値は秒単位で指定するため、OSPFv3 コンバージェンスに制限が課せられます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限方式を提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

IPsec を使用した認証サポート

OSPF for IPv6（OSPFv3）パケットが変更されずにスイッチに再送信されるようにするには、OSPFv3 パケットを認証する必要があります。OSPFv3 は、IPsec セキュア ソケット API を使用

して OSPFv3 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。OSPFv3 で使用するために必要な IPsec API は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

IPv6 の HSRP の設定

HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによっ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 IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカルアドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

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

EIGRP IPv6

IP サービス フィーチャ セットを実行中のスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートします。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。

（注） IP ベース フィーチャ セットを実行中のスイッチでは、IPv6 EIGRP スタブ ルーティングを含め、IPv6 EIGRP 機能はすべてサポートされません。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼働するため、使用可能な IPv4 ルータ ID がない場合があります。

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

SNMP and Syslog Over IPv6

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。Syslog over IPv6 は、こ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ます。

Simple Network Management Protocol (SNMP) と syslog over IPv6 は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

Over IPv6 をサポートするため、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 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザー データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス 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 マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、SNMP over IPv6 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。

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

HTTP(S) Over IPv6

HTTP クライアントは要求を IPv4 HTTP サーバーと IPv6 HTTP サーバーの両方に送信し、これらのサーバーは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 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 には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続を確立するには、基本ネットワーク接続（**ping**）がクライアントとサーバーホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」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 機能をサポートしません。

- サイトローカルアドレス宛ての 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 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。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。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。これらはソフトウェアで転送されます。
- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

IPv6 の設定

IPv6 のデフォルト設定

表 *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	アドバンスデスクトップ。デフォルトは拡張テンプレート デフォルト
IPv6 アドレス	未設定

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化

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

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。

- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、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 *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、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。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクローカルアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。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要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る）
- 全ノード向けリンクローカルマルチキャストグループ FF02::1
- 全ルータ向け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 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は、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例**： `スイッチ# 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 2	**interface** *interface-id* **例**： `スイッチ(config)# interface gigabitethernet 1/0/1`	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、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 3	**no switchport** **例**： `スイッチ(config-if)# 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）。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを使用します。
	• **ipv6 address** *ipv6-prefix/prefix length* **eui-64**
	• **ipv6 address** *ipv6-address/prefix length*
	• **ipv6 address** *ipv6-address* **link-local**
	• **ipv6 enable**
	例：
	`スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64`
	`スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1::/64`
	`スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1:: link-local`
	`スイッチ(config-if)# ipv6 enable`
		• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィッ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 処理が有効になります。
		• インターフェイスの IPv6 アドレスを手動で設定します。
		• インターフェイスで IPv6 が有効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、インターフェイス上の特定のリンク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 処理が有効になります。
		• インターフェイスに IPv6 リンクローカルアドレスを自動設定し、インターフェイスでの IPv6 処理を有効にします。リンクローカル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だけです。

ステップ 5	**exit** 例： `スイッチ(config-if)# 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	**ip routing** 例： `スイッチ(config)# 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 7	**ipv6 unicast-routing** 例： `スイッチ(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データ パケットの転送を有効にします。
ステップ 8	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	スイッチ(config)# **end**	
ステップ 9	**show ipv6 interface** *interface-id* 例： スイッチ# **show ipv6 interface gigabitethernet 1/0/1**	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： スイッチ# **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 でのファースト ホップ セキュリティの設定

IPv6 でのファースト ホップ セキュリティの前提条件

- 必要な、IPv6 が有効になっている SDM テンプレートが設定されていること。
- **mls qos** コマンドを使用して CoPP ポリシーを設定する前に、スイッチで QoS を有効にする必要があります。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピング ポリシーがアクセス スイッチに設定されると、ルータまたは DHCP サーバー/リレーに対応するアップリンク ポートが信頼できるポートとして設定されていても、IPv6（DHCPv6）サーバー パケットに対する外部 IPv6 ルータ アドバタイズメント(RA)または Dynamic Host Configuration Protocol はブロックされます。IPv6 RA または DHCPv6 サーバー メッセージを許可するには、次の手順を実行します。
  - IPv6 RA ガード ポリシー（RA の場合）または IPv6 DHCP ガード ポリシー（DHCP サーバー メッセージの場合）をアップリンク ポートに適用します。
  - 低いセキュリティ レベルでスヌーピング ポリシーを設定します（たとえば、glean や inspect など）。しかし、ファースト ホップ セキュリティ機能の利点が有効でないた

め、このようなスヌーピング ポリシーでは、低いセキュリティ レベルを設定することはお勧めしません。

- CSCvk32439 で報告された制限により、IPv6 SISF ベースのデバイス トラッキング ポリシーを使用した CoPP ポリシーには、次の制限が適用されます。
  - スイッチで IPv6 SISF ポリシーが設定されている場合、IPv6 NDP トラフィックを制限するには CoPP ポリシーが必要です。
  - NDP CoPP ポリシーが設定された後、制限されたトラフィックが CPU にヒットします。接続されているエンドポイントの合計に対応するには、NDP CoPP ポリシーの数を、スタック内の各スイッチに接続するユーザーの数よりわずかに多くする必要があります。スイッチに接続されているエンドポイントの数よりも少ない NDP CoPP ポリシーを設定すると、エンドポイントへの IP 割り当ては遅延しますが、完全に無視されるわけではありません。

（注） たとえば、5 つのスイッチのスタックに約 300 のユーザーがいる場合、NDP CoPP ポリシーは 300 を超える必要があります。

  - DHCPv6（サーバーからクライアントおよびクライアントからサーバー）CoPP ポリシーは、Lightweight DHCPv6 リレーエージェント（LDRA）がスイッチの IPv6 SISF ベースのデバイス トラッキング ポリシーで設定されている場合にのみ必要です。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシー データベースに保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能を有効にできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索（ND）プロトコル スヌーピングなどの情報ソースから作成されます。このデータベースまたはバインディング テーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND 検査など）によって使用されます。
- IPv6 ネイバー探索検査：IPv6 ND 検査は、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージは破棄されます。ND メッセージは、

そのIPv6からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。

この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータ アドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ プラットフォームに到着した不要または不正な RA ガード メッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ2デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。レイヤ2デバイスは、RAフレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA は破棄されます。

- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバーおよびリレー エージェントからの返信およびアドバタイズメント メッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバーまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバー メッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

  次の制約事項が適用されます。

  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

  - IPv6 ソース ガードがスイッチ ポートで有効になっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングを有効にする必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。

  - IPv6 ソース ガード ポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。

- インターフェイスで IPv4 および IPv6 のソース ガードを一緒に設定する場合は、**ip verify source** の代わりに **ip verify source mac-check** の使用を推奨します。2 つの異なるフィルタリング ルール（IPv4（IP フィルタ）用と IPv6（IP-MAC フィルタ）用）が設定されているため、特定のポートの IPv4 接続が切断される可能性があります。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

  IPv6 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

  IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

- IPv6 ネイバー検索マルチキャスト抑制：IPv6 ネイバー検索マルチキャスト抑制機能は、IPv6 のスヌーピング機能で、スイッチまたはワイヤレス コントローラで実行し、適切なリンク動作に必要な制御トラフィック量を削減するために使用されます。

- DHCPv6 リレー：Lightweight DHCPv6 リレー エージェント：Lightweight DHCPv6 リレー エージェント機能を使用するとリンクレイヤブリッジング（非ルーティング）機能を実行するアクセス ノードによってリレーエージェント情報が挿入されます。Lightweight DHCPv6 リレー エージェント（LDRA）機能は、DSL アクセス マルチプレクサ（DSLAM）や IPv6 制御やルーティング機能をサポートしないイーサネット スイッチなどの既存のアクセス ノードに実装できます。LDRA を使用して、DHCP バージョン 6（DHCPv6）メッセージ交換にリレーエージェント オプションを挿入して、主にクライアント側のインターフェイスを特定します。LDRA 機能は、インターフェイスと VLAN でイネーブルにできます。

（注） LDRA デバイスがクライアントに直接接続されている場合は、サーバー側で特定のサブネットまたはリンク情報を取得するために、インターフェイスにプール設定が必要です。この場合、LDRA デバイスが異なるサブネットまたはリンクに存在する場合、サーバーは正しいサブネットを取得できない場合があります。インターフェイスでプール名を設定して、クライアントに適切なサブネットまたはリンクを選択できるようになりました。

DHCPv6 リレーの詳細については、『IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.1SG』の「DHCPv6 Relay—Lightweight DHCPv6 Relay Agent」の項を参照してください。

IPv6 スヌーピング ポリシーの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **IPv6 snooping policy** *policy -name*
4. ［**data-glean** ｜**default** ｜ **device-role** ［**node**｜**switch**］ ｜**limit**｛**address-count***value*｝ ｜ **no** ｜ **protocol** ［**all** ｜ **nodhcp**｜ **ndp**］ ｜**security-level** ［**glean**｜ **guard**｜ **inspect**］｜ **tracking** ［**disable** ｜ **enable**］｜ **trusted-port** ｝
5. **exit**
6. **show ipv6 snooping policy***policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**IPv6 snooping policy** *policy -name*	グローバル コンフィギュレーション モードでスヌーピング ポリシーを作成します。

	コマンドまたはアクション	目的
ステップ 4	[**data-glean** | **default** | **device-role** [**node** | **switch**] | **limit** {**address-count***value*} | **no** | **protocol** [**all** | **nodhcp** | **ndp**] | **security-level** [**glean** | **guard** | **inspect**] | **tracking** [**disable** | **enable**] | **trusted-port** }	データ アドレス グリーニングをイネーブルにし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**data-glean**：データ アドレス グリーニングをイネーブルにします。このオプションは、デフォルトで無効です。 • （任意）**default**：すべてのデフォルト オプションを設定します。 • （任意）**device-role** [**node** | **switch**]：ポートに接続されたデバイスのロールを認定します。 • （任意）**limit** {**address-count** *value*}：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。 • （任意）**protocol** [**all** | **dhcp** | **ndp**]：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは**all**です。デフォルトを変更するには、**no protocol** コマンドを使用します。 • （任意）**security-level** [**glean** | **guard** | **inspect**]：この機能によって適用されるセキュリティのレベルを指定します。 • **glean**：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。 • **guard**：アドレスを収集し、メッセージを検査します。さらに、RAおよびDHCPサーバ メッセージを拒否します。これがデフォルトのオプションです。 • **inspect**：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • （任意）**tracking** [**disable** | **enable**]：デフォルトのトラッキング動作を上書きし、トラッキング オプションを指定します。

	コマンドまたはアクション	目的
		• （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。また、テーブル内にエントリを作成しているときに衝突が発生した場合も、信頼できるポートが優先されます。
ステップ 5	**exit**	スヌーピング ポリシー コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 snooping policy***policy-name*	スヌーピング ポリシー設定を表示します。

IPv6 スヌーピング ポリシーのインターフェイスまたは VLAN へのアタッチ方法

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface** *type number*
   - **switchport**
   - **ipv6 snooping** [**attach-policy** *policy_name*]

     または

   - **vlan configuration** *vlan list*
   - **ipv6 snooping attach-policy** *policy-name*
4. **show ipv6 snooping policy** *policy-name*
5. **show ipv6 neighbors binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	次のいずれかの作業を実行します。 • **interface** *type number* • **switchport** • **ipv6 snooping** [**attach-policy** *policy_name*] または • **vlan configuration** *vlan list* • **ipv6 snooping attach-policy** *policy-name*	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 （注） typeは物理インターフェイスでも、イーサチャネルでもかまいません。 インターフェイスをレイヤ 2 ポートとして設定します。 スヌーピング ポリシー（データ グリーニングがイネーブル）をインターフェイスに適用します。ポートと、そのポートに適用されるポリシーを指定します。 （注） スヌーピング ポリシーで **data-glean** をイネーブルにした場合は、そのポリシーをVLANではなく、インターフェイスに適用する必要があります。
ステップ 4	**show ipv6 snooping policy** *policy-name*	スヌーピング ポリシー設定を表示します。
ステップ 5	**show ipv6 neighbors binding**	スヌーピング ポリシーによって入力されたバインディング テーブル エントリを表示します。

デバイスでの IPv6 ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6ネイバー探索マルチキャスト抑制ポリシーをデバイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy** *policy-name*
4. **mode dad-proxy**
5. **mode full-proxy**
6. **mode mc-proxy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**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 3	**ipv6 nd suppress policy** *policy-name*	ネイバー探索抑制ポリシー名を定義して、ネイバー探索抑制ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**mode dad-proxy**	IPv6 DADプロキシ モードでネイバー探索抑制をイネーブルにします。
ステップ 5	**mode full-proxy**	プロキシマルチキャストおよびユニキャストのネイバー送信要求メッセージに対するネイバー探索抑制をイネーブルにします。
ステップ 6	**mode mc-proxy**	プロキシマルチキャスト ネイバー送信要求メッセージに対するネイバー探索抑制をイネーブルにします。

インターフェイスでの *IPv6* ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6 ネイバー探索マルチキャスト抑制ポリシーをインターフェイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface** *type number*
   - **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

     または

   - **vlan configuration** *vlan-id*
   - **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 3	次のいずれかの作業を実行します。 • **interface** *type number* • **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] または • **vlan configuration** *vlan-id* • **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。 IPv6 ネイバー探索マルチキャスト ポリシーをインターフェイスまたは VLAN にアタッチします。
ステップ 4	**exit**	インターフェイス コンフィギュレーション モードを終了します。

レイヤ *2 EtherChannel* インターフェイスへの *IPv6* ネイバー探索マルチキャスト抑制ポリシーのアタッチ方法

IPv6 ネイバー探索マルチキャスト抑制ポリシーを EtherChannel インターフェイスにアタッチするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの作業を実行します。
   - **interface port-channel** *port-channel-number*
   - **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

     または

   - **vlan configuration** *vlan-id*
   - **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 3	次のいずれかの作業を実行します。 • **interface port-channel** *port-channel-number* • **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] または • **vlan configuration** *vlan-id* • **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** { **add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。 IPv6 ネイバー探索マルチキャスト ポリシーをインターフェイスまたは VLAN にアタッチします。
ステップ 4	**exit**	インターフェイス コンフィギュレーション モードを終了します。

IPv6 DHCP ガード ポリシーの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp guard policy** *policy-name*
4. [**default** | **device-role** [**client** | **server**] |**no** | **exit** | **trusted-port**]
5. **exit**
6. 次のいずれかの作業を実行します。
   - **interface** *type number*
   - **ipv6 dhcp guard attach-policy** *policy-name*

     または
   - **vlan configuration** *vlan-id*
   - **ipv6 dhcp guard attach-policy** *policy-name*

7. **show ipv6 dhcp guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ipv6 dhcp guard policy** *policy-name*	DHCPv6 ガード ポリシー名を指定し、DHCPv6 ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**default** | **device-role** [**client** | **server**] |**no** | **exit** | **trusted-port**]	（任意）特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは **client** です。 • **client**：デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバー メッセージにはこのポートで破棄されます。 • **server**：適用されたデバイスが DHCPv6 サーバーであることを指定します。このポートでは、サーバー メッセージが許可されます。 （任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 5	**exit**	DHCP ガードポリシー グローバル コンフィギュレーション モードを終了します。
ステップ 6	次のいずれかの作業を実行します。 • **interface** *type number* • **ipv6 dhcp guard attach-policy** *policy-name* または	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 DHCP ガード ポリシーをインターフェイスまたは VLAN に適用します。

	コマンドまたはアクション	目的
	• **vlan configuration** *vlan-id* • **ipv6 dhcp guard attach-policy** *policy-name*	
ステップ 7	**show ipv6 dhcp guard policy** *policy_name*	DHCP ガード ポリシー設定を表示します。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan configuration 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **ipv6 source-guard** [**attach-policy** *policy-name*]
6. **exit**
7. **show ipv6 source-guard policy***policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**ipv6 source-guard policy** *policy_name*	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]	IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバル アドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカル アドレスから送信されたすべてのデータ トラフィックを許可します。
ステップ 5	**ipv6 source-guard**［**attach-policy** *policy-name*］	ポリシー名を指定します。 （任意）**attach-policy** *policy-name*：ポリシー名に基づいてフィルタリングします。
ステップ 6	**exit**	ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 7	**show ipv6 source-guard policy***policy_name*	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

デフォルト ルータ プリファレンス（DRP）の設定

ルータアドバタイズメント（RA）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 コマンドによって設定されるデフォルト ルータ プリファレンス（DRP）とともに送信されます。DRP が設定されていない場合は、RA はプリファレンス「中」とともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

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

インターフェイス上のルータの DRP を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 4	**ipv6 nd router-preference** {**high** | **medium** | **low**} 例： スイッチ(config-if)# **ipv6 nd router-preference medium**	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 5	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 interface** 例： スイッチ# **show ipv6 interface**	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： スイッチ# **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 ICMP レート制限の設定

ICMP レート制限はデフォルトで有効です。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 のレート制限パラメータを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**ipv6 icmp error-interval** *interval* [*bucketsize*] 例： スイッチ(config)# **ipv6 icmp error-interval 50 20**	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。 • *interval*：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。 • *bucketsize*：（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 4	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface** [*interface-id*] 例： スイッチ# **show ipv6 interface gigabitethernet0/1**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： スイッチ# **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 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングの設定

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最適化するためのレイヤ 3 IP スイッチングテクノロジーです。シスコ エクスプレス フォワーディングには高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。IPv4 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングはデフォルトで有効になっています。IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングはデフォルトでは無効になっていますが、IPv6 ルーティングを設定すると自動的に有効になります。

IPv6 ルーティングの設定を解除すると IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングは自動的に無効になります。IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングを設定で無効にすることはできません。IPv6 の状態を確認するには、**show ipv6 cef**特権 EXEC コマンドを入力します。

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の転送をグローバルに設定してから、**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、特定の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。

シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングの設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定

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」の章を参照してください。

スタティック IPv6 ルーティングを設定するには、次の手順を実行します。

始める前に

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有効にし、**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 パケットの転送を有効にします。また、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 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] 例： スイッチ(config)# **ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130**	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：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。 • */prefix length*：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 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（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、リンクローカルアドレスをネ

	コマンドまたはアクション	目的
		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。 （注） リンクローカルアドレスをネクストホップとして使用する場合は、*interface-id* を指定する必要があります（リンクローカルの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）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

ステップ 5	次のいずれかを使用します。
	• **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**detail**]][**recursive**] [**detail**]
	• **show ipv6 route static** [*updated*]
	例：
	`スイッチ# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	
	または
	`スイッチ# show ipv6 route static`
		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。
		• **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 ルートのみを表示します。
		• **recursive**：（任意）再帰スタティック ルートのみを表示します。**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 プレフィッ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。
		• 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

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： スイッチ# **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 RIP の設定

IPv6 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」の章を参照してください。

IPv6 の RIP ルーティングを設定するには、次の手順を実行します。

始める前に

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有効にし、**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 パケットの転送を有効にして、IPv6 RIP を有効にするレイヤ 3 インターフェイス上で IPv6 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**ipv6 router rip** *name* 例： スイッチ(config)# **ipv6 router rip cisco**	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。

	コマンドまたはアクション	目的
ステップ 4	**maximum-paths** *number-paths* 例： `スイッチ(config-router)# maximum-paths 6`	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 5	**exit** 例： `スイッチ(config-router)# 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* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	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 rip** *name* **enable** 例： `スイッチ(config-if)# ipv6 rip cisco enable`	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有効にします。
ステップ 8	**ipv6 rip** *name* **default-information** {**only** | **originate**} 例： `スイッチ(config-if)# ipv6 rip cisco default-information only`	（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。 （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。 • **only**：このインターフェイスから送信するアップデートに、デフォルト ルートを格納し、その他のすべてのルートを含めない場合に選択します。 • **originate**：このインターフェイスから送信するアップデートに、デフォルト ルートおよびその他のすべてのルートを格納する場合に選択します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

ステップ 10	次のいずれかを使用します。
	• **show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**]
	• **show ipv6 rip**
	例：
	`スイッチ# show ipv6 rip cisco interface gigabitethernet 2/0/1`
	または
	`スイッチ# show ipv6 rip`
		• 現在の 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 11	**copy running-config startup-config** 例： `スイッチ# 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 OSPF の設定

IPv6 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」の章を参照してください。

IPv6 の OSPF ルーティングを設定するには、次の手順を実行します。

始める前に

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのお客様および機能の要件を満たします。

次の注意事項に従ってください。

- 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 を有効にする前に、**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有効にし、**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 パケットの転送を有効にし、IPv6 OSPF を有効にするレイヤ 3 インターフェイスで IPv6 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**ipv6 router ospf** *process-id* 例： スイッチ(config)# **ipv6 router ospf 21**	プロセスに対して OSPF ルータ コンフィギュレーション モードを有効にします。プロセス ID は、IPv6 OSPF ルーティング プロセスを有効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 4	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*] 例： スイッチ(config)# **area .3 range 2001:0DB8::/32 not-advertise**	（任意）エリア境界でルートを統合および集約します。 • *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 プレフィッ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）アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 のサマリー リンクステート アドバタイズメント（LSA）を生成します。 • **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を設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で

	コマンドまたはアクション	目的
		使用します。指定できる値は 0 ～ 16777215 です。
ステップ 5	**maximum paths** *number-paths* 例： `スイッチ(config)# maximum paths 16`	（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 ～ 32 で、デフォルトは 16 です。
ステップ 6	**exit** 例： `スイッチ(config-if)# 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 7	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	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 8	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] 例： `スイッチ(config-if)# ipv6 ospf 21 area .3`	インターフェイスで IPv6 の OSPF を有効にします。 • **instance** *instance-id*：（任意）インスタンス ID
ステップ 9	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

ステップ 10	次のいずれかを使用します。
	• **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]
	• **show ipv6 ospf** [*process-id*] [*area-id*]
	例：
	`スイッチ# show ipv6 ospf 21 interface gigabitethernet2/0/1`
	または
	`スイッチ# show ipv6 ospf 21`
		• 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。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： スイッチ# **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。

OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf***process-id*
4. **timers lsa arrival** *milliseconds*
5. **timers pacing flood***milliseconds*
6. **timers pacing lsa-group***seconds*
7. **timers pacing retransmission***milliseconds*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**ipv6 router ospf***process-id*	OSPFv3 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。
ステップ 4	**timers lsa arrival** *milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 5	**timers pacing flood***milliseconds*	LSA フラッド パケット ペーシングを設定します。

	コマンドまたはアクション	目的
ステップ 6	**timers pacing lsa-group***seconds*	OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。
ステップ 7	**timers pacing retransmission***milliseconds*	OSPFv3 での LSA 再送信パケット ペーシングを設定します。
ステップ 8	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf***process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa***start-intervalhold-intervalmax-interval*
6. **timers lsa arrival***milliseconds*
7. **timers pacing flood***milliseconds*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `スイッチ> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `スイッチ# 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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf***process-id*	OSPFv3 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。
ステップ 4	**timers throttle spf** *spf-start spf-hold spf-max-wait*	SPF スロットリングをオンにします。
ステップ 5	**timers throttle lsa***start-intervalhold-intervalmax-interval*	OSPFv3 LSA 生成に対するレート制限値を設定します。
ステップ 6	**timers lsa arrival***milliseconds*	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 7	**timers pacing flood***milliseconds*	LSA フラッド パケット ペーシングを設定します。
ステップ 8	**end** 例： `スイッチ(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、 **ip routing global configuration** グローバル コンフィギュレーション コマンドを入力してルーティングを有効にし、**ipv6 unicast-routing global** グローバル コンフィギュレーション コマンドを入力して IPv6 パケットの転送を有効にし、IPv6 EIGRP を有効にするレイヤ 3 インターフェイス上で IPv6 を有効にします。

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、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これら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。**passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、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 の HSRP の設定

IPv6 の Hot Standby Router Protocol（HSRP）は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。

スイッチで IPv6 の HSRP がイネーブルである場合、IPv6 ホストは IPv6 ネイバー探索ルータのアドバタイズメント メッセージから使用可能な IPv6 ルータを学習します。HSRP IPv6 グループには、HSRP グループ番号に基づいて作成される仮想 MAC アドレスがあります。グループ

には、デフォルトで、HSRP 仮想 MAC アドレスに基づいて作成される仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。

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

（注） IPv6 の 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 の HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

IPv6 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」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始して、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**} 例： `スイッチ(config-if)# standby version 2`	HSRP バージョンを設定します。HSRP バージョンを変更するには、**2** を入力します。デフォルトは 1 です。
ステップ 4	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show standby** 例： `スイッチ# show standby`	設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `スイッチ# 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 の HSRP グループのイネーブル化

ここでは、レイヤ 3 インターフェイス上で IPv6 の HSRP を作成するかイネーブルにする方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	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 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。
ステップ 3	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**} 例： `スイッチ(config-if)# standby 2 ipv6 auto config`	IPv6 グループの HSRP を作成（またはイネーブルに）します。 • （任意）*group-number*：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、リンクローカル プレフィックスおよび変更された

	コマンドまたはアクション	目的
		EUI-64 形式のインターフェイス ID から自動的に生成されるリンクローカルアドレスをイネーブルにします。この場合、EUI-64 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	**standby** [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}] 例： `スイッチ(config-if)# standby 2 preempt delay reload 0`	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。 • （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（引き継ぐまで遅延がない）。 • （任意）**reload**：リロード後のプリエンプション遅延（秒）を設定します。遅延時間は、ルータのリロード後の最初のインターフェイスアップ イベントに対してだけ適用されます。 • （任意）**sync**：IP 冗長クライアントの最大同期化時間（秒）を設定します。 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 5	**standby** [*group-number*] **priority** *priority* 例： `スイッチ(config-if)# standby 2 priority 200`	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 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。 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	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show standby** [*interface-id* [*group-number*]] 例：	設定を確認します。

	コマンドまたはアクション	目的
	スイッチ# **show standby gigabitethernet 1/0/1 2**	
ステップ 8	**copy running-config startup-config** 例： スイッチ# **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。

Multi-VRF CE の設定

スイッチ上で IP サービスまたは拡張 IP サービス フィーチャ セットが稼働している場合、スイッチはカスタマー エッジ（CE）デバイスの複数の VRF ルーティング/転送（Multi-VRF）インスタンスをサポートします（Multi-VRF CE）。サービス プロバイダは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。

（注） スイッチでは、VPNのサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。

IPv6 マルチキャスト ルーティングは VRF 関連インターフェイスではサポートされません。

Multi-VRF CE のデフォルト設定

表 *2: VRF* のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

VRF の設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 unicast-routing** 例： `スイッチ(config)# ipv6 unicast routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。
ステップ 3	**vrf definition** *vrf-name* 例： `スイッチ(config)# vrf definition vpn1`	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address family** *ipv6* 例： `スイッチ(config)# address family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**rd** *route-distinguisher* 例： `スイッチ(config-vrf)# rd 100:2`	ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `スイッチ(config-vrf)# route-target both 100:2`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* は、ステップ 4 で入力した *route-distinguisher* と同一にする必要があります。
ステップ 7	**import map** *route-map* 例： `スイッチ(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。
ステップ 8	**interface** *interface-id* 例： `スイッチ(config-vrf)# interface gigabitethernet 1/0/1`	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。

	コマンドまたはアクション	目的
ステップ 9	**vrf forwarding** *vrf-name* 例： `スイッチ(config-if)# vrf forwarding vpn1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `スイッチ# show vrf interfaces vpn1`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 12	**copy running-config startup-config** 例： `スイッチ# 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。

VRF 認識サービスの設定

次のサービスは、VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル（SNMP）
- ホットスタンバイ ルータ プロトコル（HSRP）
- ユニキャスト RPF（uRPF）
- Syslog
- traceroute
- FTP および TFTP

（注） このスイッチでは、ユニキャスト RPF（uRPF）およびネットワーク タイム プロトコル（NTP）に対して VRF 認識のサービスはサポートされません。

ネイバー探索用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 neighbors vrf***vrf-name* 例： `スイッチ# show ipv6 neighbors vrf vpn1`	指定された VRF 内の ARP テーブルを表示します。

ping 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**ping vrf***vrf-name***ipv6***ipv6-address* 例： `スイッチ# ping vrf vpn1 ipv6`	指定された VRF 内の ARP テーブルを表示します。

HSRP 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release 12.4*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： スイッチ# **interface gigabitethernet1/0/1**	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、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	**no switchport** 例： スイッチ# 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 4	**vrf forwarding***vrf-name* 例： スイッチ# vrf forwarding vpn1	インターフェイス上で VRF を設定します。
ステップ 5	**ipv6 address***ipv6 address* 例： スイッチ# ipv6 address 2001::DB8:1/64	インターフェイスの IPv6 アドレスを入力します。
ステップ 6	**standby 1 ipv6***ipv6 address* 例： スイッチ# standby 1 ipv6 2001::DB8:1/64	HSRP をイネーブルにし、仮想 IP アドレスを設定します。
ステップ 7	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。

traceroute 用 VRF 認識サービスの設定

コマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Switching Services Command Reference, Release*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf***vrf-nameipv6-address* 例： スイッチ# traceroute vrf**vpn1 2001::DB8:1/64**	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP 用 VRF 認識サービスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **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 ftp source-interface** *interface-type interface-number* 例： スイッチ(config)# ip ftp source-interface gigabitethernet 1/0/2	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	**end** 例： スイッチ(config)#end	特権 EXEC モードに戻ります。
ステップ 4	**configure terminal** 例： スイッチ# 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 5	**ip tftp source-interface** *interface-type interface-number* 例： スイッチ(config)# ip tftp source-interface gigabitethernet 1/0/2	TFTP 接続用の送信元 IP アドレスを指定します。
ステップ 6	**end** 例： スイッチ(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**end** 例： スイッチ(config)#end	特権 EXEC モードに戻ります。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされるルーティング プロトコル（OSPF、EIGRP、または BGP）、またはスタティック ルーティングで設定できます。ここで説明する設定はOSPF のものですが、その他のプロトコルでも手順は同じです。

（注） VRF インスタンス内で EIGRP ルーティングプロセスが実行されるように設定するには、**autonomous-system** *autonomous-system-number* アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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	**router ospfv3** *process-id* 例： `スイッチ(config)# router ospfv3 1`	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、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	**router** *router-id* 例： `スイッチ(config)# router router-id`	この OSPFv3 プロセスの OSPF ルータ ID を IP アドレス形式で指定します。
ステップ 4	**log-adjacency-changes** 例： `スイッチ(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。これは、デフォルトの状態です。
ステップ 5	**address-family ipv6 unicast vrf** *vrf-name* 例： `スイッチ(config-router)# address-family ipv6 unicast vrf vpn1`	その VRF に対してアドレス ファミリ コマンド モードを開始します。
ステップ 6	**area** *area-id normal* 例： `スイッチ(config-router)# area 2`	OSPFv3 エリア パラメータとタイプを指定します。

	コマンドまたはアクション	目的
ステップ 7	**redistribute bgp** *autonomous-system-number* 例： `スイッチ(config-router)# redistribute bgp 10`	BGP ルーティング プロセスから OSPF ルーティング プロセスにルートを再配布します。
ステップ 8	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ospfv3 vrf** *vrf-name* 例： `スイッチ# show ospfv3 vrf vpn1`	OSPFv3 ネットワークの設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `スイッチ# 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。

BGP PE/CE ルーティング セッションの設定

手順

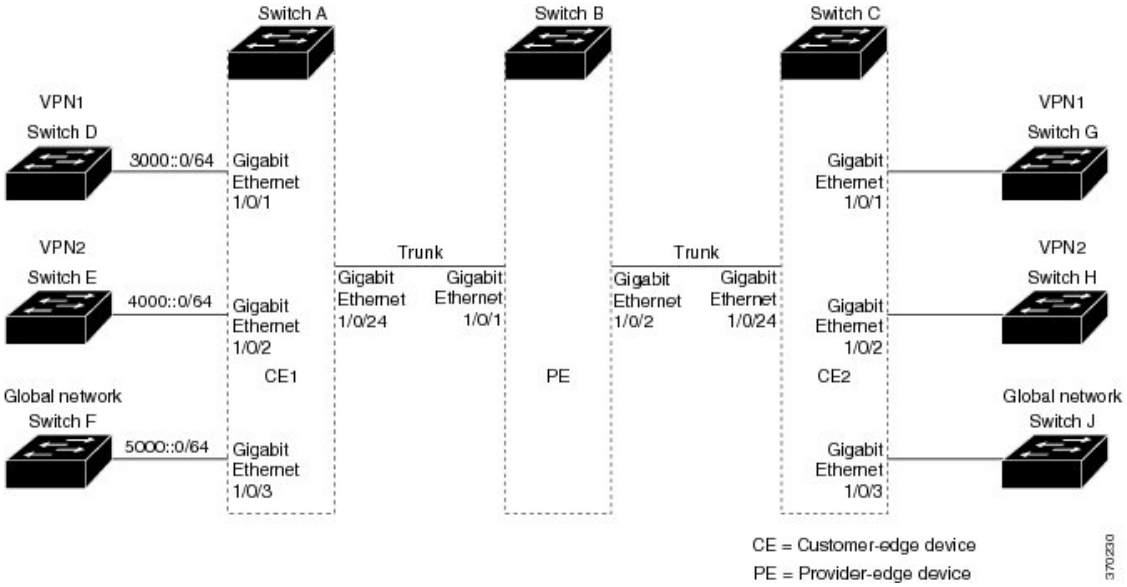
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* 例： `スイッチ(config)# router bgp 2`	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**bgp router id** *router-id* 例： `スイッチ(config)# bgp router-id`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル ルータの ID として設定します。
ステップ 4	**redistribute ospf** *process-id* 例：	OSPF 内部ルートを再配布するようにスイッチを設定します。

	コマンドまたはアクション	目的
	`スイッチ(config-router)# redistribute ospf 1`	
ステップ 5	**address-family ipv6 vrf** *vrf-name* 例： `スイッチ(config-router)# address-family ipv6 vrf vpn1`	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 6	**network** *ipv6 network-number* 例： `スイッチ(config-router)# network ipv6 255.255.255.0`	BGP を使用して IPv6 ネットワーク番号をアナウンスするように指定します。
ステップ 7	**neighbor** *ipv6 address* **remote-as** *as-number* 例： `スイッチ(config-router)# neighbor 10.1.1.2 remote-as 2`	PE と CE ルータの間の BGP セッションを定義します。
ステップ 8	**neighbor** *address* **activate** 例： `スイッチ(config-router)# neighbor 10.2.1.1 activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `スイッチ(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show bgp vrf** *vrf-name* 例： `スイッチ# show ip bgp ipv4 neighbors`	VRF の BGP 設定を確認します。
ステップ 11	**copy running-config startup-config** 例： `スイッチ# 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。

Multi-VRF CE の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。図のあとに続く出力は、スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と E の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同様です。

図 *1 : Multi-VRF CE* の設定例



スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ipv6 unicast-routing
スイッチ(config)# vrf definition v11
スイッチ(config-vrf)# rd 11:1
スイッチ(config-vrf)# address-family ipv6
スイッチ(config-vrf)# exit
スイッチ(config-vrf)# vrf definition v12
スイッチ(config-vrf)# rd 12:1
スイッチ(config-vrf)# address-family ipv6
スイッチ(config-vrf-af)# end
```

スイッチ A の物理インターフェイスを設定します。ギガビット イーサネット インターフェイス 1/0/24 は PE へのトランク接続です。ギガビット イーサネット ポート 1/0/1 と 1/0/2 は VPN に接続されます。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# interface GigabitEthernet 1/0/1
スイッチ(config-if)# switchport access vlan 208
スイッチ(config-if)# no ip address
```

```
スイッチ(config-if)# exit
スイッチ(config)# interface gigabitEthernet 1/0/2
スイッチ(config-if)# switchport access vlan 118
スイッチ(config-if)# no ip address
スイッチ(config-if)# exit
スイッチ(config)# interface GigabitEthernet 1/0/24
スイッチ(config-if)# switchport trunk encapsulation dot1q
スイッチ(config-if)# switchport mode trunk
スイッチ(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ E とスイッチ D を含む VPN に使用されます。

```
スイッチ(config)# interface vlan10
スイッチ(config-if)# vrf forwarding v11
スイッチ(config-if)# ipv6 address 1000::1/64
スイッチ(config-if)# exit

スイッチ(config)# interface vlan20
スイッチ(config-if)# vrf forwarding v12
スイッチ(config-if)# ipv6 address 2000::1/64
スイッチ(config-if)# exit

スイッチ(config)# interface vlan208
スイッチ(config-if)# vrf forwarding v11
スイッチ(config-if)# ipv6 address 3000::1/64
スイッチ(config-if)# exit

スイッチ(config)# interface vlan118
スイッチ(config-if)# vrf forwarding v12
スイッチ(config-if)# ipv6 address 4000::1/64
スイッチ(config-if)# exit
```

VPN1 と VPN2 で OSPFv3 ルーティングを設定します。

```
スイッチ(config)# router ospfv3 1
スイッチ(config-router)# router-id 10.1.1.10
スイッチ(config-router)# address-family ipv6 unicast vrf v11
スイッチ(config-router-af)# area 0 normal
スイッチ(config-router-af)# redistribute bgp 800
スイッチ(config-router)# exit
スイッチ(config)# router ospfv3 2
スイッチ(config-router)# router-id 2.2.2.2
スイッチ(config-router)# address-family ipv6 unicast vrf v12
スイッチ(config-router-af)# area 0 normal
スイッチ(config-router-af)# redistribute bgp 800
スイッチ(config-router-af)# exit
スイッチ(config-router)# exit
スイッチ(config)# exit
```

CE/PE ルーティングに BGP を設定します。

```
スイッチ(config)# router bgp 800
スイッチ(config-router)# bgp router-id 8.8.8.8
スイッチ(config-router)# address-family ipv6 vrf v11
スイッチ(config-router-af)# redistribute ospf 1
スイッチ(config-router-af)# neighbor 1000::2 remote-as 100
スイッチ(config-router-af)# neighbor 1000::2 activate
スイッチ(config-router-af)# network 3000::/64
スイッチ(config-router-af)# exit

スイッチ(config)# address-family ipv6 vrf v12
スイッチ(config-router-af)# redistribute ospf 2
スイッチ(config-router-af)# neighbor 2000::2 remote-as 100
スイッチ(config-router-af)# neighbor 2000::2 activate
スイッチ(config-router-af)# network 4000::/64
```

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
スイッチ# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)# ipv6 unicast-routing
スイッチ(config)# interface GigabitEthernet 5/0/16
スイッチ(config-if)# no switchport
スイッチ(config-if)# ipv6 address 3000::2/64
スイッチ(config-if)# exit

スイッチ(config-router)# router ospfv3 101
スイッチ(config-router)# address-family ipv6
スイッチ(config-router-af)# area 0 normal
スイッチ(config-router-af)# redistribute connected
スイッチ(config-router-af)# exit
スイッチ(config-router)# exit
```

スイッチ E は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
スイッチ(config)# ipv6 unicast-routing
スイッチ(config)# interface GigabitEthernet 3/0/13
スイッチ(config-if)# switchport access vlan 20
スイッチ(config-if)# exit
スイッチ(config)# interface vlan 20
スイッチ(config-if)# ipv6 address 4000::2/64


スイッチ(config)# router ospfv3 101
スイッチ(config-router)# address-family ipv6
スイッチ(config-router-af)# area 0 normal
スイッチ(config-router-af)# redistribute connected
スイッチ(config-router-af)# end
```

このコマンドをスイッチB（PEルータ）で使用すると、CEデバイス、スイッチAに対する接続だけが設定されます。

```
スイッチ(config)# vrf definition v1
スイッチ(config-vrf)# rd 1:1
スイッチ(config-vrf)# address-family ipv6
スイッチ(config-vrf-af)# exit
スイッチ(config-vrf)# exit

スイッチ(config)# vrf definition v2
スイッチ(config-vrf)# rd 2:1
スイッチ(config-vrf)# address-family ipv6
スイッチ(config-vrf-af)# exit
スイッチ(config-vrf)# exit

スイッチ(config-if)# interface g 1/0/2
スイッチ(config-if)# vrf forwarding v1
スイッチ(config-if)# ipv6 address 1000::2/64
スイッチ(config-if)# exit
スイッチ(config)# interface g 1/0/4
スイッチ(config-if)# vrf forwarding v2
スイッチ(config-if)# ipv6 address 2000::2/64

スイッチ(config-if)# interface gigabitEthernet 1/0/1
スイッチ(config-if)# switchport trunk encapsulation dot1q
スイッチ(config-if)# switchport mode trunk

スイッチ(config)# router bgp 100
スイッチ(config-router)# address-family ipv6 vrf v1
スイッチ(config-router-af)# neighbor 1000::1 remote-as 100
スイッチ(config-router-af)# neighbor 1000::1 activate
スイッチ(config-router-af)# network 3000::/64
スイッチ(config-router-af)# exit
スイッチ(config-router)# address-family ipv6 vrf v2
スイッチ(config-router-af)# neighbor 2000::1 remote-as 100
スイッチ(config-router-af)# neighbor 2000::1 activate
スイッチ(config-router-af)# network 4000::/64
```

Multi-VRF CE ステータスの表示

表 *3 : Multi-VRF CE* 情報を表示するコマンド

コマンド	目的
show ipv6 protocols vrf*vrf -name*	VRFに対応付けられたルーティングプロトコル情報を表示します。
show ipv6 route vrf*vrf -name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRFに対応付けられたIPルーティングテーブル情報を表示します。

コマンド	目的
show ipv6 vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。

IPv6 の表示

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

表 *4 : IPv6* をモニタリングするコマンド

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 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface *interface-id*	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に IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバーキャッシュ エントリを表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
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。

DHCP for IPv6 アドレス割り当ての設定

この項では、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバー、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」の章を参照してください。

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

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。

- 以下の手順では、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。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上で有効である必要があります。
  - 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ネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバー、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、サーバー、およびリレー機能は、インターフェイスで相互に排他的です。

DHCPv6 サーバー機能の有効化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバー機能を無効にするには、**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。

インターフェイスで DHCPv6 サーバー機能を有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 dhcp pool** *poolname* 例： `スイッチ(config)# ipv6 dhcp pool 7`	DHCP プール コンフィギュレーション モードを開始して、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 4	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： `スイッチ(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime 3600`	（任意）アドレス割り当て用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 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効な状態を維持するタイム インターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。時間間隔なしの場合は、**infinite** を指定します。
ステップ 5	**link-address** *IPv6-prefix* 例： `スイッチ(config-dhcpv6)# link-address 2001:1002::0/64`	（任意）link-address 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のリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバーは設定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 進数で指定する必要があります。
ステップ 6	**vendor-specific** *vendor-id* 例： `スイッチ(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 7	**suboption** *number* { **address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} 例： `スイッチ(config-dhcpv6-vs)# suboption 1 address 1000:235D::`	（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 進文字列をサブオプション パラメータで定義されているように入力します。
ステップ 8	**exit** 例： `スイッチ(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `スイッチ(config-dhcpv6)# 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	**interface** *interface-id* 例： `スイッチ(config)# interface gigabitethernet 1/0/1`	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 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] 例： `スイッチ(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバー機能を有効にします。 • *poolname*：（任意）IPv6 DHCP プールのユーザー定義の名前。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）サーバーが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージを交換する方式を許可します。 • **preference** 値：（任意）サーバーによって送信されるアドバタイズメント メッセージ内のプリファレンス オプションで指定するプリファレンス値を設定します。範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバーが SOLICIT メッセージに含まれるクライアントの提案を考慮するかどうかを指定します。デフォルトでは、サーバーはクライアントのヒントを無視します。
ステップ 12	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	次のいずれかを実行します。	• DHCPv6 プール設定を確認します。

	コマンドまたはアクション	目的
	• **show ipv6 dhcp pool** • **show ipv6 dhcp interface** 例： スイッチ# **show ipv6 dhcp pool** または スイッチ# **show ipv6 dhcp interface**	• DHCPv6 サーバー機能がインターフェイス上で有効であることを確認します。
ステップ 14	**copy running-config startup-config** 例： スイッチ# **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 クライアント機能の有効化

インターフェイスで DHCPv6 クライアントを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： スイッチ# **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 3	**interface** *interface-id* 例： スイッチ(config)# **interface gigabitethernet 1/0/1**	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 4	**ipv6 address dhcp** [**rapid-commit**] 例： スイッチ(config-if)# **ipv6 address dhcp rapid-commit**	インターフェイスで DHCPv6 サーバーから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てに 2 つのメッセージを交換する方式を許可します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 dhcp client request** [**vendor-specific**] 例： `スイッチ(config-if)# 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 6	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 dhcp interface** 例： `スイッチ# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスで有効になっていることを確認します。

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクローカルアドレスおよびグローバルアドレスを使用して、IPv6 を有効にする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**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 プレフィックス 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すために追加されています。

```
スイッチ(config)# ipv6 unicast-routing
スイッチ(config)# interface gigabitethernet0/11

スイッチ(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
スイッチ(config-if)# end
スイッチ# show ipv6 interface gigabitethernet0/11
GigabitEthernet0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# interface gigabitethernet1/0/1
スイッチ(config-if)# ipv6 nd router-preference high
スイッチ(config-if)# end
```

IPv6 の HSRP グループのイネーブル化：例

次に、ポートのグループ 1 で IPv6 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 グループで使用される IP アドレスは、IPv6 の HSRP を使用して学習されます。

（注） これは、IPv6 の 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。

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

DHCPv6 サーバー機能の有効化：例

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

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

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

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

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
スイッチ# configure terminal
スイッチ(config)# ipv6 dhcp pool 350
スイッチ(config-dhcpv6)# address prefix 2001:1005::0/48
スイッチ(config-dhcpv6)# vendor-specific 9
スイッチ(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
スイッチ(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
スイッチ(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能の有効化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションを有効にする例を示します。

```
スイッチ(config)# interface gigabitethernet2/0/1
スイッチ(config-if)# ipv6 address dhcp rapid-commit
```

IPv6 ICMP レート制限の設定：例

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。

```
スイッチ(config)#ipv6 icmp error-interval 50 20
```

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
スイッチ(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 1/0/1 130
```

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* を有効にし、インターフェイス上でこれを有効にする例を示します。

```
スイッチ(config)# ipv6 router rip cisco
スイッチ(config-router)# maximum-paths 8
スイッチ(config)# exit
スイッチ(config)# interface gigabitethernet2/0/11
スイッチ(config-if)# ipv6 rip cisco enable
```

IPv6 の表示：例

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

```
スイッチ# 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>
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。