IPv6 アドレッシングおよび基本的な接続のコンフィギュレーション ガイド、Cisco IOS XE Release 3S

初版：2012 年 08 月 28 日

最終更新：2012 年 11 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

IPv6 のアドレッシングと基本接続

Internet Protocol Version 6（IPv6）は、ネットワーク アドレス ビット数を（IPv4 での）32 ビットから 128 ビットに拡張しているため、地球上のすべてのネットワーク デバイスにグローバルに一意な IP アドレスを十分に提供できます。 IPv6 によってアドレス空間が無制限に提供されるため、シスコは、信頼性があり、ユーザ エクスペリエンスやセキュリティが改善されたより新しいアプリケーションおよびサービスをさらに多く提供できます。

シスコ ソフトウェアでの基本的な IPv6 接続の実装は、個々のデバイス インターフェイスへの IPv6 アドレスの割り当てで構成されます。 IPv6 トラフィックの転送はグローバルにイネーブルにでき、IPv6 のシスコ エクスプレス フォワーディング スイッチングをイネーブルにすることもできます。 ユーザは、ドメイン ネーム システム（DNS）の名前からアドレスおよびアドレスから名前のルックアップ プロセスで AAAA レコード タイプのサポートを設定し、IPv6 ネイバー探索を管理することで基本接続を拡張できます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 アドレッシングと基本接続の実装の制約事項

- スイッチは、IPv6 フレームを転送する前にレイヤ 3 パケット情報を確認しないため、IPv6 パケットは、レイヤ 2 LAN スイッチに対して透過的です。 したがって、IPv6 ホストをレイヤ 2 LAN スイッチに直接接続できます。
- 1 つのインターフェイス上で同じプレフィックス内に複数の IPv6 グローバル アドレスを設定できますが、1 つのインターフェイス上の複数の IPv6 リンクローカル アドレスはサポートされていません。

IPv6 のアドレッシングと基本接続に関する情報

シスコ ソフトウェアの IPv6

以前は IPng（次世代）と呼ばれていた IPv6 は、インターネット プロトコル（IP）の最新バージョンです。 IP は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。 IP バージョン 4（IPv4）の 32 ビット アドレッシング方式ではインターネットの成長の需要を十分に満たせないことが明らかになったときに、IPv6 が提案されました。 長い議論のあとで、IP を IPng のベースにするが、はるかに大きなアドレス空間と、簡略化されたメイン ヘッダーや拡張ヘッダーなどの改善を追加することが決定されました。 IPv6 は、Internet Engineering Task Force（IETF）から発行されている RFC 2460、『*Internet Protocol, Version 6 (IPv6) Specification*』で最初に説明されています。 IPv6 でサポートされるアーキテクチャとサービスについては他の RFC で規定されています。

IPv6 のアーキテクチャは、エンドツーエンドのセキュリティ、Quality of Service（QoS）、グローバルに一意なアドレスなどのサービスを提供する一方で、既存の IPv4 ユーザが IPv6 に簡単に移行できるように設計されています。 拡大された IPv6 アドレス空間により、ネットワークのスケーラビリティが可能となり、グローバルな到達可能性が提供されます。 簡素化された IPv6 パケット ヘッダー形式により、パケットの処理効率が向上しています。 IPv6 プレフィックス集約、簡略化されたネットワーク リナンバリング、および IPv6 サイト マルチホーミング機能によって、より効率的なルーティングを実現する IPv6 アドレッシング階層が提供されます。 IPv6 は、Routing Information Protocol（RIP）、Integrated Intermediate System-to-Intermediate System（IS-IS）、IPv6 向け Open Shortest Path First（OSPF）、マルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）などの広く採用されているルーティング プロトコルをサポートしています。 他の使用可能な機能には、ステートレス自動設定、数が増えたマルチキャスト アドレスなどがあります。

一意のアドレスを確保するための大きな IPv6 アドレス空間

グローバルに一意な IP アドレスの需要を満たす必要があることが、IPv6 の主な目的です。 IPv6 は、ネットワーク アドレス ビット数を（IPv4 での）32 ビットの 4 倍の 128 ビットにしているため、地球上のすべてのネットワークデバイスにグローバルに一意なIPアドレスを十分に提供できます。IPv6アドレスをグローバルに一意にすることで、ネットワークデバイスのグローバルな到達可能性とエンドツーエンドのセキュリティが実現されます。これは、アドレスの需要を喚起するアプリケーションとサービスに不可欠な機能です。また、柔軟性の高いIPv6アドレス空間により、プライベート アドレスの必要性が低減されます。したがって、IPv6 を使用すると、ネットワークエッジにある境界デバイスによる特別な処理を必要としない新しいアプリケーションプロトコルがイネーブルになります。

IPv6 アドレス形式

IPv6アドレスは、x:x:x:x:x:x:x:x のようにコロン（:）で区切られた一連の 16 ビットの 16 進フィールドで表されます。 次に、IPv6 アドレスの例を 2 つ示します。

2001:DB8:7654:3210:FEDC:BA98:7654:3210

2001:DB8:0:0:8:800:200C:417A

IPv6アドレスには、通常、連続するゼロの16進フィールドが含まれます。 IPv6アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続 16 進数フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。 次の表に、圧縮された IPv6 アドレスの形式をリストします。

連続する 16 ビット値がゼロとして指定されている場合は、2 つのコロンを *ipv6-address* 引数の一部として使用できます。インターフェイスごとに複数のIPv6アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

（注） IPv6アドレスでは、最も長く連続するゼロの16進フィールドを表すために2つのコロン（::）を 1 回だけ使用できます。 IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

表 *1*：圧縮された *IPv6* アドレス形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

ノードは、上の表に示されているループバック アドレスを使用して、IPv6 パケットを自身に送信できます。 IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注） IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。 IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。 IPv6 デバイスは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

上の表に示されている未指定アドレスは、IPv6 アドレスがないことを示します。 たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注） IPv6 未指定アドレスは、インターフェイスに割り当てることができません。 未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ipv6-prefix/*prefix-length* 形式の IPv6 アドレス プレフィックスを使用すると、アドレス空間全体のビット単位の連続ブロックを表現できます。 *ipv6-prefix* は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。 プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。 たとえば、2001:DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 アドレスの出力表示

IPv6 または IPv4 コマンドの出力に IPv6 アドレスが表示される場合、長い IPv6 アドレスが隣接フィールドにオーバーフローし、出力が読みにくくなることがあります。 出力フィールドは、考えられる最長の IPv4 アドレス（15 文字）に対応するように設計されました。IPv6 アドレスは最大 39 文字です。 適切な長さの IPv6 アドレスを表示し、必要に応じて以降のフィールドを次の行に移動するために、以下の方式が IPv4 および IPv6 コマンドに採用されました。 移動されるフィールドは、ヘッダー行に位置揃えされます。

次の例では、8 つの接続が表示されています。 最初の 6 つの接続には IPv6 アドレスを使用し、最後の 2 つの接続には IPv4 アドレスを使用しています。

```
Device# where
Conn Host                Address             Byte  Idle Conn Name
   1 test5               2001:DB8:3333:4::5    6    24 test5
   2 test4               2001:DB8:3333:44::5
                                               6    24 test4
   3 2001:DB8:3333:4::5 2001:DB8:3333:4::5     6    24 2001:DB8:3333:4::5
   4 2001:DB8:3333:44::5
                         2001:DB8:3333:44::5
                                               6    23 2001:DB8:3333:44::5
   5 2001:DB8:3000:4000:5000:6000:7000:8001
                         2001:DB8:3000:4000:5000:6000:7000:8001
                                               6    20 2001:DB8:3000:4000:5000:6000:
```

```
   6 2001:DB8:1::1       2001:DB8:1::1          0     1 2001:DB8:1::1
   7 10.1.9.1             10.1.9.1              0     0 10.1.9.1
   8 10.222.111.222       10.222.111.222        0     0 10.222.111.222
```

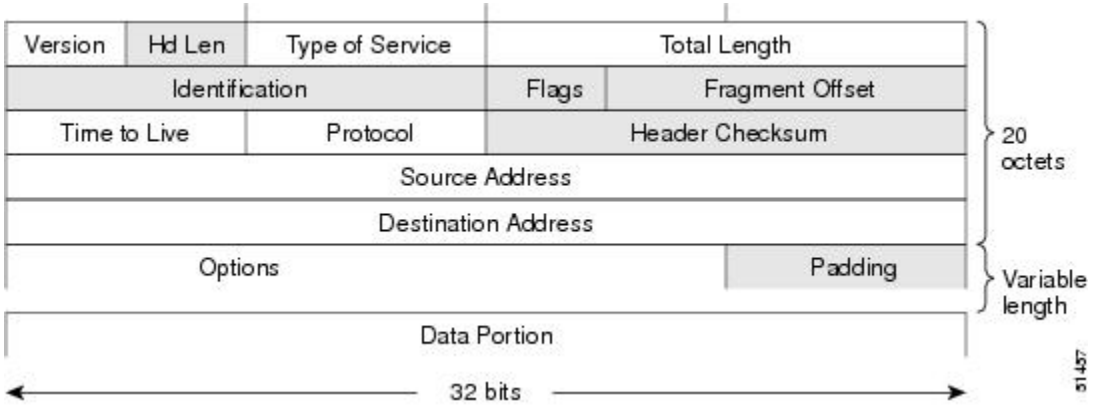
接続 1 には、アドレス フィールドの最大アドレス長を使用する IPv6 アドレスが含まれます。 接続 2 では、IPv6 アドレスによってアドレス フィールドがオーバーフローし、以降のフィールドが次の行に移動されますが、適切なヘッダーに位置揃えされていることが示されています。 接続 3 には、どの行もラップせずにホスト名フィールドとアドレス フィールドの最大長を充てんする IPv6 が含まれます。 接続 4 は、ホスト名フィールドとアドレス フィールドの両方に長い IPv6 アドレスが含まれる場合の結果を示しています。 出力は、適切な見出し位置を維持したまま、3 行にわたって表示されています。 接続 5 は接続 4 と同様に、ホスト名フィールドとアドレス フィールドの両方に非常に長い IPv6 アドレスが存在する結果を示しています。 実際には、接続名フィールドは切り捨てられています。 接続 6 では、表示の変更が不要な非常に短い IPv6 アドレスが表示されます。 接続 7 および 8 では、短い IPv4 アドレスと長い IPv4 アドレスが表示されます。

（注） IPv6 アドレスの出力表示は、IPv6 アドレスを表示するすべてのコマンドに適用されます。

簡易 IPv6 パケット ヘッダー

基本 IPv4 パケット ヘッダーには、合計サイズが 20 オクテット（160 ビット）の 12 のフィールドがあります（次の図を参照）。 この 12 個のフィールドのあとにはオプション フィールドが、さらにそのあとに、通常はトランスポート レイヤ パケットであるデータ部分が続く場合があります。 可変長のオプション フィールドは、IPv4 パケット ヘッダーの合計サイズに加算されます。 次の図に示す IPv4 パケット ヘッダーのグレーのフィールドは、IPv6 パケット ヘッダーに含まれません。

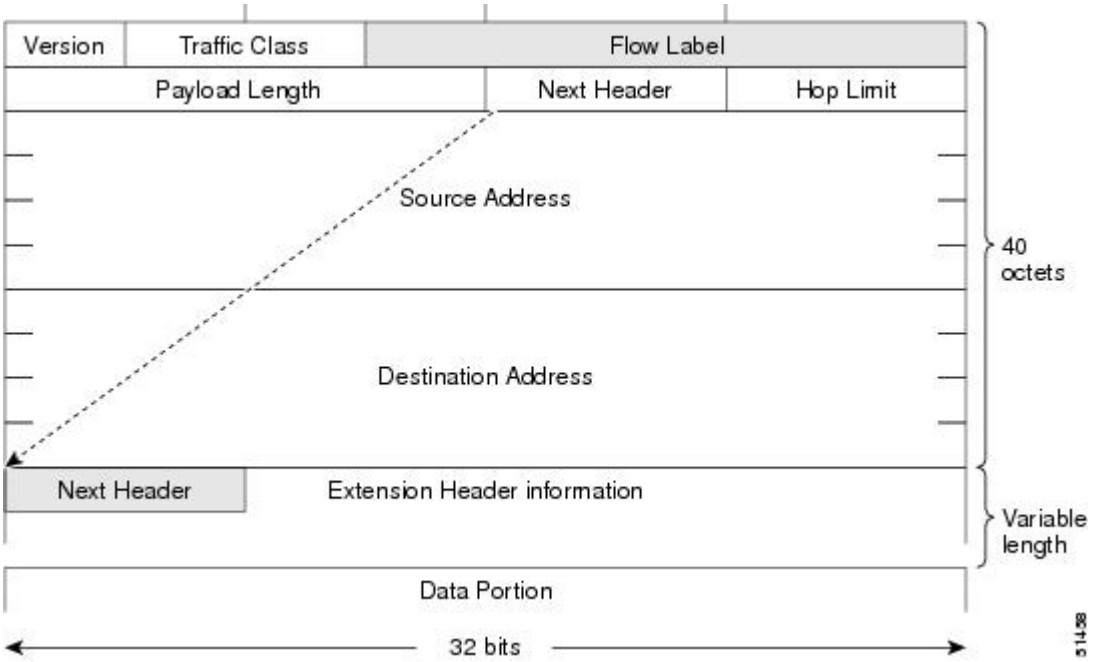
図 *1*：*IPv4* パケット ヘッダー形式



基本 IPv6 パケット ヘッダーには、合計サイズが 40 オクテット（320 ビット）の 8 つのフィールドがあります（次の図を参照）。 IPv6 では、フラグメンテーションはデバイスによって処理されず、チェックサムはネットワーク層で使用されないため、IPv6 ヘッダーからフィールドが除去されました。 代わりに、IPv6 のフラグメンテーションはパケットの送信元によって処理され、チェックサムはデータ リンク層とトランスポート層で使用されます （IPv4 では、UDP トランスポート

層でオプションのチェックサムが使用されます。 IPv6 では、内部パケットの整合性をチェックするために UDP チェックサムを使用する必要があります）。また、基本 IPv6 パケット ヘッダーとオプション フィールドは 64 ビットに揃えられるため、IPv6 パケットの処理が簡単になります。

図 *2*：*IPv6* パケット ヘッダー形式



次の表に、基本 IPv6 パケット ヘッダーのフィールドをリストします。

表 *2*：基本 *IPv6* パケット ヘッダー フィールド

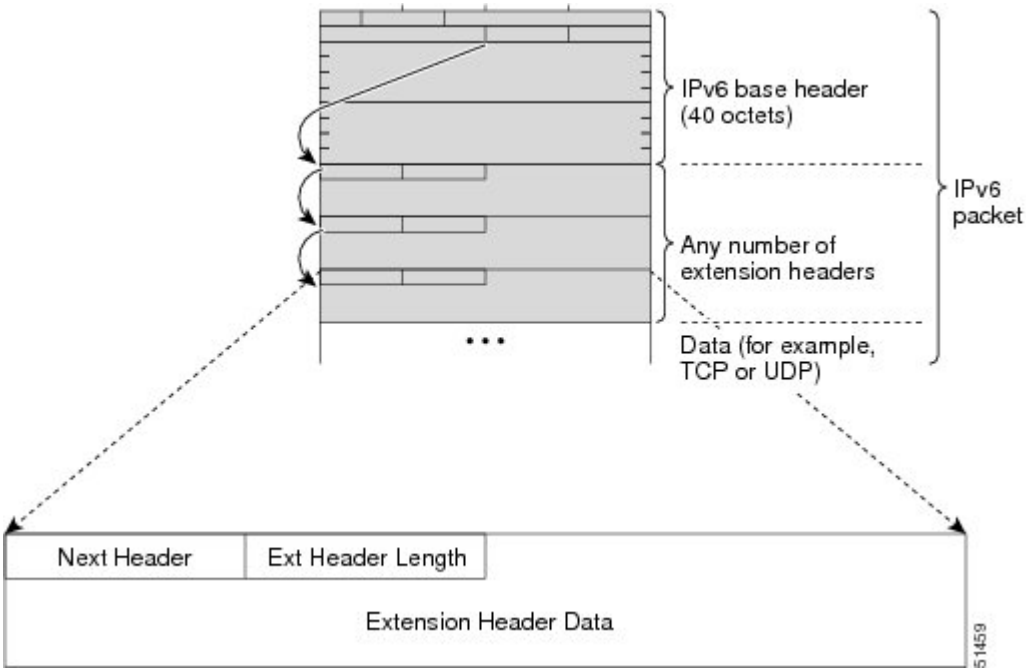
フィールド	説明
バージョン	IPv4 パケット ヘッダーのバージョン フィールドに該当しますが、IPv4 で示される数字 4 の代わりに、IPv6 では数字 6 が示されます。
トラフィック クラス	IPv4 パケット ヘッダーのタイプ オブ サービス フィールドと同様です。 トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。
フロー ラベル	IPv6 パケット ヘッダーの新しいフィールドです。 フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。

フィールド	説明
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。 ペイロード長フィールドは、パケットのデータ部分の合計長を示します。
次ヘッダー	IPv4 パケット ヘッダーのプロトコル フィールドと同様です。 次ヘッダー フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。 基本 IPv6 ヘッダーに続く情報のタイプは、上の図に示すように、TCP や UDP パケットなどのトランスポート レイヤ パケット、または拡張ヘッダーです。
ホップ リミット	IPv4 パケット ヘッダーの存続可能時間フィールドと同様です。 ホップ リミット フィールドの値は、IPv6 パケットが無効と見なされる前に通過できるデバイスの最大数です。 各デバイスを通過するたびに、この値が 1 ずつ減少します。 IPv6 ヘッダーにはチェックサムがないため、デバイスは値を減らすたびにチェックサムを再計算する必要がなく、処理リソースが節約されます。
送信元アドレス	IPv4 パケット ヘッダーの送信元アドレス フィールドと同様ですが、IPv4 の 32 ビット送信元アドレスの代わりに、IPv6 では 128 ビットの送信元アドレスが含まれます。
宛先アドレス	IPv4 パケット ヘッダーの宛先アドレス フィールドと同様ですが、IPv4 の 32 ビット宛先アドレスの代わりに、IPv6 では 128 ビットの宛先アドレスが含まれます。

基本 IPv6 パケット ヘッダーの 8 つのフィールドの後に、オプションの拡張ヘッダーおよびパケットのデータ部分が続きます。 存在する場合は、各拡張ヘッダーが 64 ビットに揃えられます。 IPv6 パケットの拡張ヘッダーの数は固定されていません。 拡張ヘッダーがヘッダーのチェーンを形成します。 各拡張ヘッダーは、前のヘッダーの次ヘッダー フィールドによって識別されます。 通

常は、最後の拡張ヘッダーに、TCP や UDP などのトランスポートレイヤプロトコルの次ヘッダーフィールドがあります。 次の図に、IPv6 拡張ヘッダー形式を示します。

図 *3* : *IPv6* 拡張ヘッダー形式



次の表に、拡張ヘッダー タイプとその次ヘッダー フィールド値をリストします。

表 *3* : *IPv6* 拡張ヘッダー タイプ

ヘッダー タイプ	次ヘッダーの値	説明
ホップバイホップ オプション ヘッダー	0	このヘッダーは、パケットのパス上のすべてのホップで処理されます。 存在する場合、ホップバイホップ オプション ヘッダーは、常に基本 IPv6 パケット ヘッダーの直後に続きます。
宛先オプション ヘッダー	60	宛先オプションヘッダーは、任意のホップバイホップ オプション ヘッダーの後に続くことがあります。その場合、宛先オプションヘッダーは、最終的な宛先と、ルーティングヘッダーで指定された各通過アドレスでも処理されます。また、宛先オプションヘッダーは、任意のカプセル化セキュリティ ペイロード（ESP）ヘッダーの後に続くこともあります。その場合、宛先オプションヘッダーは、最終的な宛先でだけ処理されます。

ヘッダー タイプ	次ヘッダーの値	説明
ルーティング ヘッダー	43	ルーティングヘッダーは送信元のルーティングに使用されます。
フラグメント ヘッダー	44	フラグメントヘッダーは、送信元が、送信元と宛先の間のパスの最大伝送単位（MTU）よりも大きいパケットをフラグメント化する必要がある場合に使用されます。フラグメントヘッダーは、フラグメント化された各パケットで使用されます。
認証ヘッダー および ESP ヘッダー	51 50	認証ヘッダーと ESP ヘッダーは、パケットの認証、整合性、および機密性を提供するために IP セキュリティ プロトコル（IPsec）内で使用されます。 これらのヘッダーは、IPv4 と IPv6 の両方で同一です。
上位層ヘッダー	6（TCP） 17（UDP）	上位層（トランスポート）ヘッダーは、データを転送するためにパケットの内部で使用される典型的なヘッダーです。 2 つの主要なトランスポート プロトコルは TCP と UDP です。
モビリティ ヘッダー	135	バインディングの作成と管理に関連するすべてのメッセージで、モバイル ノード、通信ノード、およびホームエージェントによって使用される拡張ヘッダーです。

DNS for IPv6

IPv6 では、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスでサポートされる DNS レコード タイプがサポートされます。 DNS レコード タイプでは、IPv6 アドレスがサポートされます。 IPv6 では、IPv6 アドレスから DNS 名への逆マッピングもサポートされます。

次の表に、IPv6 DNS レコード タイプをリストします。

表 *4*：*IPv6 DNS* レコード タイプ

レコード タイプ	説明	フォーマット
AAAA	ホスト名を IPv6 アドレスにマッピングします （IPv4 の A レコードと同等）。	www.abc.test AAAA 3FFE:YYYY:C18:1::2

レコード タイプ	説明	フォーマット
PTR	IPv6アドレスをホスト名にマッピングします （IPv4 の PTR レコードと同等）。 （注） シスコ ソフトウェアでは、IP6.INT ドメインの PTR レコードの解決がサポートされます。	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

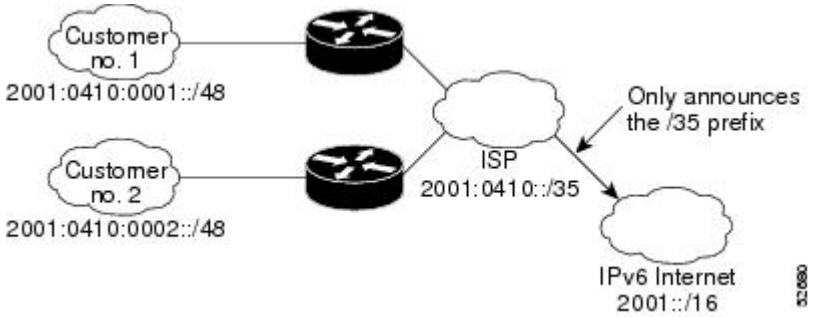
Cisco Discovery Protocol IPv6 アドレスのサポート

ネイバー情報の Cisco Discovery Protocol IPv6 アドレス サポート機能により、2 台のシスコ デバイス間でIPv6アドレッシング情報を転送する機能が追加されます。 IPv6アドレス向けCisco Discovery Protocol サポートは、ネットワーク管理製品およびトラブルシューティング ツールに IPv6 情報を提供します。

IPv6 プレフィックス集約

IPv6アドレス空間の集約可能な特性により、IPv6アドレッシング階層がイネーブルになります。たとえば、企業はサービスプロバイダーの単一のIPv6プレフィックスを複数のより長いプレフィックスに分割して、社内ネットワーク内で使用できます。反対に、サービスプロバイダーは、カスタマーのすべてのプレフィックスを、サービスプロバイダーがIPv6インターネット上でアドバタイズできる単一のより短いプレフィックスに集約できます（次の図を参照）。

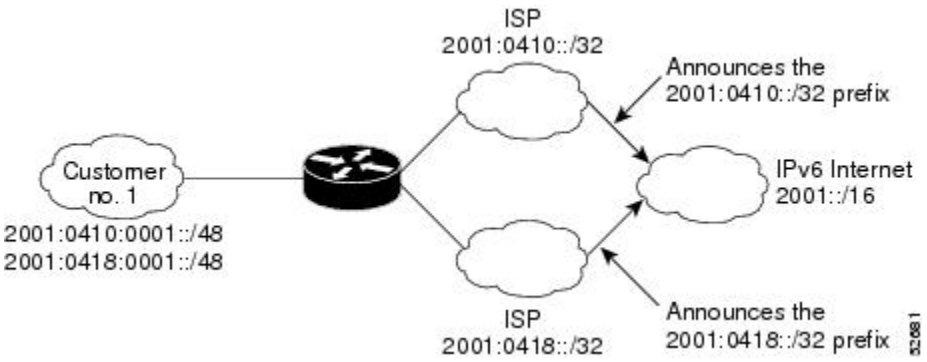
図 *4*：*IPv6* プレフィックス集約



IPv6 サイト マルチホーミング

複数の IPv6 プレフィックスをネットワークとホストに割り当てることができます。 複数のプレフィックスをネットワークに割り当てると、グローバル ルーティング テーブルを壊すことなくネットワークを複数の ISP に簡単に接続できるようになります（次の図を参照）。

図 *5*：*IPv6* サイト マルチホーミング



IPv6 データ リンク

IPv6ネットワークでは、データ リンクは特定のリンクローカルプレフィックスを共有するネットワークです。データ リンクは、接続しているネットワークのアドレッシングの複雑さをサブネットワークから隠しながらマルチレベルの階層ルーティング構造を提供するために、ネットワーク管理者によって任意にセグメント化されるネットワークです。 IPv6 のサブネットワークの機能は、IPv4 のサブネットワークと同様です。 サブネットワーク プレフィックスは 1 つのデータ リンクに関連付けられ、複数のサブネットワーク プレフィックスを同じデータ リンクに割り当てることができます。

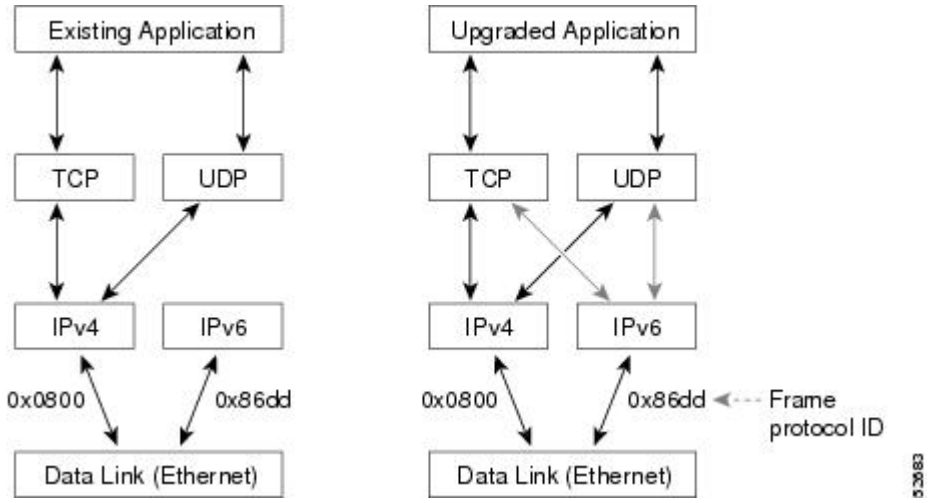
IPv6 では、FDDI、フレーム リレー PVC、Cisco ハイレベル データリンク コントロール（HDLC）、PPP over Packet over SONET、ISDN、シリアル インターフェイスの各データ リンクがサポートされます。

IPv4 と IPv6 の二重プロトコル スタック

デュアル IPv4 および IPv6 プロトコル スタック手法を使用して IPv6 に移行できます。 これにより、ノードで稼働しているアプリケーションに対する段階的な 1 つずつのアップグレードが可能になります。ノードで稼働しているアプリケーションは、IPv6プロトコルスタックを使用するようにアップグレードされます。 アップグレードされていないアプリケーション（IPv4プロトコルスタックだけをサポートするなど）は、1 つのノードでアップグレードされたアプリケーション

と共存できます。 新しいアプリケーションとアップグレードされたアプリケーションでは、IPv4 と IPv6 の両方のプロトコル スタックを使用します（次の図を参照）。

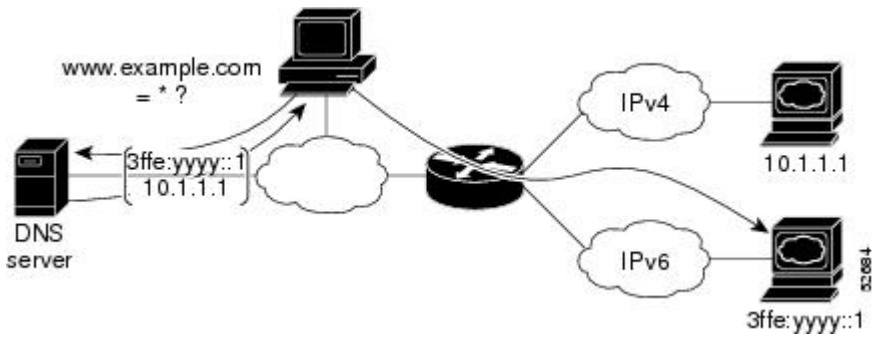
図 *6*：デュアル *IPv4* および *IPv6* プロトコル スタック手法



1 つのアプリケーション プログラム インターフェイス（API）で、IPv4 アドレスと IPv6 アドレスの両方および DNS 要求がサポートされます。 アプリケーションを新しい API にアップグレードしても、依然として IPv4 プロトコル スタックだけを使用できます。 シスコ ソフトウェアでは、デュアル IPv4 および IPv6 プロトコル スタック手法がサポートされます。 IPv4 アドレスと IPv6 アドレスの両方でインターフェイスが設定されている場合、インターフェイスは IPv4 と IPv6 両方のトラフィックを転送します。

次の図では、デュアル IPv4 および IPv6 プロトコル スタックをサポートするアプリケーションは、宛先ホスト名 www.example.com で使用可能なすべてのアドレスを DNS サーバに要求します。 DNS サーバは、www.example.com で使用可能なすべてのアドレス（IPv4 アドレスと IPv6 アドレスの両方）で返信します。 アプリケーションはアドレスを選択し（ほとんどの場合、IPv6 アドレスがデフォルトの選択肢です）、IPv6 プロトコル スタックを使用して送信元ノードを宛先に接続します。

図 *7*：デュアル *IPv4* および *IPv6* プロトコル スタック アプリケーション



IPv6 アドレッシングと基本接続の設定方法

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

IPv6アドレスを個々のデバイスインターフェイスに割り当て、IPv6 トラフィックの転送をデバイス上でグローバルにイネーブルにするには、次の作業を実行します。デフォルトでは、IPv6アドレスは設定されず、IPv6 ルーティングはディセーブルになります。

（注） 1 つのインターフェイス上で複数の IPv6 リンクローカル アドレスはサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. 次のいずれかを実行します。
   - **ipv6 address** *ipv6-prefix /prefix-length* **eui-64**
   -
   - **ipv6 address** *ipv6-address* / *prefix-length* **link-local**
   -
   -
   - **ipv6 enable**
5. **exit**
6. **ipv6 unicast-routing**

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 モードをイネーブルにします。 • 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： `Device# 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	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	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。

ステップ 4	次のいずれかを実行します。
	
	• **ipv6 address** *ipv6-prefix /prefix-length* **eui-64**
	•
	• **ipv6 address** *ipv6-address / prefix-length* **link-local**
	•
	•
	• **ipv6 enable**
	
	例：
	
	`Device(config-if)# ipv6 address 2001:DB8:0:1::/64 eui-64`
	
	例：
	
	例：
	
	`Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`
	
	例：
	
	例：
	
	例：
	
	`Device(config-if)# ipv6 enable`
		インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
		
		または
		
		インターフェイスに割り当てられている IPv6 アドレスを指定し、そのインターフェイスで IPv6 処理をイネーブルにします。
		
		または
		
		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、インターフェイスで IPv6 処理も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の通信にだけ使用できます。
		
		• **ipv6 address eui-64** コマンドを指定して、IPv6 アドレスの下位 64 ビットにインターフェイス識別子（ID）を持つグローバル IPv6 アドレスを設定します。 指定する必要があるのはアドレスの 64 ビット ネットワーク プレフィックスだけです。最後の 64 ビットはインターフェイス ID から自動的に計算されます。
		
		• **ipv6 address link-local** コマンドを指定して、IPv6 がインターフェイスでイネーブルになっている場合に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されるリンクローカル アドレスを、インターフェイスに設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-if)# 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、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

IPv6 アドレスへのホスト名のマッピング

hostname-to-address マッピング

ネーム サーバを使用して、ドメイン名に関連付けられている情報を追跡します。 ネーム サーバでは、ホスト名からアドレスへのマッピングのデータベースを維持できます。 各名前は、1 つ以上の IPv4 アドレス、IPv6 アドレス、または両方のアドレス タイプにマッピングできます。 このサービスを使用してドメイン名を IPv6 アドレスにマッピングするには、ネーム サーバを指定し、DNS をイネーブルにする必要があります。DNS は、ネットワーク デバイスを一意に識別するインターネットのグローバルな命名体系です。

シスコ ソフトウェアは、**connect**、**telnet**、ping の各コマンド、関連する Telnet サポート操作、およびコマンド出力を生成する他の多くのコマンドで使用するために、ホスト名からアドレスへのマッピングのキャッシュを維持します。 このキャッシュによって、名前からアドレスへの変換が高速になります。

IPv4 と同様に、IPv6 で使用されるネーミング方式では、ドメインに対して提供する階層名前空間内の場所によってネットワーク デバイスを識別できます。 ドメイン名は、ピリオド（.）を区切り文字として結合されます。 たとえば、シスコは *com* ドメイン名で識別される商業組織であるため、ドメイン名は *cisco.com* です。 このドメイン内の特定のデバイス、たとえば FTP サーバは、*ftp.cisco.com* として識別されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]
4. 次のいずれかを実行します。
   - **ip domain name** [**vrf** *vrf-name*] *name*
   -
   -
   - **ip domain lis**t [**vrf** *vrf-name*] *name*
5. **ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]
6. **ip domain-lookup**

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 モードをイネーブルにします。 • 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： `Device# 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 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*] 例： `Device(config)# ipv6 host cisco-sj 2001:DB8:20:1::12`	ホスト名からアドレスへのスタティック マッピングをホスト名キャッシュに定義します。 • 通常は、数字のアドレスではなくシンボリック名でネットワーク デバイスを参照する方が簡単です（Telnet などのサービスでは、ホスト名またはアドレスを使用できます）。ホスト名と IPv6 アドレスは、静的または動的な手段で相互に関連付けることができます。 • ダイナミック マッピングが使用可能でない場合は、ホスト名をアドレスに手動で割り当てると便利です。
ステップ 4	次のいずれかを実行します。 • **ip domain name** [**vrf** *vrf-name*] *name*	（任意）非修飾ホスト名を完成させるためにシスコ ソフトウェアで使用されるデフォルトのドメイン名を定義します。 または

	コマンドまたはアクション	目的

	•
	•
	• **ip domain list** [**vrf** *vrf-name*] *name*
	
	例：
	`Device(config)# ip domain-name cisco.com`
	
	例：
	
	例：
	`Device(config)# ip domain list cisco1.com`
		（任意）非修飾ホスト名を完成させるためのデフォルト ドメイン名のリストを定義します。
		• ドメイン名要求を完成させるためにシスコ ソフトウェアで使用されるデフォルトのドメイン名を指定できます。単一のドメイン名またはドメイン名のリストを指定できます。完全なドメイン名を含まないホスト名では、名前が検索される前に、指定したデフォルト ドメイン名が付加されます。
		（注） **ip domain name** コマンドと **ip domain list** コマンドは、IPv4 と IPv6 の両方で使用できるデフォルト ドメイン名の指定に使用されます。

ステップ 5	**ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*] 例： `Device(config)# ip name-server 2001:DB8::250:8bff:fee8:f800 2001:DB8:0:f004::1`	名前情報を提供する 1 つ以上のホストを指定します。 • DNS に名前情報を提供するネーム サーバとして機能できる 1 つ以上（6 つまで）のホストを指定します。 （注） *server-address* 引数には、IPv4 アドレスまたは IPv6 アドレスを指定できます。
ステップ 6	**ip domain-lookup** 例： `Device(config)# ip domain-lookup`	DNS ベースのアドレス変換をイネーブルにします。 • DNS はデフォルトでイネーブルになっています。

IPv6 リダイレクト メッセージの表示

手順の概要

1. **enable**
2. **show ipv6 interface** [**brief**] [*type number*] [**prefix**]
3. **show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics**
4. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
5. **show ipv6 traffic**
6. **show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**]
7. **enable**
8. **show running-config**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ipv6 interface** [**brief**] [*type number*] [**prefix**] 例： `Device# show ipv6 interface gigabitethernet 0/0/0`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。
ステップ 3	**show ipv6 neighbors** [*interface-type interface-number*	*ipv6-address*	*ipv6-hostname*] **statistics** 例： `Device# show ipv6 neighbors gigabitethernet 2/0/0`	IPv6 ネイバー探索キャッシュ情報を表示します。
ステップ 4	**show ipv6 route** [*ipv6-address*	*ipv6-prefix*/*prefix-length*	*protocol*	*interface-type interface-number*] 例： `Device# show ipv6 route`	（任意）IPv6 ルーティング テーブルの現在の内容を表示します。

	コマンドまたはアクション	目的
ステップ 5	**show ipv6 traffic** 例： `Device# show ipv6 traffic`	（任意）IPv6 トラフィックの統計情報を表示します。
ステップ 6	**show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**] 例： `Device# show hosts`	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
ステップ 7	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 8	**show running-config** 例： `Device# show running-config`	デバイスで実行されている現在の設定を表示します。

IPv6 アドレッシングと基本接続の設定例

例：IPv6 アドレッシングと IPv6 ルーティングの設定

次の例では、IPv6 は、デバイス上で IPv6 プレフィックス 2001:DB8:c18:1::/64 に基づくリンクローカル アドレスとグローバル アドレスの両方でイネーブルになっています。 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** コマンドからの出力は、インターフェイス ID（260:3EFF:FE47:1530）がギガビットイーサネットインターフェイス 0/0/0 のリンクローカル プレフィックス FE80::/64 にどのように追加されるかを示します。

```
ipv6 unicast-routing
interface gigabitethernet 0/0/0
  ipv6 address 2001:DB8:c18:1::/64 eui-64
Device# show ipv6 interface gigabitethernet 0/0/0
Gigabitethernet0/0/0 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
  Global unicast address(es):
    2001:DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:DB8:C18:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
```

```
    FF02::1:FF47:1530
    FF02::9
  MTU is 1500 bytes
  ICMP error messages limited to one every 500 milliseconds
  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.
```

例：デュアル プロトコル スタックの設定

次の例では、デバイスでIPv6ユニキャストデータグラムの転送をグローバルにイネーブルにし、IPv4 アドレスと IPv6 アドレスの両方でギガビット イーサネット インターフェイス 0/0/0 を設定します。

```
ipv6 unicast-routing
interface gigabitethernet0/0/0
  ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:DB8:c18:1::3/64
```

例：ホスト名からアドレスへのマッピングの設定

次の例では、ホスト名キャッシュに2つの静的なホスト名からアドレスへのマッピングを定義し、未修飾のホスト名を完成させるための複数の代替ドメイン名でドメイン リストを設定します。また、ホスト 2001:DB8::250:8bff:fee8:f800 とホスト 2001:DB8:0:f004::1 をネーム サーバとして指定し、DNS サービスを再びイネーブルにします。

```
ipv6 host cisco-sj 2001:DB8:700:20:1::12
ipv6 host cisco-hq 2001:DB8:768::1 2001:DB8:20:1::22
ip domain list domain1-list.com
ip domain list serviceprovider2-name.com
ip domain list college2-name.edu
ip name-server 2001:DB8::250:8bff:fee8:f800 2001:DB8:0:f004::1
ip domain-lookup
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 サービスの設定	『*IP Application Services Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 アドレッシングと基本接続の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *5*：*IPv6* アドレッシングと基本接続の機能情報

機能名	リリース	機能情報
Internet Protocol Version 6（IPv6）	12.0(22)S 12.2(2)T 12.2(14)S 12.2(17a)SX1 12.2(25)SEA 12.2(28)SB 12.2(33)SRA Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	IPv6 は、ネットワーク アドレス ビット数を 32 ビットから 128 ビットに拡張しているため、地球上のすべてのネットワーク デバイスにグローバルに一意な IP アドレスを十分に提供できます。 Cisco IOS XE Release 3.9S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。 コマンド **ip address**、**ip domain list**、**ip domain-lookup ip domain name**、**ip name-server**、**ipv6 address**、**ipv6 address anycast**、**ipv6 address eui-64**、**ipv6 address link-local**、**ipv6 enable**、**ipv6 host**、**ipv6 unicast-routing** が追加または変更されました。

機能名	リリース	機能情報
IPv6 データ リンク：Cisco スイッチ間リンクを使用した VLAN	12.2(2)T 12.2(18)SXE 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.0(2)SG 3.2.0SG	IPv6 は、この機能をサポートします。 追加または変更されたコマンドはありません。
IPv6 データ リンク：IEEE 802.1Q カプセル化を使用した VLAN	12.2(2)T 12.2(18)SXE 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.0(2)SG 3.2.0SG Cisco IOS XE Release 3.9S	IPv6 は、この機能をサポートします。 追加または変更されたコマンドはありません。 Cisco IOS XE Release 3.9S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。
IPv6 サービス：Cisco Discovery Protocol：ネイバー情報の IPv6 アドレス ファミリ サポート	12.2(8)T 12.2(14)S 12.2(18)SXE 12.2(25)SEE 12.2(25)SG 12.2(33)SRA Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	ネイバー情報の Cisco Discovery Protocol IPv6 アドレス サポート機能により、2 台のシスコ デバイス間で IPv6 アドレッシング情報を転送する機能が追加されます。 Cisco IOS XE Release 3.8S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。 追加または変更されたコマンドはありません。

第 2 章

IPv6 エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。 エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 エニーキャスト アドレスについて

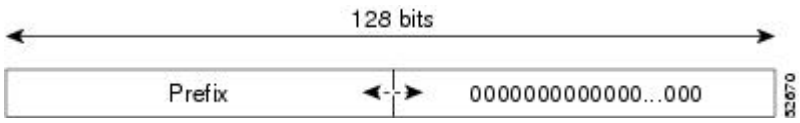
IPv6 アドレス タイプ：エニーキャスト

エニーキャストアドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。 エニーキャスト アドレスに送信されたパケットは、使用しているルーティング プロトコルの定義に従って、そのエニーキャストアドレスが示す最も近いインターフェイスに送信されます。 エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。 ユニキャスト アドレスを複数のインターフェイスに割り当てると、ユニキャストアドレスがエニーキャストアドレスになります。エニーキャストアドレスを割り当てるノードは、アドレスがエニーキャストアドレスであることを認識するように明示的に設定する必要があります。

（注） エニーキャスト アドレスを使用できるのはデバイスだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。

次の図に、サブネット デバイス エニーキャスト アドレスの形式を示します。アドレスには、連続するゼロで連結されたプレフィックス（インターフェイス ID）があります。 サブネット デバイス エニーキャスト アドレスを使用すると、サブネット デバイス エニーキャスト アドレスのプレフィックスが示すリンク上のデバイスに到達できます。

図 *8*：サブネット デバイス エニーキャスト アドレスの形式



IPv6 エニーキャスト アドレスの設定方法

IPv6 エニーキャスト アドレスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel mode ipv6ip** [**6rd** | **6to4** | **auto-tunnel** | **isatap**]
5. **tunnel source** { *ip address* | *ipv6-address* | *interface-type interface-number* }
6. **ipv6 address** { *ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length* }
7. **ipv6 address** *ipv6-prefix/prefix-length* **anycast**

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 モードをイネーブルにします。 • 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： `Device# 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** *type number* 例： `Device(config)# interface tunnel0`	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。
ステップ 4	**tunnel mode ipv6ip** [**6rd** | **6to4** | **auto-tunnel** | **isatap**] 例： `Device(config-if)# tunnel mode ipv6ip 6to4`	スタティック IPv6 トンネル インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**tunnel source** { *ip address* | *ipv6-address* | *interface-type interface-number* } 例： `Device(config-if)# tunnel source GigabitEthernet1`	トンネル インターフェイスの送信元アドレスを設定します。 ここで使用されるアドレスは、イーサネット インターフェイス 1 に割り当てられているアドレスです。
ステップ 6	**ipv6 address** { *ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length* } 例： `Device(config-if)# ipv6 address 2001:db8:A00:1::1/64`	IPv6 アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ 7	**ipv6 address** *ipv6-prefix/prefix-length* **anycast** 例： `Device(config-if)# ipv6 address 2002:db8:c058::/128 anycast`	**ipv6 address anycast** コマンドを指定して、IPv6 エニーキャスト アドレスを追加します。

IPv6 エニーキャスト アドレスの設定例

例：IPv6 エニーキャスト アドレスの設定

```
interface tunnel0
  tunnel mode ipv6ip 6to4
  tunnel source ethernet1
  ipv6 address 2001:0db8:1::1/64
  ipv6 address 2002:0db8:6301::/128 anycast
 !
 interface gigabitethernet1
  ip address 10.0.0.1 255.255.255.0
  ip address 192.88.99.1 255.255.255.0 secondary
```

IPv6 のソース ガードおよびプレフィックス ガードのその他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 アドレス指定	『*IP Addressing: IPv4 Addressing Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 エニーキャスト アドレスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *6*：*IPv6* エニーキャスト アドレスの機能情報

機能名	リリース	機能情報
IPv6：エニーキャスト アドレス	12.2(25)SEA 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(4)T 15.0(2)SG Cisco IOS XE Release 2.1 3.2.0SG	エニーキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。 エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。 **ipv6 address anycast**、**show ipv6 interface** の各コマンドが追加または変更されています。

第 3 章

IPv6 スイッチング：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サポート

シスコ エクスプレス フォワーディング機能は、IPv6 パケットを転送するためのレイヤ 3 IP スイッチング テクノロジーです。 分散型シスコ エクスプレス フォワーディングは、シスコ エクスプレス フォワーディングと同じ機能を実行しますが、分散アーキテクチャ プラットフォーム用です。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6スイッチングの前提条件：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サポート

- シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングを使用して IPv6 トラフィックを転送するには、デバイス上で IPv6 ユニキャスト データグラムの転送をグローバルに設定するか、インターフェイスにIPv6アドレスを設定する必要があります。
- デバイス上で IPv6 のシスコ エクスプレス フォワーディングをグローバルにイネーブルにする前に、デバイス上で IPv4 のシスコ エクスプレス フォワーディングをグローバルにイネーブルに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両方をサポートする分散アーキテクチャ プラットフォームでは、デバイス上で IPv6 の分散型シスコ エクスプレス フォワーディングをグローバルにイネーブルにする前に、デバイス上で IPv4 の分散型シスコ エクスプレス フォワーディングをグローバルにイネーブルにする必要があります。
- 非分散型プラットフォームでは、分散型シスコ エクスプレス フォワーディングはサポートされませんが、一部の分散型プラットフォームでは、シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングの両方がサポートされます。
- ユニキャスト リバース パス転送（uRPF）を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。 シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。 シスコ エクスプレス フォワーディングがデバイス上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングに設定されている非分散および分散アーキテクチャ プラットフォームに次の制約が適用されます。

- グローバルな送信元および宛先アドレスを持つ IPv6 パケットは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングでスイッチングされる。
- リンクローカルの送信元アドレスと宛先アドレスを持つIPv6パケットは、プロセスでスイッチングされる。

- 手動で設定した IPv6 トンネル内でトンネリングされる IPv6 パケットは、シスコ エクスプレス フォワーディングでスイッチングされる。

IPv6 スイッチングについて：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サポート

IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチング

シスコ エクスプレス フォワーディングは、IPv6 パケットを転送するための高度なレイヤ 3 IP スイッチング テクノロジーです。 分散型シスコ エクスプレス フォワーディングは、シスコ エクスプレスフォワーディングと同じ機能を実行しますが、分散アーキテクチャプラットフォーム用です。 IPv6 の分散型シスコ エクスプレス フォワーディングおよび IPv6 のシスコ エクスプレス フォワーディングは、IPv4 の分散型シスコ エクスプレス フォワーディングおよび IPv4 のシスコ エクスプレスフォワーディングと同じ機能と利点を提供します。使用しているルーティングプロトコルの指示に従って追加、削除、または変更された IPv6 ルーティング情報ベース（RIB）のネットワーク エントリが転送情報ベース（FIB）に反映され、IPv6 隣接関係テーブルによって各 FIB のすべてのエントリのレイヤ 2 ネクストホップ アドレスが管理されます。

各 IPv6 ルータ インターフェイスには、1 つの IPv6 グローバル FIB と 1 つの IPv6 リンクローカル FIB への関連付けがあります（複数のインターフェイスが同じ FIB への関連付けを持つことができます）。 同じ IPv6 リンクに接続されているすべての IPv6 ルータ インターフェイスが、同じ IPv6 リンクローカル FIB を共有します。 IPv6 グローバル宛先アドレスを持つ IPv6 パケットは、IPv6 グローバル FIB で処理されます。ただし、IPv6 グローバル宛先アドレスおよび IPv6 リンクローカル送信元アドレスを持つパケットは、プロセス スイッチングおよびスコープエラー処理のために RP に送信されます。 リンクローカル送信元アドレスを持つパケットはローカルリンクから転送されません。また、プロセス スイッチングおよびスコープエラー処理のために RP に送信されます。

IPv6スイッチングの設定方法：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サポート

分散型および非分散型アーキテクチャ プラットフォームでのシスコ エクスプレス フォワーディング スイッチングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **ipv6 cef**
   - **ipv6 cef distributed**
4. **ipv6 cef accounting** [**non-recursive** | **per-prefix** | **prefix-length**]

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 モードをイネーブルにします。 • 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： `Device# 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	次のいずれかを実行します。 • **ipv6 cef** • **ipv6 cef distributed**	デバイスでシスコ エクスプレス フォワーディングをグローバルにイネーブルにします。 または デバイスで分散型シスコ エクスプレス フォワーディングをグローバルにイネーブルにします。

	コマンドまたはアクション	目的

	例：
	`Device(config)# ipv6 cef`
	
	例：
	`Device(config)# ipv6 cef distributed`	

ステップ 4	**ipv6 cef accounting** [**non-recursive** | **per-prefix** | **prefix-length**] 例： `Device(config)# ipv6 cef accounting`	デバイスで、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ネットワーク アカウンティングをグローバルにイネーブルにします。 • 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ネットワーク アカウンティングにより、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トラフィックに固有の統計情報を収集することで、ネットワーク内のシスコ エクスプレス フォワーディング トラフィック パターンをよりよく理解できます。 たとえば、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ネットワーク アカウンティングにより、宛先にスイッチングされたパケット数とバイト数や、宛先を経由してスイッチングされたパケット数などの情報を収集できます。 • オプションの **per-prefix** キーワードでは、IPv6 宛先（または IPv6 プレフィックス）にエクスプレス フォワーディングされたパケット数とバイト数の収集をイネーブルにします。 • オプションの **prefix-length** キーワードでは、IPv6 プレフィックス長にエクスプレス フォワーディングされたパケット数とバイト数の収集をイネーブルにします。 （注） シスコ エクスプレス フォワーディングがデバイスでグローバルにイネーブルになっている場合、アカウンティング情報は RP で収集されます。分散型シスコ エクスプレス フォワーディングがデバイスでグローバルにイネーブルになっている場合、アカウンティング情報はラインカードで収集されます。

IPv6 スイッチングの設定例：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サポート

例：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

次の例では、IPv6 のシスコ エクスプレス フォワーディングおよび IPv6 のシスコ エクスプレス フォワーディングのネットワーク アカウンティングの両方が非分散型アーキテクチャデバイスでグローバルにイネーブルになっていて、IPv6 のシスコエクスプレスフォワーディングがギガビットイーサネットインターフェイス 0/0/0 でイネーブルになっています。 例では、**ipv6 unicast-routing** コマンドを使用して IPv6 ユニキャストデータグラムの転送がデバイス上でグローバルに設定されていること、**ipv6 address** コマンドを使用して IPv6 アドレスがギガビット イーサネット インターフェイス 0/0/0 に設定されていること、および **ip cef** コマンドを使用して IPv4 のシスコ エクスプレス フォワーディングがデバイスでグローバルに設定されていることも示されています。

```
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
interface gigabitethernet0/0/0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:DB8:C18:1::/64 eui-64
```

次の例では、IPv6 の分散型シスコ エクスプレス フォワーディングおよび IPv6 の分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングの両方が分散型アーキテクチャデバイスでグローバルにイネーブルになっています。 **ipv6 unicast-routing** コマンドで IPv6 ユニキャスト データグラムの転送がデバイスでグローバルに設定され、**ip cef distributed** コマンドで IPv4 の分散型シスコ エクスプレス フォワーディングがデバイスでグローバルに設定されています。

```
ip cef distributed
ipv6 unicast-routing
ipv6 cef distributed
ipv6 cef accounting prefix-length
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』

関連項目	参照先
IPv4 スイッチングの設定	『*IP Switching Cisco Express Forwarding Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6スイッチングの機能情報：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サポート

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 7：*IPv6* スイッチングの機能情報：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サポート

機能名	リリース	機能情報
IPv6 スイッチング：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サポート	12.2(13)T 12.2(17a)SX1 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.0(2)SG 15.3(1)S Cisco IOS XE Release 2.1 3.2.0SG	Cisco Express Forwarding for IPv6 は、IPv6 パケットを転送するための高度なレイヤ 3 IP スイッチング テクノロジーです。 IPv6 の分散型シスコ エクスプレス フォワーディングは、IPv6 のシスコ エクスプレス フォワーディングと同じ機能を実行しますが、分散アーキテクチャ プラットフォーム用です。 **ipv6 cef**、**ipv6 cef accounting**、**ipv6 cef distributed** の各コマンドが追加または変更されています。

IPv6 スイッチングの機能情報：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サポート

第 4 章

IPv6 のユニキャスト リバース パス転送

IPv6 のユニキャスト リバース パス転送機能により、IPv6 デバイスを経由する不正形式または偽造（スプーフィング）IPv6 送信元アドレスを原因とする問題が軽減されます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 のユニキャスト リバース パス転送の前提条件

- ユニキャスト リバース パス転送（uRPF）を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッ

チングをイネーブルにします。 シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。 シスコ エクスプレス フォワーディングがデバイス上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

- uRPF が機能するためには、デバイスでシスコ エクスプレス フォワーディングがグローバルに設定されている必要があります。 uRPF は、シスコ エクスプレス フォワーディングがないと動作しません。
- uRPF は、ネットワーク内部のインターフェイスでは使用できません。 内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。 uRPF は、元々対称であるか、対称に設定されている場合にだけ適用してください。

  たとえば、ISP のネットワークのエッジにあるデバイスは、ISP ネットワークのコアにあるデバイスよりも対称リバース パスを持つ可能性が高くなります。 ISP ネットワークのコアにあるデバイスでは、デバイスからの最良の転送パスがデバイスへ返されるパケットに対して選択されるパスとなることが保証されません。 したがって、非対称ルーティングの可能性がある uRPF の適用は推奨されません。 ネットワークのエッジにだけ、または ISP の場合はネットワークのカスタマー エッジにだけ uRPF を配置します。

IPv6 のユニキャスト リバース パス転送について

ユニキャスト リバース パス転送

IPv6 のユニキャスト リバース パス転送機能を使用すると、IPv6 デバイスを経由する不正形式またはスプーフィング IPv6 送信元アドレスを原因とする問題が軽減されます。 不正形式または偽造送信元アドレスは、送信元 IPv6 アドレス スプーフィングに基づくサービス拒絶（DoS）攻撃を示すことがあります。

インターフェイスで uRPF がイネーブルになっている場合、デバイスはそのインターフェイスで受信したすべてのパケットを調べます。デバイスは、送信元アドレスがルーティング テーブルにあり、パケットが受信されるインターフェイスと一致するか確認します。 この「後方参照」機能を使用できるのは、シスコエクスプレス フォワーディングがデバイスでイネーブルにされている場合のみです。これは、ルックアップが転送情報ベース（FIB）の存在に依存しているためです。シスコ エクスプレス フォワーディングでは、その動作の一部として FIB が生成されます。

（注） uRPF は入力機能であり、接続のアップストリーム エンドのデバイスの入力インターフェイスだけに適用されます。

uRPF 機能では、デバイス インターフェイスで受信されたパケットが、パケットの送信元への最良リターン パスの 1 つで着信するかどうかが検証されます。 この機能では、シスコ エクスプレス フォワーディング テーブルのリバース ルックアップが実行されます。 uRPF がパケットのリバース パスを見つけることができない場合、uRPF は、アクセス コントロール リスト（ACL）が

指定されているかどうかに応じてパケットをドロップまたは転送できます。ACLが指定されている場合は、パケットが uRPF チェックに失敗した場合にだけ、パケットが（ACL の deny ステートメントを使用して）ドロップされる必要があるか、（ACL の permit ステートメントを使用して）転送される必要があるかを確認するために ACL がチェックされます。 パケットがドロップされるか転送されるかにかかわらず、パケットは、uRPF ドロップのグローバル IP トラフィック統計情報と uRPF のインターフェイス統計情報でカウントされます。

ACL が指定されていない場合、デバイスは偽造または不正形式のパケットを即時にドロップし、ACL ロギングは行われません。 デバイスおよびインターフェイス uRPF カウンタが更新されます。

uRPF イベントは、ACL エントリのロギング オプションを指定することでロギングできます。 ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

（注） uRPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。 複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ数や加重など）が他のパスと等しく、そのルートが FIB 内にあるかぎり、uRPF は機能します。

IPv6 のユニキャスト リバース パス転送の設定方法

ユニキャスト RPF の設定

はじめる前に

uRPF を使用するには、デバイスでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。 シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。 シスコ エクスプレス フォワーディングがデバイス上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

（注） デバイスでシスコ エクスプレス フォワーディングがグローバルに設定されている必要があります。 uRPF は、シスコ エクスプレス フォワーディングがないと動作しません。

（注） uRPF は、ネットワーク内部のインターフェイスでは使用できません。 内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。 uRPF は、元々対称であるか、対称に設定されている場合にだけ適用してください。

たとえば、ISP のネットワークのエッジにあるデバイスは、ISP ネットワークのコアにあるデバイスよりも対称リバース パスを持つ可能性が高くなります。 ISP ネットワークのコアにあるデバイスでは、デバイスからの最良の転送パスがデバイスへ返されるパケットに対して選択されるパスとなることが保証されません。 したがって、非対称ルーティングの可能性がある uRPF の適用は推奨されません。 ネットワークのエッジにだけ、または ISP の場合はネットワークのカスタマー エッジにだけユニキャスト uRPF を配置するのが最も単純です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Device# 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** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	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。
ステップ 4	**ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-name*	送信元アドレスが FIB テーブルに存在していることを確認し、uRPF をイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device(config-if)# ipv6 verify unicast source reachable-via any`	

IPv6 のユニキャスト リバース パス転送の設定例

例：IPv6 のユニキャスト リバース パス転送の設定

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 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
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 スイッチングの設定	『*IP Switching Cisco Express Forwarding Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』

関連項目	参照先
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 のユニキャスト リバース パス転送の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *8*：*IPv6* のユニキャスト リバース パス転送の機能情報

機能名	リリース	機能情報
IPv6 のユニキャスト リバース パス転送	12.2(50)SY Cisco IOS XE Release 2.1	uRPF 機能を使用すると、IPv6 デバイスを経由する不正形式またはスプーフィング IPv6 送信元アドレスを原因とする問題が軽減されます。 不正な形式の送信元アドレスまたは偽装された送信元アドレスは、送信元 IPv6 アドレスのスプーフィングに基づく DoS 攻撃である場合があります。 **ipv6 verify unicast source reachable-via**、**show ipv6 traffic** の各コマンドが追加または変更されています。

第 5 章

IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップ

IPv6 基本接続は、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスで AAAA レコード タイプのサポートを設定することで拡張できます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップについて

DNS for IPv6

IPv6では、DNSの名前からアドレスおよびアドレスから名前のルックアッププロセスでサポートされるDNSレコードタイプがサポートされます。 DNSレコードタイプでは、IPv6アドレスがサポートされます。 IPv6では、IPv6アドレスからDNS名への逆マッピングもサポートされます。

次の表に、IPv6 DNS レコード タイプをリストします。

表 *9*：*IPv6 DNS* レコード タイプ

レコード タイプ	説明	フォーマット
AAAA	ホスト名を IPv6 アドレスにマッピングします （IPv4 の A レコードと同等）。	www.abc.test AAAA 3FFE:YYYY:C18:1::2
PTR	IPv6アドレスをホスト名にマッピングします （IPv4 の PTR レコードと同等）。 （注） シスコ ソフトウェアでは、IP6.INT ドメインの PTR レコードの解決がサポートされます。	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 サービスの設定	『*IP Application Services Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *10*：*IPv6* サービス：*IPv4* トランスポートでの *AAAA DNS* ルックアップの機能情報

機能名	リリース	機能情報
IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップ	12.2(2)T 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 15.0(2)SG 15.3(1)S Cisco IOS XE Release 2.1 3.2.0SG	IPv6 基本接続は、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスで AAAA レコード タイプのサポートを設定することで拡張できます。 追加または変更されたコマンドはありません。
IPv6 サービス：IPv6 トランスポートでの DNS ルックアップ	12.2(8)T 12.2(25)SED 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 15.0(2)SG 15.3(1)S Cisco IOS XE Release 2.1 3.2.0SG	IPv6は、この機能をサポートします。 追加または変更されたコマンドはありません。 Cisco IOS XE Release 3.8S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。

第 6 章

IPv6 MTU パス ディスカバリ

IPv6 MTU パス 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最大伝送単位（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。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェアリリースに対応した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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 MTU パス ディスカバリについて

IPv6 MTU パス ディスカバリ

IPv4 の場合と同様に、IPv6 のパス MTU ディスカバリを使用すると、特定のデータ パス上のすべてのリンクの MTU サイズの差をホストが動的に検出し、調整できます。 ただし、IPv6 では、特定のデータ パス上の 1 つのリンクのパス MTU がパケットのサイズに十分に対応できる大きさでない場合に、フラグメンテーションはパケットの送信元によって処理されます。 IPv6 ホストでパケット フラグメンテーションを処理すると、IPv6 デバイスの処理リソースが節約され、IPv6 ネットワークの効率が向上します。

（注） IPv6 では、最小リンク MTU は 1280 オクテットです。 IPv6 リンクには、1500 オクテットの MTU 値の使用をお勧めします。

IPv6 パス MTU ディスカバリによって、IPv6 トラフィックの発信デバイスに ICMPv6「toobig」メッセージで受信した MTU 値を含む MTU が割り当てられます。 攻撃者が MTU のキャッシュを満たさないようにするため、デバイスは発信（送信）されたトラフィックの宛先を追跡し続け、追跡対象の宛先のいずれかと一致する内部宛先を持つ toobig ICMPv6 メッセージのみを受け入れます。

悪意のあるデバイスがトラフィックを発信するデバイスの宛先を学習することができる場合、攻撃者がこの宛先のパスに存在しなくても、この宛先の toobig ICMPv6 メッセージをデバイスに送信でき、強制的に MTU キャッシュに侵入できます。その後、デバイスはこの宛先へのトラフィックのフラグメンテーションを開始します。これは、デバイスのパフォーマンスに多大な影響を与えます。

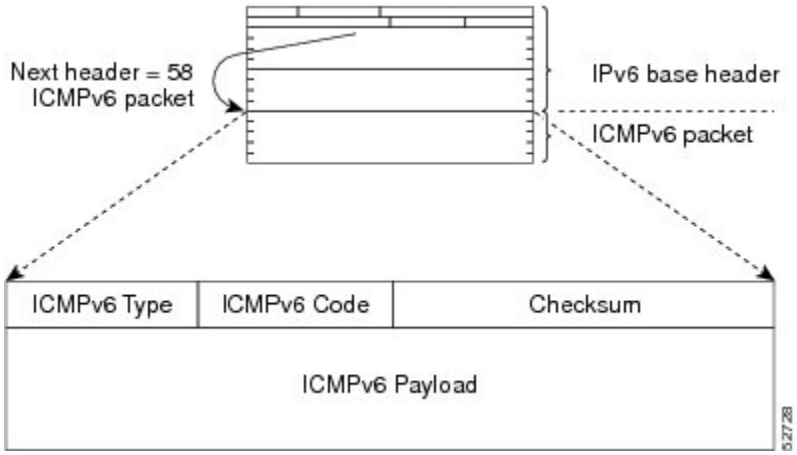
ローカルに生成されたトラフィックのフローラベルのマーキングをイネーブルにすると、この攻撃を軽減できます。発信されたパケットはフローラベルでマークされ（ランダムに生成され、毎分変更され）、受信した toobig メッセージが送信された値に対してチェックされます。 攻撃者がトラフィックをスヌープできない場合、攻撃者は使用するフローテーブルがわからず、toobig メッセージがドロップされます。

ICMP for IPv6

IPv6 のインターネット制御メッセージプロトコル（ICMP）の機能は、IPv4 の ICMP と同じです。 ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。 また、ICMP for IPv6 パケットは、IPv6 ネイバー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD）プロトコル for IPv6 で使用されます。 MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 デバイスで使用されます。 MLD は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。 ICMP for IPv6 パケットは、すべての拡張ヘッダーに続いて IPv6 パケットの末尾に配置される点でトランスポートレイヤ パケットに似ています。 IPv6 ICMP パケット内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサム フィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから抽出されます。 ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。 次の図に、IPv6 ICMP パケット ヘッダー形式を示します。

図 *9*：*IPv6 ICMP* パケット ヘッダーの形式



IPv6 MTU パス ディスカバリの設定方法

デバイスから送信されるパケットのフローラベルマーキングのイネーブル化

この機能を使用すると、デバイスは1280バイト以上のパケットを送信したデバイスの宛先を追跡できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 flowset**
4. **exit**
5. **clear ipv6 mtu**

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 モードをイネーブルにします。 • 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： `Device# 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 flowset** 例： `Device(config)# ipv6 flowset`	デバイスから送信された 1280 バイト以上のパケットにフローラベル マーキングを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了して、デバイスを特権 EXEC モードにします。
ステップ 5	**clear ipv6 mtu** 例： `Device# clear ipv6 mtu`	メッセージの MTU キャッシュをクリアします。

IPv6 MTU パス ディスカバリの設定例

例：IPv6 インターフェイス統計情報の表示

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスが FastEthernet インターフェイス 1/0 に対して正しく設定されていることを確認します。 IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、ステートレス自動設定、および MTU サイズのステータスに関する情報も表示されることがあります。

```
Device# show ipv6 interface fastethernet 1/0

Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/64
```

```
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
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.
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 MTU パス ディスカバリの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *11*：*IPv6 MTU* パス ディスカバリの機能情報

機能名	リリース	機能情報
IPv6 MTU パス ディスカバリ	12.2(2)T 12.2(17a)SX1 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.0(2)SG Cisco IOS XE Release 2.1 3.2.0SG	IPv6 のパス MTU ディスカバリを使用すると、特定のデータパス上のすべてのリンクの MTU サイズの差をホストが動的に検出し、調整できます。 **clear ipv6 mtu**、**ipv6 flowset** の各コマンドが追加または変更されています。

第 7 章

ICMP for IPv6

ICMP for IPv6 は、IPv4 の ICMP と同じ働きをします。 ICMP for IPv6 は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ICMP for IPv6 について

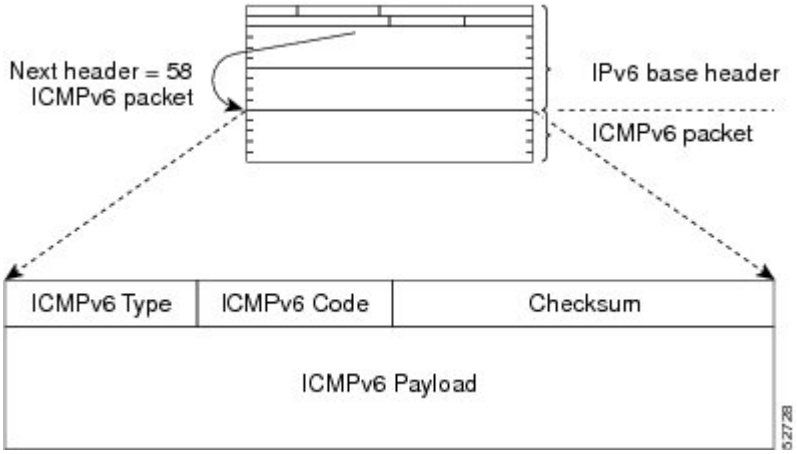
ICMP for IPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）の機能は、IPv4 の ICMP と同じです。ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。 また、ICMP for IPv6 パケットは、IPv6 ネイ

バー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD）プロトコル for IPv6 で使用されます。 MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャストアドレスを宛先としたマルチキャストパケットを受信するために使用するノード）を検出するために IPv6 デバイスで使用されます。 MLD は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。 ICMP for IPv6 パケットは、すべての拡張ヘッダーに続いて IPv6 パケットの末尾に配置される点でトランスポートレイヤ パケットに似ています。 IPv6 ICMP パケット内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサム フィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから抽出されます。 ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。次の図に、IPv6 ICMP パケット ヘッダー形式を示します。

図 *10*：*IPv6 ICMP* パケット ヘッダーの形式

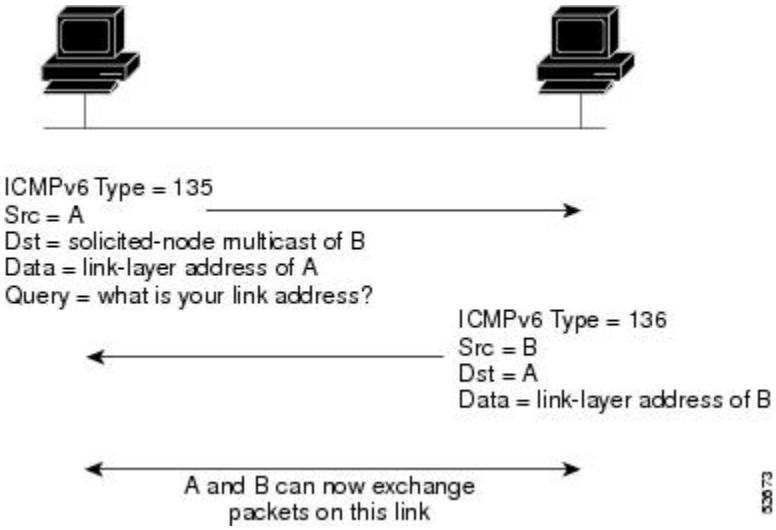


IPv6 ネイバー送信要求メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 135 は、ネイバー送信要求メッセージを示します。ネイバー送信要求メッセージは、ノードが同じローカル リンク上の別のノードのリンク層アドレスを判断する必要がある場合にローカル リンクに送信されます（次の図を参照）。ノードが別のノードのリンク層アドレスを判断する必要がある場合、ネイバー請求メッセージ内の送信元アドレスは、ネイバー請求メッセージを送信するノードの IPv6 アドレスです。ネイバー送信要求メッセージ内の宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノード マルチ

キャストアドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

図 *11*：*IPv6* ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージを受信した後に、宛先ノードは、ICMP パケット ヘッダーのタイプ フィールドに値 136 を含むネイバー アドバタイズメント メッセージをローカル リンクに送信することで応答します。 ネイバー アドバタイズメント メッセージの送信元アドレスは、ネイバー アドバタイズメントメッセージを送信するノードのIPv6アドレス（具体的には、ノードインターフェイスのIPv6アドレス）です。ネイバーアドバタイズメントメッセージ内の宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。 ネイバー アドバタイズメント メッセージのデータ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバー アドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。 あるノードがネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスはネイバーのユニキャスト アドレスです。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。そのような変更があった場合、ネイバーアドバタイズメントの宛先アドレスは全ノード マルチキャスト アドレスになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。 ネイバー到達不能検出では、ネイバーの障害またはネイバーへの転送パスの障害が識別されます。この検出は、ホストとネイバー ノード（ホストまたはデバイス）間のすべてのパスで使用されます。 ネイバー到達不能検出は、ユニキャストパケットだけが送信されるネイバーに対して実行され、マルチキャスト パケットが送信されるネイバーに対しては実行されません。

ネイバーは、（以前にネイバーに送信されたパケットが受信され、処理されたことを示す）肯定確認応答がネイバーから返された場合に、到達可能と見なされます。 到達可能であるという確認は、接続が動作中（宛先に到達中）であることを示す上位層プロトコル（TCP など）からの情報や、ネイバー送信要求メッセージに対するネイバーアドバタイズメントメッセージを受信することで行われます。 パケットがピアに到達している場合、それらのパケットは送信元のネクストホップネイバーにも到達しています。 したがって、転送の進行により、ネクストホップネイバーが到達可能であることも確認されます。

ローカルリンク上にない宛先の場合、転送の進行は、ファーストホップデバイスが到達可能であることを暗に意味します。 上位層プロトコルからの確認応答がない場合、ノードは、ユニキャストネイバー送信要求メッセージを使用してネイバーを探し、転送パスがまだ機能していることを確認します。

ネイバーから返信された請求ネイバーアドバタイズメントメッセージは、転送パスがまだ機能しているという肯定確認応答です（請求フラグが値 1 に設定されたネイバー アドバタイズメントメッセージは、ネイバー請求メッセージへの返信としてだけ送信されます）。 非送信要求メッセージでは、送信元ノードから宛先ノードへの一方向パスだけが確認されます。送信要求ネイバーアドバタイズメント メッセージは、両方向のパスが機能していることを示します。

（注） 送信要求フラグが値 0 に設定されたネイバー アドバタイズメント メッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

ネイバー送信要求メッセージは、ユニキャストIPv6アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。新規のリンクローカルIPv6アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。 具体的には、ノードは未指定の送信元アドレスと一時的なリンクローカル アドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。 そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカルアドレスを含むネイバー アドバタイズメント メッセージを返します。 別のノードが同じアドレスの一意性を同時に検証している場合は、そのノードもネイバー送信要求メッセージを返します。ネイバー送信要求メッセージの返信としてネイバー アドバタイズメント メッセージが受信されず、同じ一時アドレスの検証を試行している他のノードからのネイバー送信要求メッセージも受信されない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンクローカル アドレスを一意であると見なし、そのアドレスをインターフェイスに割り当てます。

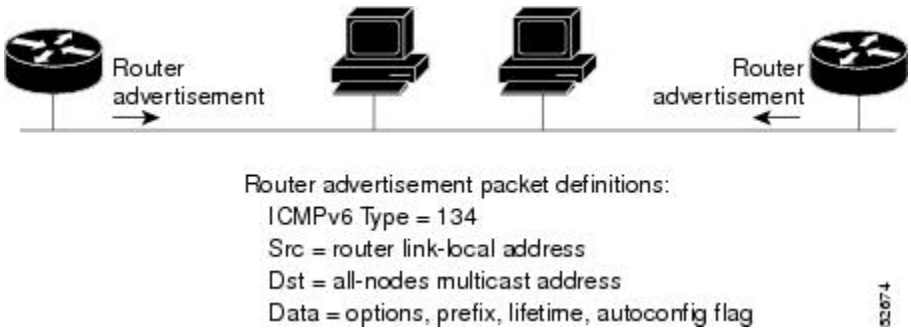
リンク上のすべてのIPv6ユニキャストアドレス（グローバルまたはリンクローカル）が一意であることを検証する必要がありますが、リンクローカル アドレスの一意性が確認されるまでは、リンクローカルアドレスに関連付けられている他のIPv6アドレスに対して重複アドレス検出は実行されません。 シスコ ソフトウェアでの重複アドレス検出のシスコ実装では、64 ビット インターフェイス識別子から生成されるエニーキャストアドレスまたはグローバルアドレスの一意性は確認されません。

IPv6 ルータ アドバタイズメント メッセージ

ルータ アドバタイズメント（RA）メッセージは、ICMP パケット ヘッダーのタイプ フィールドが値 134 であり、IPv6 ルータの設定済みの各インターフェイスへ定期的に送信されます。 ステートレス自動設定が正しく機能するには、RA メッセージでアドバタイズされたプレフィックス長が常に 64 ビットである必要があります。

RA メッセージは、全ノード マルチキャスト アドレスに送信されます（次の図を参照）。

図 *12* : *IPv6* ネイバー探索 -- *RA* メッセージ



通常、RA メッセージには次の情報が含まれます。

- ローカル リンク上のノードがその IPv6 アドレスの自動設定に使用できる 1 つ以上のオンリンク IPv6 プレフィックス
- アドバタイズメントに含まれる各プレフィックスのライフタイム情報
- 完成可能な自動設定のタイプ（ステートレスまたはステートフル）を示すフラグのセット
- デフォルト ルータ情報（アドバタイズメントを送信しているルータをデフォルト ルータとして使用する必要があるかどうか、また使用する必要がある場合はルータをデフォルト ルータとして使用する必要のある秒単位での時間）
- ホストが発信するパケットで使用する必要のあるホップ リミットや MTU など、ホストに関する詳細情報

RA は、ルータ送信要求メッセージへの返信としても送信されます。 ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。 ルータ送信要求メッセージが通常システム起動時にホストによって送信される（ホストにユニキャスト アドレスが設定されていない）場合、ルータ送信要求メッセージの送信元アドレスは、通常は未指定の IPv6 アドレス（0:0:0:0:0:0:0:0）です。 ホストに設定済みのユニキャスト アドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャスト アドレスが、メッセージ内の送信元アドレスとして使用されます。 ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。 RA がルータ送信要求への返信として送信される場合、RA メッセージ内の宛先アドレスは、ルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次の RA メッセージ パラメータを設定できます。

- RA メッセージが定期的に送信される時間の間隔
- （特定のリンク上のすべてのノードで使用される）デフォルト ルータとしてのルータの実用性を示す「ルータ ライフタイム」値
- 特定のリンクで使用されているネットワーク プレフィックス
- （特定のリンクで）ネイバー送信要求メッセージが再送信される時間の間隔
- ノードによってネイバーが到達可能である（特定のリンク上のすべてのノードで使用できる）と見なされるまでの時間

設定されたパラメータはインターフェイスに固有です。 RA メッセージ（デフォルト値を含む）の送信は、**ipv6 unicast-routing** コマンドの設定時に FDDI インターフェイスで自動的にイネーブルになります。 その他のインターフェイス タイプの場合は、**no ipv6 nd ra suppress** コマンドを使用して、RA メッセージの送信を手動で設定する必要があります。 個々のインターフェイスで、**ipv6 nd ra** suppress コマンドを使用して、RA メッセージの送信をディセーブルにできます。

トラフィック エンジニアリングのデフォルト ルータ プリファレンス

ホストは、ルータ アドバタイズメント（RA）をリスニングすることでデフォルト デバイスを検出し、選択します。 通常のデフォルト デバイス選択メカニズムは、トラフィック エンジニアリングが必要な場合など、特定のケースでは次善のメカニズムです。 たとえば、リンク上の 2 台のデバイスが、同等だが等しくはないコストのルーティングを提供している場合や、ポリシーによってデバイスの一方を優先することが指示されている場合があります。 次に例をいくつか示します。

- 異なるプレフィックス セットへルーティングする複数のデバイス：リダイレクト（宛先に対して最適でないデバイスによって送信される）は、ホストが任意のデバイスを選択でき、システムが機能することを意味します。 ただし、トラフィック パターンが、デバイスの 1 つを選択することによって、リダイレクト数が大きく削減されることを意味する場合があります。
- 新しいデバイスの誤った展開：新しいデバイスを完全に設定する前に展開すると、ホストによって新しいデバイスがデフォルト デバイスとして採用され、トラフィックが消える可能性があります。 ネットワーク管理者は、一部のデバイスが他のデバイスよりも優先されることを指定できます。
- マルチホーム環境：複数の物理リンクと IPv6 トランスポートでのトンネリングの使用により、マルチホーム環境はより一般的になる可能性があります。 一部のデバイスは、6-to-4 プレフィックスにだけルーティングするか、企業イントラネットにだけルーティングするため、完全なデフォルト ルーティングを提供しないことがあります。 このような状況は、単一リンク上でだけ機能するリダイレクトでは解決できません。

デフォルト ルータ プリファレンス（DRP）機能は、基本的なプリファレンス メトリック（低、中、高）をデフォルト デバイスに提供します。 デフォルト デバイスの DRP は、RA メッセージ内の未使用ビットで通知されます。 この拡張は、デバイス（DRP ビットの設定）とホスト（DRP

ビットの解釈）の両方に対して下位互換性があります。これらのビットは、DRP 拡張を実装しないホストでは無視されます。同様に、DRP 拡張を実装しないデバイスによって送信される値は、DRP 拡張を実装するホストによって「中」のプリファレンスが指定されたものと解釈されます。DRP は手動で設定する必要があります。

IPv6 ネイバー探索マルチキャスト抑制のその他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ICMP for IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *12* : *ICMP for IPv6* の機能情報

機能名	リリース	機能情報
IPv6: ICMPv6	12.0(22)S 12.2(2)T 12.2(14)S 12.2(17a)SX1 12.2(25)SG 12.2(28)SB 12.2(33)SRA 12.2(2)T 15.3(1)S Cisco IOS XE Release 2.1	IPv6 の ICMP は、IPv4 の ICMP と同様の働きをします。 ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。 追加または変更されたコマンドはありません。

第 8 章

IPv6 ICMP レート制限

IPv6 ICMP レート制限機能によって、IPv6 インターネット制御メッセージ プロトコル（ICMP）エラー メッセージがネットワークへ送信されるレートを制限するためのトークン バケット アルゴリズムが実装されます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

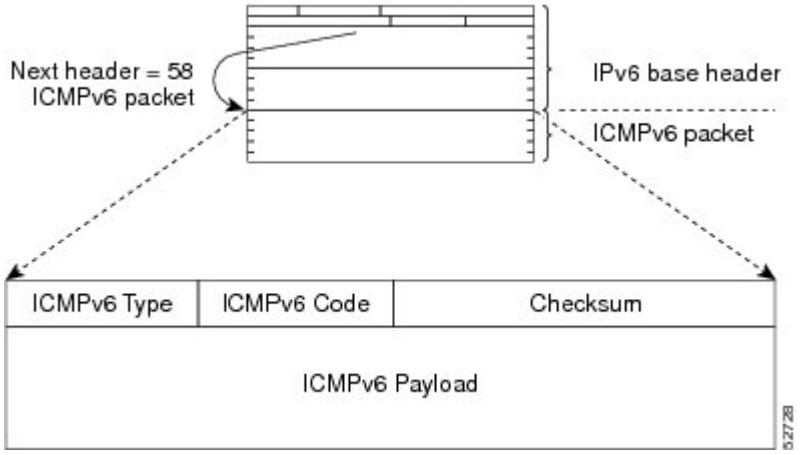
IPv6 ICMP レート制限に関する情報

ICMP for IPv6

IPv6 のインターネット制御メッセージプロトコル（ICMP）の機能は、IPv4 の ICMP と同じです。ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。 また、ICMP for IPv6 パケットは、IPv6 ネイバー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD）プロトコル for IPv6 で使用されます。 MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャストアドレスを宛先としたマルチキャストパケットを受信するために使用するノード）を検出するために IPv6 デバイスで使用されます。 MLD は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。 ICMP for IPv6 パケットは、すべての拡張ヘッダーに続いて IPv6 パケットの末尾に配置される点でトランスポートレイヤ パケットに似ています。 IPv6 ICMP パケット内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサムフィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから抽出されます。 ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。次の図に、IPv6 ICMP パケット ヘッダー形式を示します。

図 *13*：*IPv6 ICMP* パケット ヘッダーの形式



IPv6 ICMP レート制限

IPv6 ICMP レート制限機能によって、IPv6 ICMP エラー メッセージがネットワークへ送信されるレートを制限するためのトークン バケット アルゴリズムが実装されます。 IPv6 ICMP レート制限の初期の実装では、エラー メッセージ間に固定の間隔が定義されていましたが、traceroute などの

一部のアプリケーションでは、間断なく送信される要求のグループへの返信が必要になる場合があります。 エラー メッセージ間の固定間隔は、traceroute などのアプリケーションで動作するのに十分な柔軟性がなく、アプリケーションが失敗する原因となることがあります。

トークン バケット方式を実装すると、複数のトークンを仮想バケットに格納できます。トークンごとに 1 つのエラー メッセージを送信できます。 バケットに格納できるトークンの最大数を指定でき、エラー メッセージが送信されるたびに 1 つのトークンがバケットから削除されます。 一連のエラーメッセージが生成された場合は、バケットが空になるまでエラーメッセージを送信できます。 トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラー メッセージは送信されません。 トークン バケット アルゴリズムは、レート制限の平均時間間隔を増やさず、固定時間間隔方式よりも柔軟性が高くなります。

IPv6 ICMP レート制限の設定方法

IPv6 ICMP レート制限のカスタマイズ

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 icmp error-interval** *milliseconds* [*bucketsize*]

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 モードをイネーブルにします。 • 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： `Device# 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** *milliseconds* [*bucketsize*] 例： `Device(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 サイズをカスタマイズします。

IPv6 ICMP レート制限の設定例

例：IPv6 ICMP レート制限の設定

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
ipv6 icmp error-interval 50 20
```

例：ICMP レート制限カウンタに関する情報の表示

次の例では、ICMP レート制限カウンタに関する情報が表示されます。

```
Device# show ipv6 traffic

ICMP statistics:
  Rcvd: 188 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 175 router advert, 0 redirects
        0 neighbor solicit, 12 neighbor advert
  Sent: 7376 output, 56 rate-limited
        unreach: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        15 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 7326 router advert, 0 redirects
        2 neighbor solicit, 22 neighbor advert
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ICMP レート制限の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *13*：*IPv6 ICMP* レート制限の機能情報

機能名	リリース	機能情報
IPv6 ICMP レート制限	12.2(8)T 15.3(1)S Cisco IOS XE Release 2.1	IPv6 ICMP レート制限機能によって、IPv6 ICMP エラー メッセージがネットワークへ送信されるレートを制限するためのトークン バケット アルゴリズムが実装されます。 **ipv6 icmp error-interval** コマンドが追加または変更されました。

第 9 章

ICMP for IPv6 リダイレクト

IPv6 リダイレクト メッセージ機能により、デバイスはインターネット制御メッセージ プロトコル（ICMP）IPv6 ネイバー リダイレクト メッセージを送信して、宛先へのパス上のより適切なファースト ホップ ノード（デバイスまたはホスト）をホストに通知できます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

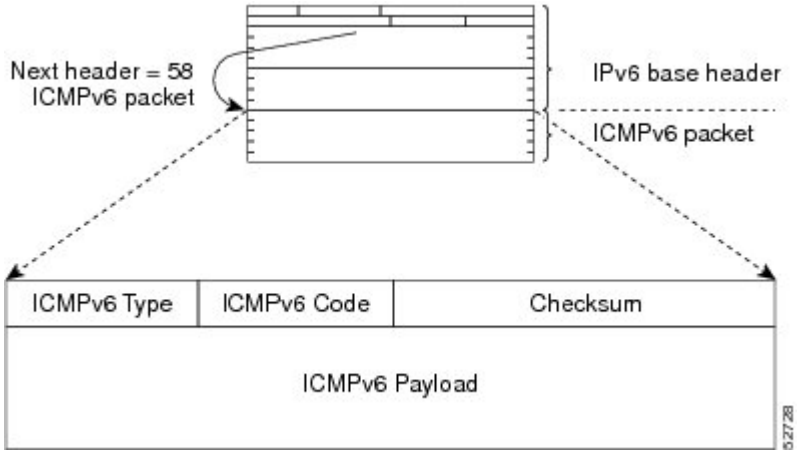
ICMP for IPv6 リダイレクトについて

ICMP for IPv6

IPv6 のインターネット制御メッセージプロトコル（ICMP）の機能は、IPv4 の ICMP と同じです。ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。 また、ICMP for IPv6 パケットは、IPv6 ネイバー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD）プロトコル for IPv6 で使用されます。 MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャストアドレスを宛先としたマルチキャストパケットを受信するために使用するノード）を検出するために IPv6 デバイスで使用されます。 MLD は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。 ICMP for IPv6 パケットは、すべての拡張ヘッダーに続いて IPv6 パケットの末尾に配置される点でトランスポートレイヤ パケットに似ています。 IPv6 ICMP パケット内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサムフィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから抽出されます。 ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。次の図に、IPv6 ICMP パケット ヘッダー形式を示します。

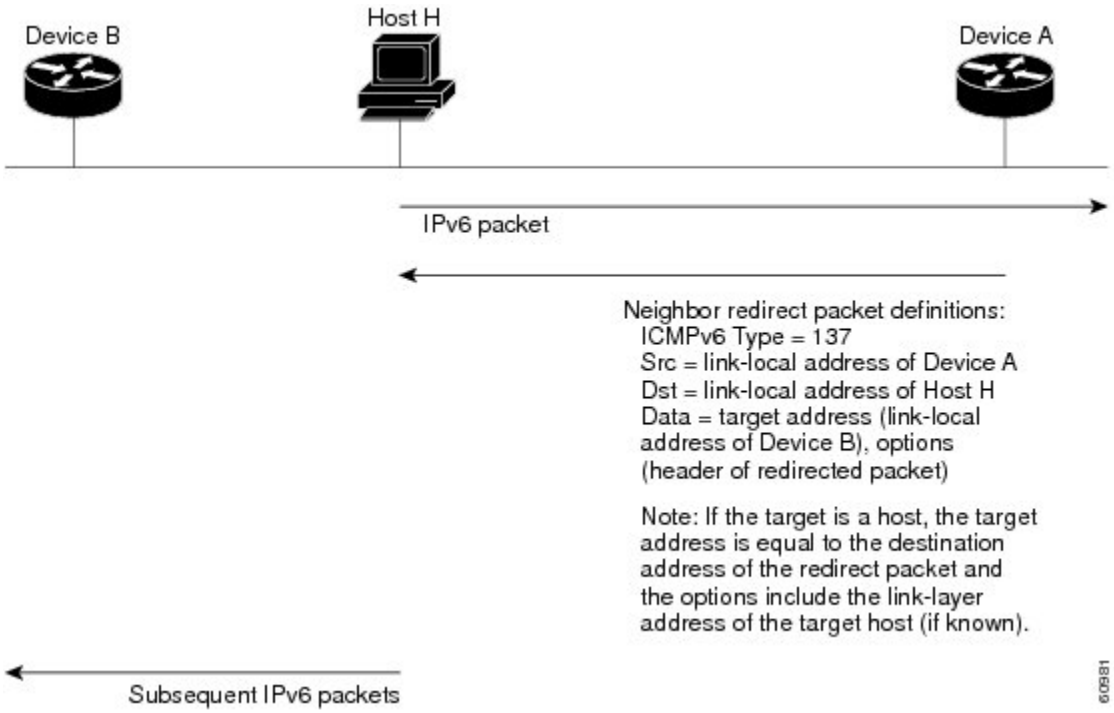
図 *14*：*IPv6 ICMP* パケット ヘッダーの形式



IPv6 ネイバー リダイレクト メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 137 は、IPv6 ネイバー リダイレクト メッセージを示します。 デバイスは、ネイバー リダイレクト メッセージを送信して、宛先へのパス上のより適切なファーストホップ ノードをホストに通知します（次の図を参照）。

図 *15*：*IPv6* ネイバー探索 - ネイバー リダイレクト メッセージ



（注） リダイレクト メッセージ内のターゲット アドレス（最終的な宛先）によって隣接デバイスのリンクローカル アドレスが確実に識別されるように、デバイスは各隣接デバイスのリンクローカル アドレスを判断できる必要があります。 スタティック ルーティングの場合、ネクストホップ デバイスのアドレスは、デバイスのリンクローカル アドレスを使用して指定する必要があります。ダイナミック ルーティングの場合は、すべての IPv6 プロトコルが隣接デバイスのリンクローカル アドレスを交換する必要があります。

パケットの転送後に、次の条件が満たされる場合、デバイスはパケットの送信元にリダイレクト メッセージを送信する必要があります。

- パケットの宛先アドレスがマルチキャスト アドレスではない。
- パケットがデバイスにアドレッシングされていなかった。
- パケットが、そのパケットを受信したインターフェイスから送信されようとしている。

- デバイスが、パケットにより適したファーストホップ ノードはパケットの送信元と同じリンク上にあると判断した。
- パケットの送信元アドレスが、同じリンク上のネイバーのグローバル IPv6 アドレス、またはリンクローカル アドレスである。

ネイバー リダイレクト メッセージなどのすべての IPv6 ICMP エラー メッセージをデバイスが生成するレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。これにより、リンク層の輻輳が最終的に低減されます。

（注） デバイスはネイバー リダイレクト メッセージを受信してもそのルーティング テーブルを更新せず、ホストはネイバー リダイレクト メッセージを発信しません。

IPv6 リダイレクト メッセージの表示方法

IPv6 リダイレクト メッセージの表示

手順の概要

1. **enable**
2. **show ipv6 interface** [**brief**] [*type number*] [**prefix**]
3. **show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics**
4. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
5. **show ipv6 traffic**
6. **show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**]
7. **enable**
8. **show running-config**

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 モードをイネーブルにします。 • 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	**show ipv6 interface** [**brief**] [*type number*] [**prefix**] 例： `Device# show ipv6 interface gigabitethernet 0/0/0`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。
ステップ 3	**show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics** 例： `Device# show ipv6 neighbors gigabitethernet 2/0/0`	IPv6 ネイバー探索キャッシュ情報を表示します。
ステップ 4	**show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*] 例： `Device# show ipv6 route`	（任意）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 5	**show ipv6 traffic** 例： `Device# show ipv6 traffic`	（任意）IPv6 トラフィックの統計情報を表示します。
ステップ 6	**show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**] 例： `Device# show hosts`	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
ステップ 7	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 8	**show running-config** 例： `Device# show running-config`	デバイスで実行されている現在の設定を表示します。

ICMP for IPv6 リダイレクトの設定例

例：IPv6 インターフェイス統計情報の表示

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスが GigabitEthernet インターフェイス 0/0/0 に対して正しく設定されていることを確認します。 IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、およびステートレス自動設定のステータスに関する情報も表示されます。

```
Device# show ipv6 interface gigabitethernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  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.
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ICMP for IPv6 リダイレクトの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *14* : *ICMPv for IPv6* リダイレクトの機能情報

機能名	リリース	機能情報
IPv6：ICMPv6 リダイレクト	12.0(22)S 12.2(4)T 12.2(14)S 12.2(17a)SX1 12.2(25)SG 12.2(28)SB 12.2(33)SRA 15.3(1)S Cisco IOS XE Release 2.1	IPv6 リダイレクト メッセージ機能により、デバイスは ICMP IPv6 ネイバー リダイレクト メッセージを送信して、宛先へのパス上のより適切なファーストホップ ノードをホストに通知できます。 **show ipv6 interface**、**show ipv6 neighbors**、**show ipv6 route**、**show ipv6 traffic** の各コマンドが追加または変更されています。

第 10 章

IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、インターネット制御メッセージ プロトコル（ICMP）メッセージおよび送信要求ノード 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断し、ネイバーに到達可能かどうかを確認し、ネイバー デバイスを追跡します。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 ネイバー ディスカバリについて

IPv6 ネイバー探索

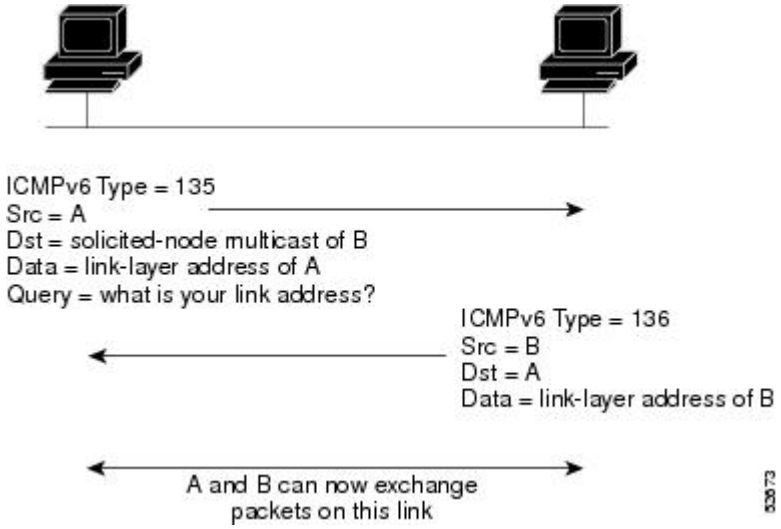
IPv6 ネイバー探索プロセスでは、ICMP メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判断し、ネイバーに到達可能かどうかを確認し、ネイバー デバイスを追跡します。

ネイバー探索用の IPv6 スタティック キャッシュ エントリ機能により、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。 スタティック ルーティングでは、管理者が、各デバイスの各インターフェイスのIPv6アドレス、サブネットマスク、ゲートウェイ、および対応するメディア アクセス コントロール（MAC）アドレスをテーブルに入力する必要があります。 スタティック ルーティングによって、より詳細な制御が可能になりますが、テーブルの保守作業が増えます。 ルートが追加または変更されるたびにテーブルを更新する必要があります。

IPv6 ネイバー送信要求メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 135 は、ネイバー送信要求メッセージを示します。 ネイバー送信要求メッセージは、ノードが同じローカルリンク上の別のノードのリンク層アドレスを判断する必要がある場合にローカルリンクに送信されます（次の図を参照）。 ノードが別のノードのリンク層アドレスを判断する必要がある場合、ネイバー請求メッセージ内の送信元アドレスは、ネイバー請求メッセージを送信するノードのIPv6アドレスです。 ネイバー送信要求メッセージ内の宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノード マルチキャストアドレスです。 ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

図 *16*：*IPv6* ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージを受信した後に、宛先ノードは、ICMP パケット ヘッダーのタイプ フィールドに値 136 を含むネイバー アドバタイズメント メッセージをローカル リンクに送信することで応答します。 ネイバー アドバタイズメント メッセージの送信元アドレスは、ネイバー アドバタイズメント メッセージを送信するノードの IPv6 アドレス（具体的には、ノード インターフェイスの IPv6 アドレス）です。ネイバーアドバタイズメントメッセージ内の宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。 ネイバー アドバタイズメント メッセージのデータ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバー アドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。 あるノードがネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスはネイバーのユニキャスト アドレスです。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。そのような変更があった場合、ネイバーアドバタイズメントの宛先アドレスは全ノード マルチキャスト アドレスになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。 ネイバー到達不能検出では、ネイバーの障害またはネイバーへの転送パスの障害が識別されます。この検出は、ホストとネイバー ノード（ホストまたはデバイス）間のすべてのパスで使用されます。 ネイバー到達不能検出は、ユニキャストパケットだけが送信されるネイバーに対して実行され、マルチキャスト パケットが送信されるネイバーに対しては実行されません。

ネイバーは、（以前にネイバーに送信されたパケットが受信され、処理されたことを示す）肯定確認応答がネイバーから返された場合に、到達可能と見なされます。 到達可能であるという確認は、接続が動作中（宛先に到達中）であることを示す上位層プロトコル（TCP など）からの情報や、ネイバー送信要求メッセージに対するネイバーアドバタイズメントメッセージを受信することで行われます。 パケットがピアに到達している場合、それらのパケットは送信元のネクスト ホップ ネイバーにも到達しています。 したがって、転送の進行により、ネクストホップ ネイバーが到達可能であることも確認されます。

ローカル リンク上にない宛先の場合、転送の進行は、ファーストホップデバイスが到達可能であることを暗に意味します。 上位層プロトコルからの確認応答がない場合、ノードは、ユニキャスト ネイバー送信要求メッセージを使用してネイバーを探し、転送パスがまだ機能していることを確認します。

ネイバーから返信された請求ネイバーアドバタイズメントメッセージは、転送パスがまだ機能しているという肯定確認応答です（請求フラグが値 1 に設定されたネイバー アドバタイズメント メッセージは、ネイバー請求メッセージへの返信としてだけ送信されます）。 非送信要求メッセージでは、送信元ノードから宛先ノードへの一方向パスだけが確認されます。送信要求ネイバー アドバタイズメント メッセージは、両方向のパスが機能していることを示します。

（注） 送信要求フラグが値 0 に設定されたネイバー アドバタイズメント メッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

ネイバー送信要求メッセージは、ユニキャストIPv6アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。新規のリンクローカルIPv6アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。 具体的には、ノードは未指定の送信元アドレスと一時的なリンクローカル アドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。 そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカル アドレスを含むネイバー アドバタイズメント メッセージを返します。 別のノードが同じアドレスの一意性を同時に検証している場合は、そのノードもネイバー送信要求メッセージを返します。ネイバー送信要求メッセージの返信としてネイバー アドバタイズメント メッセージが受信されず、同じ一時アドレスの検証を試行している他のノードからのネイバー送信要求メッセージも受信されない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンクローカル アドレスを一意であると見なし、そのアドレスをインターフェイスに割り当てます。

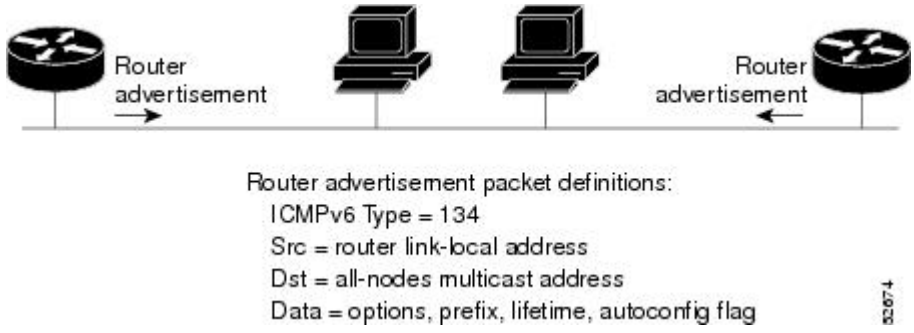
リンク上のすべてのIPv6ユニキャストアドレス（グローバルまたはリンクローカル）が一意であることを検証する必要がありますが、リンクローカル アドレスの一意性が確認されるまでは、リンクローカルアドレスに関連付けられている他のIPv6アドレスに対して重複アドレス検出は実行されません。 シスコ ソフトウェアでの重複アドレス検出のシスコ実装では、64 ビット インターフェイス識別子から生成されるエニーキャストアドレスまたはグローバルアドレスの一意性は確認されません。

IPv6 ルータ アドバタイズメント メッセージ

ルータ アドバタイズメント（RA）メッセージは、ICMP パケット ヘッダーのタイプ フィールドが値 134 であり、IPv6 ルータの設定済みの各インターフェイスへ定期的に送信されます。 ステートレス自動設定が正しく機能するには、RA メッセージでアドバタイズされたプレフィックス長が常に 64 ビットである必要があります。

RA メッセージは、全ノード マルチキャスト アドレスに送信されます（次の図を参照）。

図 *17* : ***IPv6* ネイバー探索 -- *RA* メッセージ**



通常、RA メッセージには次の情報が含まれます。

- ローカル リンク上のノードがその IPv6 アドレスの自動設定に使用できる 1 つ以上のオンリンク IPv6 プレフィックス

- アドバタイズメントに含まれる各プレフィックスのライフタイム情報
- 完成可能な自動設定のタイプ（ステートレスまたはステートフル）を示すフラグのセット
- デフォルト ルータ情報（アドバタイズメントを送信しているルータをデフォルト ルータとして使用する必要があるかどうか、また使用する必要がある場合はルータをデフォルトルータとして使用する必要のある秒単位での時間）
- ホストが発信するパケットで使用する必要のあるホップ リミットや MTU など、ホストに関する詳細情報

RA は、ルータ送信要求メッセージへの返信としても送信されます。 ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。 ルータ送信要求メッセージが通常システム起動時にホストによって送信される（ホストにユニキャスト アドレスが設定されていない）場合、ルータ送信要求メッセージの送信元アドレスは、通常は未指定の IPv6 アドレス（0:0:0:0:0:0:0:0）です。 ホストに設定済みのユニキャスト アドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャスト アドレスが、メッセージ内の送信元アドレスとして使用されます。 ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。 RA がルータ送信要求への返信として送信される場合、RA メッセージ内の宛先アドレスは、ルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次の RA メッセージ パラメータを設定できます。

- RA メッセージが定期的に送信される時間の間隔
- （特定のリンク上のすべてのノードで使用される）デフォルト ルータとしてのルータの実用性を示す「ルータ ライフタイム」値
- 特定のリンクで使用されているネットワーク プレフィックス
- （特定のリンクで）ネイバー送信要求メッセージが再送信される時間の間隔
- ノードによってネイバーが到達可能である（特定のリンク上のすべてのノードで使用できる）と見なされるまでの時間

設定されたパラメータはインターフェイスに固有です。 RA メッセージ（デフォルト値を含む）の送信は、**ipv6 unicast-routing** コマンドの設定時に FDDI インターフェイスで自動的にイネーブルになります。 その他のインターフェイス タイプの場合は、**no ipv6 nd ra suppress** コマンドを使用して、RA メッセージの送信を手動で設定する必要があります。 個々のインターフェイスで、**ipv6 nd ra** suppress コマンドを使用して、RA メッセージの送信をディセーブルにできます。

トラフィック エンジニアリングのデフォルト ルータ プリファレンス

ホストは、ルータ アドバタイズメント（RA）をリスニングすることでデフォルト デバイスを検出し、選択します。 通常のデフォルト デバイス選択メカニズムは、トラフィック エンジニアリングが必要な場合など、特定のケースでは次善のメカニズムです。 たとえば、リンク上の 2 台のデバイスが、同等だが等しくはないコストのルーティングを提供している場合や、ポリシーによっ

てデバイスの一方を優先することが指示されている場合があります。 次に例をいくつか示します。

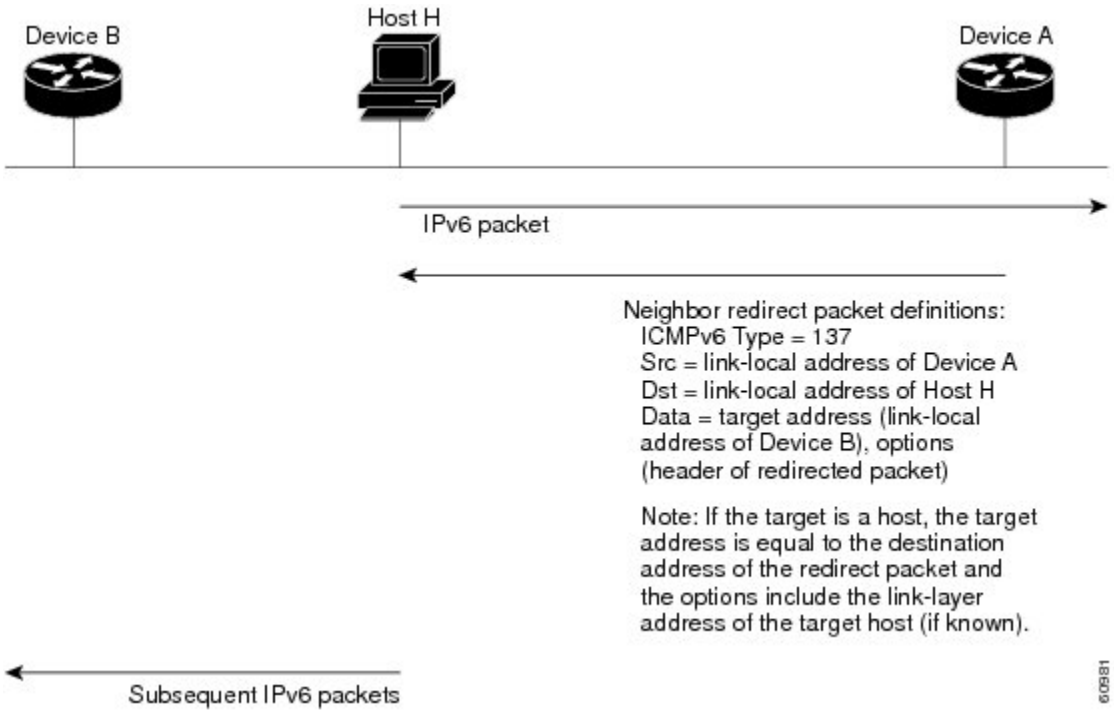
- 異なるプレフィックスセットへルーティングする複数のデバイス：リダイレクト（宛先に対して最適でないデバイスによって送信される）は、ホストが任意のデバイスを選択でき、システムが機能することを意味します。 ただし、トラフィック パターンが、デバイスの 1 つを選択することによって、リダイレクト数が大きく削減されることを意味する場合があります。
- 新しいデバイスの誤った展開：新しいデバイスを完全に設定する前に展開すると、ホストによって新しいデバイスがデフォルトデバイスとして採用され、トラフィックが消える可能性があります。 ネットワーク管理者は、一部のデバイスが他のデバイスよりも優先されることを指定できます。
- マルチホーム環境：複数の物理リンクと IPv6 トランスポートでのトンネリングの使用により、マルチホーム環境はより一般的になる可能性があります。 一部のデバイスは、6-to-4 プレフィックスにだけルーティングするか、企業イントラネットにだけルーティングするため、完全なデフォルト ルーティングを提供しないことがあります。 このような状況は、単一リンク上でだけ機能するリダイレクトでは解決できません。

デフォルト ルータ プリファレンス（DRP）機能は、基本的なプリファレンス メトリック（低、中、高）をデフォルト デバイスに提供します。 デフォルト デバイスの DRP は、RA メッセージ内の未使用ビットで通知されます。 この拡張は、デバイス（DRP ビットの設定）とホスト（DRP ビットの解釈）の両方に対して下位互換性があります。 これらのビットは、DRP 拡張を実装しないホストでは無視されます。 同様に、DRP 拡張を実装しないデバイスによって送信される値は、DRP 拡張を実装するホストによって「中」のプリファレンスが指定されたものと解釈されます。 DRP は手動で設定する必要があります。

IPv6 ネイバー リダイレクト メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 137 は、IPv6 ネイバー リダイレクト メッセージを示します。 デバイスは、ネイバー リダイレクト メッセージを送信して、宛先へのパス上のより適切なファーストホップ ノードをホストに通知します（次の図を参照）。

図 *18*：*IPv6* ネイバー探索 - ネイバー リダイレクト メッセージ



（注） リダイレクト メッセージ内のターゲット アドレス（最終的な宛先）によって隣接デバイスのリンクローカルアドレスが確実に識別されるように、デバイスは各隣接デバイスのリンクローカル アドレスを判断できる必要があります。 スタティック ルーティングの場合、ネクストホップ デバイスのアドレスは、デバイスのリンクローカル アドレスを使用して指定する必要があります。ダイナミック ルーティングの場合は、すべての IPv6 プロトコルが隣接デバイスのリンクローカル アドレスを交換する必要があります。

パケットの転送後に、次の条件が満たされる場合、デバイスはパケットの送信元にリダイレクト メッセージを送信する必要があります。

- パケットの宛先アドレスがマルチキャスト アドレスではない。
- パケットがデバイスにアドレッシングされていなかった。
- パケットが、そのパケットを受信したインターフェイスから送信されようとしている。

- デバイスが、パケットにより適したファーストホップ ノードはパケットの送信元と同じリンク上にあると判断した。
- パケットの送信元アドレスが、同じリンク上のネイバーのグローバル IPv6 アドレス、またはリンクローカル アドレスである。

ネイバー リダイレクト メッセージなどのすべての IPv6 ICMP エラー メッセージをデバイスが生成するレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。これにより、リンク層の輻輳が最終的に低減されます。

（注） デバイスはネイバー リダイレクト メッセージを受信してもそのルーティング テーブルを更新せず、ホストはネイバー リダイレクト メッセージを発信しません。

IPv6 ネイバー探索の設定方法

IPv6 ネイバー探索のパラメータ調整

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd nud retry** *base interval max-attempts*
5. **ipv6 nd cache expire** *expire-time-in-seconds* [**refresh**]
6. **ipv6 nd na glean**

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 モードをイネーブルにします。 • 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： `Device# 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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/0`	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。
ステップ 4	**ipv6 nd nud retry** *base interval max-attempts* 例： `Device(config-if)# ipv6 nd nud retry 1 1000 3`	NUD がネイバー送信要求に再送信する回数を設定します。
ステップ 5	**ipv6 nd cache expire** *expire-time-in-seconds* [**refresh**] 例： `Device(config-if)# ipv6 nd cache expire 7200`	IPv6 ND キャッシュ エントリの期限が切れるまでの時間を設定します。
ステップ 6	**ipv6 nd na glean** 例： `Device(config-if)# ipv6 nd na glean`	非請求 NA からのエントリを収集するように ND を設定します。

IPv6 ICMP レート制限のカスタマイズ

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 icmp error-interval** *milliseconds* [*bucketsize*]

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 モードをイネーブルにします。 • 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** 例： `Device# 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** *milliseconds* [*bucketsize*] 例： `Device(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 サイズをカスタマイズします。

IPv6 リダイレクト メッセージの表示

手順の概要

1. **enable**
2. **show ipv6 interface** [**brief**] [*type number*] [**prefix**]
3. **show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics**
4. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
5. **show ipv6 traffic**
6. **show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**]
7. **enable**
8. **show running-config**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ipv6 interface** [**brief**] [*type number*] [**prefix**] 例： `Device# show ipv6 interface gigabitethernet 0/0/0`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics** 例： `Device# show ipv6 neighbors gigabitethernet 2/0/0`	IPv6 ネイバー探索キャッシュ情報を表示します。
ステップ 4	**show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*] 例： `Device# show ipv6 route`	（任意）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 5	**show ipv6 traffic** 例： `Device# show ipv6 traffic`	（任意）IPv6 トラフィックの統計情報を表示します。
ステップ 6	**show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**] 例： `Device# show hosts`	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
ステップ 7	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 8	**show running-config** 例： `Device# show running-config`	デバイスで実行されている現在の設定を表示します。

IPv6 ネイバー探索の設定例

例：IPv6 ネイバー探索のパラメータのカスタマイズ

次の例では、IPv6 ND NA グリーニングをイネーブルにし、IPv6 ND キャッシュの有効期限を 7200 秒（2 時間）に設定しています。

```
interface Port-channel189
 no ip address
 ipv6 address FC07::789:1:0:0:3/64
 ipv6 nd reachable-time 2700000
 ipv6 nd na glean
 ipv6 nd cache expire 7200
 no ipv6 redirects
 standby version 2
 standby 2 ipv6 FC07::789:1:0:0:1/64
 standby 2 priority 150
 standby 2 preempt
```

例：IPv6 ICMP レート制限の設定

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
ipv6 icmp error-interval 50 20
```

例：ICMP レート制限カウンタに関する情報の表示

次の例では、ICMP レート制限カウンタに関する情報が表示されます。

```
Device# show ipv6 traffic

ICMP statistics:
  Rcvd: 188 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 175 router advert, 0 redirects
        0 neighbor solicit, 12 neighbor advert
  Sent: 7376 output, 56 rate-limited
        unreach: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        15 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 7326 router advert, 0 redirects
        2 neighbor solicit, 22 neighbor advert
```

例：IPv6 インターフェイス統計情報の表示

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスが FastEthernet インターフェイス 1/0 に対して正しく設定されていることを確認します。IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、ステートレス自動設定、および MTU サイズのステータスに関する情報も表示されることがあります。

```
Device# show ipv6 interface fastethernet 1/0

Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  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.
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ネイバー探索の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *15* : *IPv6* ネイバー探索の機能情報

機能名	リリース	機能情報
IPv6 ネイバー探索	12.0(22)S 12.2(2)T 12.2(14)S 12.2(17a)SX1 12.2(25)SG 12.2(28)SB 12.2(33)SRA Cisco IOS XE Release 2.1 12.2(50)SY 15.0(1)SY 3.2.0SG	IPv6 ネイバー探索プロセスでは、ICMP メッセージおよび送信要求ノード 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断し、ネイバーに到達可能かどうかを確認し、ネイバー デバイスを追跡します。 **ipv6 nd cache expire**、**ipv6 nd na glean**、**ipv6 nd nud retry** の各コマンドが追加または変更されています。
IPv6：ネイバー探索重複アドレス検出	12.0(22)S 12.2(4)T 12.2(17a)SX1 12.2(14)S 12.2(25)SG 12.2(28)SB 12.2(33)SRA 12.2(50)SY 15.0(1)SY 15.1(1)SY 15.3(1)S Cisco IOS XE Release 2.1	新規のリンクローカル IPv6 アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に IPv6 ネイバー探索重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。 追加または変更されたコマンドはありません。
IPv6ネイバー探索ノンストップフォワーディング	12.2(33)SRE 15.0(1)S 15.0(1)SY 15.1(1)SY	IPv6ネイバー探索ノンストップフォワーディング機能は、IPv6 ハイアベイラビリティのサポートを提供します。 追加または変更されたコマンドはありません。

第 11 章

IPv6 のネイバー探索キャッシュ

IPv6 ネイバー探索キャッシュ機能により、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。

Per-Interface ネイバー探索キャッシュ制限機能を使用すると、インターフェイスに接続されている特定のお客様が（意図的に、または意図せずに）ネイバー探索キャッシュをオーバーロードしないようにすることができます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ネイバー探索用の IPv6 スタティック キャッシュ エントリについて

IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、ICMP メッセージおよび送信要求ノード 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断し、ネイバーに到達可能かどうかを確認し、ネイバー デバイスを追跡します。

ネイバー探索用の IPv6 スタティック キャッシュ エントリ機能により、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。 スタティック ルーティングでは、管理者が、各デバイスの各インターフェイスの IPv6 アドレス、サブネットマスク、ゲートウェイ、および対応するメディア アクセス コントロール（MAC）アドレスをテーブルに入力する必要があります。 スタティック ルーティングによって、より詳細な制御が可能になりますが、テーブルの保守作業が増えます。 ルートが追加または変更されるたびにテーブルを更新する必要があります。

Per-Interface ネイバー探索キャッシュ制限

ネイバー探索キャッシュ内のエントリ数は、インターフェイスごとに制限できます。 この制限に達すると、新しいエントリは追加されなくなります。 Per-Interface ネイバー探索キャッシュ制限機能を使用すると、インターフェイスに接続されている特定のお客様が（意図的に、または意図せずに）ネイバー探索キャッシュをオーバーロードしないようにすることができます。

この機能をグローバルにイネーブルにすると、デバイス上のすべてのインターフェイスに、共通のインターフェイス単位のキャッシュ サイズ制限が設定されます。この機能をインターフェイスごとにイネーブルにすると、キャッシュ サイズ制限はそれに対応するインターフェイス上で設定されます。 インターフェイスごとの制限は、グローバルに設定された制限よりも優先されます。

IPv6 ネイバー探索キャッシュの設定方法

指定したインターフェイス上でのネイバー探索キャッシュ制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd cache interface-limit** *size* [**log** *rate*]

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 モードをイネーブルにします。 • 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： `Device# 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** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/0`	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。
ステップ 4	**ipv6 nd cache interface-limit** *size* [**log** *rate*] 例： `Device(config-if)# ipv6 nd cache interface-limit 1`	デバイス上の指定したインターフェイスにネイバー探索キャッシュ制限を設定します。 • このコマンドを実行すると、グローバル コンフィギュレーション モードで **ipv6 nd cache interface-limit** を実行して作成されている設定が上書きされます。

すべてのデバイスインターフェイス上でのネイバー探索キャッシュ制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd cache interface-limit** *size* [**log** *rate*]

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 モードをイネーブルにします。 • 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： `Device# 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 cache interface-limit** *size* [**log** *rate*] 例： `Device(config)# ipv6 nd cache interface-limit 4`	デバイス上のすべてのインターフェイスにネイバー探索キャッシュ制限を設定します。

IPv6 ネイバー探索キャッシュの設定例

例：ネイバー探索キャッシュ制限の設定

```
Device# show ipv6 interface GigabitEthernet2/0/0

Interface GigabitEthernet2/0/0, entries 2, static 0, limit 4

IPv6 Address                Age Link-layer Addr State  Interface
2001:0db8::94                 0 aabb.cc00.5d02    REACH  GE2/0/0
FE80::A8BB:CCFF:FE00:5D02   0 aabb.cc00.5d02    DELAY  GE2/0/0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ネイバー探索キャッシュの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *16*：*IPv6* ネイバー探索キャッシュの機能情報

機能名	リリース	機能情報
IPv6：Per-Interface ネイバー探索キャッシュ制限	15.1(1)SY 15.1(3)T Cisco IOS XE Release 2.6	Per-Interface ネイバー探索キャッシュ制限機能を使用すると、インターフェイスに接続されている特定のお客様が（意図的に、または意図せずに）ネイバー探索キャッシュをオーバーロードしないようにすることができます。 **ipv6 nd cache interface-limit**、**show ipv6 interface** の各コマンドが追加または変更されています。
ネイバー探索用の IPv6 スタティック キャッシュ エントリ	12.2(8)T 12.2(17)SX1 12.2(25)SEA 12.2(25)SG 12.2(33)SRA 15.3(1)S Cisco IOS XE Release 2.1 15.0(2)SG 3.2.0SG	ネイバー探索用の IPv6 スタティック キャッシュ エントリ機能により、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。 **ipv6 nd cache interface-limit**、**show ipv6 interface** の各コマンドが追加または変更されています。

第 12 章

IPv6 デフォルト ルータ プリファレンス

IPv6 デフォルト ルータ プリファレンス機能は、大まかなプリファレンス メトリック（低、中、高）をデフォルト デバイスに提供します。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 デフォルト ルータ プリファレンスについて

トラフィック エンジニアリングのデフォルト ルータ プリファレンス

ホストは、ルータ アドバタイズメント（RA）をリスニングすることでデフォルト デバイスを検出し、選択します。 通常のデフォルト デバイス選択メカニズムは、トラフィック エンジニアリングが必要な場合など、特定のケースでは次善のメカニズムです。 たとえば、リンク上の 2 台のデバイスが、同等だが等しくはないコストのルーティングを提供している場合や、ポリシーによってデバイスの一方を優先することが指示されている場合があります。 次に例をいくつか示します。

- 異なるプレフィックスセットへルーティングする複数のデバイス：リダイレクト（宛先に対して最適でないデバイスによって送信される）は、ホストが任意のデバイスを選択でき、システムが機能することを意味します。 ただし、トラフィック パターンが、デバイスの 1 つを選択することによって、リダイレクト数が大きく削減されることを意味する場合があります。
- 新しいデバイスの誤った展開：新しいデバイスを完全に設定する前に展開すると、ホストによって新しいデバイスがデフォルトデバイスとして採用され、トラフィックが消える可能性があります。 ネットワーク管理者は、一部のデバイスが他のデバイスよりも優先されることを指定できます。
- マルチホーム環境：複数の物理リンクと IPv6 トランスポートでのトンネリングの使用により、マルチホーム環境はより一般的になる可能性があります。 一部のデバイスは、6-to-4 プレフィックスにだけルーティングするか、企業イントラネットにだけルーティングするため、完全なデフォルト ルーティングを提供しないことがあります。 このような状況は、単一リンク上でだけ機能するリダイレクトでは解決できません。

デフォルト ルータ プリファレンス（DRP）機能は、基本的なプリファレンス メトリック（低、中、高）をデフォルト デバイスに提供します。 デフォルト デバイスの DRP は、RA メッセージ内の未使用ビットで通知されます。 この拡張は、デバイス（DRP ビットの設定）とホスト（DRP ビットの解釈）の両方に対して下位互換性があります。 これらのビットは、DRP 拡張を実装しないホストでは無視されます。 同様に、DRP 拡張を実装しないデバイスによって送信される値は、DRP 拡張を実装するホストによって「中」のプリファレンスが指定されたものと解釈されます。 DRP は手動で設定する必要があります。

IPv6 デフォルト ルータ プリファレンスの設定方法

トラフィック エンジニアリングの DRP 拡張の設定

RA に DRP 拡張を設定してデフォルト ルータにプリファレンス値をシグナリングするには、このタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd router-preference** {**high** | **medium** | **low**

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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	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。
ステップ 4	**ipv6 nd router-preference** {**high**	**medium**	**low** 例： `Router(config-if)# ipv6 nd router-preference high`	特定のインターフェイス上のルータに DRP を設定します。

IPv6 デフォルト ルータ プリファレンスの設定例

例：IPv6 デフォルト ルータ プリファレンス

次に、このデバイスによってインターフェイス経由でアドバタイズされるDRPプリファレンス値の状態を表示する例を示します。

```
Device# show ipv6 interface gigabitethernet 0/1

GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::130
  Description: Management network (dual stack)
  Global unicast address(es):
    FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:130
  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
  ND advertised default router preference is Low
  Hosts use stateless autoconfig for addresses.
```

次に、その他のデバイスによってアドバタイズされるDRPプリファレンス値の状態を表示する例を示します。

```
Device# show ipv6 routers

Router FE80::169 on GigabitEthernet0/1, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  Preference=Medium
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix FEC0:240:104:1000::/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 デフォルト ルータ プリファレンスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *17* : *IPv6* デフォルト ルータ プリファレンスの機能情報

機能名	リリース	機能情報
IPv6 デフォルト ルータ プリファレンス	12.2(33)SRA 12.2(33)SXH 12.2(46)SE 12.2(46)SG 12.4(2)T 15.0M 15.0(2)SG 3.2.0SG Cisco IOS XE Release 3.9S	この機能は、基本的なプリファレンス メトリック（低、中、高）をデフォルト デバイスに提供します。 Cisco IOS XE Release 3.9S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。 Cisco IOS XE Release 3.9S では、Cisco CSR 1000V のサポートが追加されました。 **ipv6 nd router-preference**、**show ipv6 interface**、**show ipv6 router** の各コマンドが追加または変更されています。

第 13 章

IPv6 ステートレス自動設定

IPv6 ステートレス自動設定機能を使用して、リンク、サブネット、およびサイト アドレッシングの変更を管理できます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェアリリースに対応した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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 ステートレス自動設定について

IPv6 ステートレス自動設定

IPv6 ノード上のすべてのインターフェイスには、通常はインターフェイスの識別子とリンクローカル プレフィックス FE80::/10 から自動的に設定されるリンクローカル アドレスが必要です。 リンクローカル アドレスを使用すると、ノードがリンク上の他のノードと通信できます。また、リンクローカル アドレスを使用して、ノードをさらに設定することもできます。

ノードは、手動の設定や Dynamic Host Configuration Protocol（DHCP）サーバなどのサーバの支援を必要とすることなく、ネットワークに接続し、グローバル IPv6 アドレスを自動的に生成できます。 IPv6 では、リンク上のデバイスは、ルータ アドバタイズメント（RA）メッセージ内で、任意のグローバルプレフィックスと、リンクのデフォルトデバイスとして機能する旨をアドバタイズします。 RA メッセージは、定期的に送信される場合と、システム始動時にホストから送信されるデバイス送信要求メッセージに対する応答として送信される場合があります。

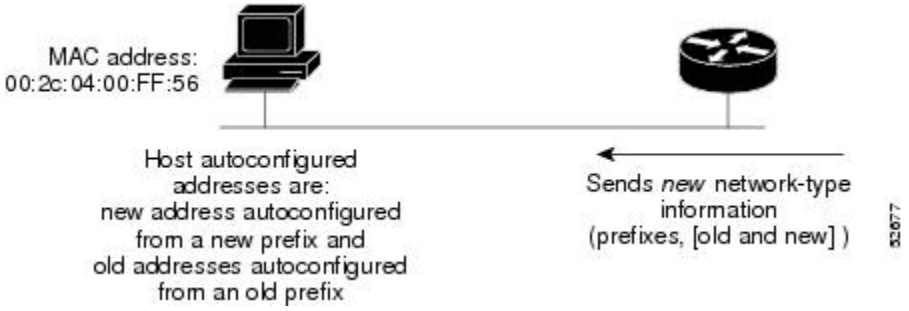
リンク上のノードは、RA メッセージに含まれるプレフィックス（64 ビット）にインターフェイス識別子（64 ビット）を付加することで、グローバル IPv6 アドレスを自動的に設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。 RA メッセージでアドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。 ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるデバイス送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。

IPv6 ホストの簡易ネットワーク リナンバリング

グローバル ルーティング テーブルの厳格な集約では、ネットワークのサービス プロバイダーが変更された場合にネットワークをリナンバリングする必要があります。 IPv6 のステートレス自動設定機能を使用してネットワークをリナンバリングする場合は、新しいサービス プロバイダーからのプレフィックスが、リンク上に送信される RA メッセージに追加されます （RA メッセージには、古いサービスプロバイダーからのプレフィックスと新しいサービスプロバイダーからのプレフィックスの両方が含まれます）。リンク上のノードは、新しいサービス プロバイダーからのプレフィックスを使用して追加アドレスを自動的に設定します。 ノードは、新しいプレフィックスから作成されたアドレスとリンク上の古いプレフィックスから作成された既存のアドレスを使用できます。 古いプレフィックスと新しいプレフィックスに関連付けられているライフタイムパラメータの設定は、リンク上のノードが、新しいプレフィックスから作成されたアドレスだけを使用するように移行できることを意味します。 遷移期間中は、古いプレフィックスが RA メッセー

ジから削除され、新しいプレフィックスを含むアドレスだけがリンク上で使用されます（リナンバリングが完了します）（次の図を参照）。

図 *19*：ステートレス自動設定を使用したホストの *IPv6* ネットワーク リナンバリング



IPv6 ステートレス自動設定の設定方法

IPv6 ステートレス自動設定のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address autoconfig**

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 モードをイネーブルにします。 • 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： `Device# 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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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。
ステップ 4	**ipv6 address autoconfig** 例： `Device(config-if)# ipv6 address autoconfig`	インターフェイスに対してステートレス自動設定を使用した IPv6 アドレスの自動設定をイネーブルにし、インターフェイスにおける IPv6 処理をイネーブルにします。

IPv6 ステートレス自動設定の設定例

例：IPv6 インターフェイス統計情報の表示

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスが GigabitEthernet インターフェイス 0/0/0 に対して正しく設定されていることを確認します。 IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、およびステートレス自動設定のステータスに関する情報も表示されます。

```
Device# show ipv6 interface gigabitethernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  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.
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ステートレス自動設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *18*：*IPv6* ステートレス自動設定の機能情報

機能名	リリース	機能情報
IPv6 ステートレス自動設定	12.2(2)T 12.2(17a)SX1 12.2(25)SEA 12.2(33)SRA 12.2(25)SG 15.0(2)SG 15.3(1)S Cisco IOS XE Release 2.1 3.2.0SG	IPv6 ステートレス自動設定機能を使用して、リンク、サブネット、およびサイト アドレッシングの変更を管理できます。 コマンド **ipv6 address autoconfig** が追加または変更されました。

第 14 章

IPv6 RFCs

標準および **RFC**

RFC	タイトル
RFC 1195	『*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*』
RFC 1267	『*A Border Gateway Protocol 3 (BGP-3)*』
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』
RFC 1583	『*OSPF version 2*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1886	『*DNS Extensions to Support IP version 6*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2080	『*RIPng for IPv6*』
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』

RFC	タイトル
RFC 2375	『*IPv6 Multicast Address Assignments*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2427	『*Multiprotocol Interconnect over Frame Relay*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』

RFC	タイトル
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2492	『*IPv6 over ATM*』
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Specification*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2684	『*Multiprotocol Encapsulation over ATM Adaptation Layer 5*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』
RFC 2710	『*Multicast Listener Discovery (MLD) for IPv6*』
RFC 2711	『*IPv6 Router Alert Option*』
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 2765	『*Stateless IP/ICMP Translation Algorithm (SIIT)*』
RFC 2766	『*Network Address Translation-Protocol Translation (NAT-PT)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 3068	『*An Anycast Prefix for 6to4 Relay Routers*』

RFC	タイトル
RFC 3095	『*RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 3137	『*OSPF Stub Router Advertisement*』
RFC 3147	『*Generic Routing Encapsulation over CLNS*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 3414	『*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3576	『*Change of Authorization*』
RFC 3587	『*IPv6 Global Unicast Address Format*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』
RFC 3596	『*DNS Extensions to Support IP Version 6*』
RFC 3633	『*DHCP IPv6 Prefix Delegation*』

RFC	タイトル
RFC 3646	『*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3697	『*IPv6 Flow Label Specification*』
RFC 3736	『*Stateless DHCP Service for IPv6*』
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3759	『*RObust Header Compression (ROHC): Terminology and Channel Mapping Examples*』
RFC 3775	『*Mobility Support in IPv6*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 3846	『*Mobile IPv4 Extension for Carrying Network Access Identifiers*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』
RFC 3956	『*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 3971	『*SEcure Neighbor Discovery (SEND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』

RFC	タイトル
RFC 4087	『*IP Tunnel MIB*』
RFC 4091	『*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework*』
RFC 4092	『*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4191	『*Default Router Preferences and More-Specific Routes*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4282	『*The Network Access Identifier*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6*』
RFC 4285	『*Authentication Protocol for Mobile IPv6*』
RFC 4291	『*IP Version 6 Addressing Architecture*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

RFC	タイトル
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4443	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 4594	『*Configuration Guidelines for DiffServ Service Classes*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*』
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』
RFC 4798	『*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*』
RFC 4818	『*RADIUS Delegated-IPv6-Prefix Attribute*』
RFC 4861	『*Neighbor Discovery for IP version 6 (IPv6)*』
RFC 4862	『*IPv6 Stateless Address Autoconfiguration*』
RFC 4884	『*Extended ICMP to Support Multi-Part Messages*』
RFC 4885	『*Network Mobility Support Terminology*』
RFC 4887	『*Network Mobility Home Network Models*』
RFC 5015	『*Bidirectional Protocol Independent Multicast (BIDIR-PIM)*』

RFC	タイトル
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5072	『*IPv6 over PPP*』
RFC 5095	『*Deprecation of Type 0 Routing Headers in IPv6*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5130	『*A Policy Control Mechanism in IS-IS Using Administrative Tags*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5213	『*Proxy Mobile IPv6*』
RFC 5308	『*Routing IPv6 with IS-IS*』
RFC 5340	『*OSPF for IPv6*』
RFC 5460	『*DHCPv6 Bulk Leasequery*』
RFC 5643	『*Management Information Base for OSPFv3*』
RFC 5838	『*Support of Address Families in OSPFv3*』
RFC 5844	『*IPv4 Support for Proxy Mobile IPv6*』
RFC 5845	『*Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6*』
RFC 5846	『*Binding Revocation for IPv6 Mobility*』
RFC 5881	『*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*』
RFC 5905	『*Network Time Protocol Version 4: Protocol and Algorithms Specification*』
RFC 5969	『*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) -- Protocol Specification*』
RFC 6105	『*IPv6 Router Advertisement Guard*』

RFC	タイトル
RFC 6620	『*FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*』