IPv6 の設定

この章では、Cisco NX-OS デバイス上でのインターネット プロトコル バージョン 6（IPv6）（アドレス指定を含む）、ネイバー探索プロトコル（ND）、および Internet Control Message Protocol（ICMP）の構成方法を説明します。

この章は、次の項で構成されています。

IPv6 について

IPv6 は、IPv4 の後継として設計されており、ネットワーク アドレス ビット数が 32 ビット（IPv4 の場合）から 128 ビットに増やされています。IPv6 は IPv4 に基づいていますが、アドレス空間が大幅に拡大されており、メインヘッダーと拡張ヘッダーの簡素化など、その他の機能強化が含まれています。

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。柔軟性の高い IPv6 アドレス空間により、プライベート アドレスの必要性と、プライベート（グローバルに一意ではない）アドレスを限られた数のパブリック アドレスに変換するネットワーク アドレス変換（NAT）の使用が削減されます。IPv6 を使用すると、ネットワークの境界にある境界ルータ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。

プレフィックス集約、簡易ネットワーク再番号割り当て、IPv6 サイト マルチホーミング機能などの IPv6 機能により、さらに効率的にルーティングが行われます。IPv6 は、IPv6 向け Open Shortest Path First（OSPF）やマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）をサポートしています。

IPv6 アドレス形式

IPv6 アドレスは 128 ビットつまり 16 バイトです。このアドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 16 ビット 16 進数のブロック 8 つに分かれています。次に、IPv6 アドレスの例を 2 つ示します。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:32102001:0DB8:0:0:8:800:200C:417A
```

IPv6 アドレスの中には、連続するゼロが含まれます。IPv6 アドレスの先頭、中間、または末尾で、この連続するゼロの代わりに 2 つのコロン（::）を使用できます。次の表は、圧縮された IPv6 アドレス フォーマットの一覧です。

（注） IPv6 アドレスでは、アドレス中で最も長く連続するゼロの代わりに、2 つのコロン（::）を 1 度だけ使用できます。

連続する 16 ビット値がゼロで示されている場合は、2 つのコロンを IPv6 アドレス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。

IPv6 アドレス中の 16 進数の文字の大文字と小文字は区別されません。

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

ノードは表「**圧縮された IPv6 アドレス形式（Compressed IPv6 Address Formats）**」にあるループバック アドレスを使用して、IPv6 パケットを自分宛てテーブルにに送信できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレスと同じです。詳細については、概要を参照してください。

（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はできません。送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットは、そのパケットを作成したノードの外には転送できません。IPv6 ルータは、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。

（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はできません。未指定 IPv6 アドレスは、IPv6 パケット内の宛先アドレスまたは IPv6 ルーティング ヘッダーとして使用しないでください。

IPv6 プレフィックスは、RFC 2373 で規定された形式です。この形式では、IPv6 アドレスが、コロンに囲まれた 16 ビット値を使用した 16 進数で指定されています。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、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 ユニキャスト アドレス

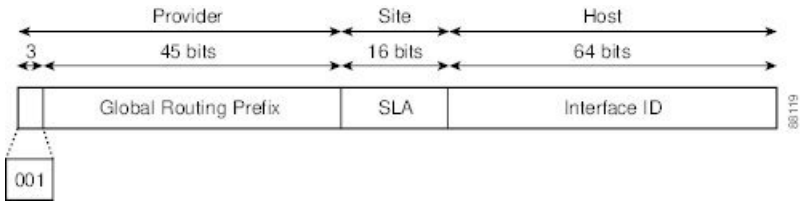
IPv6ユニキャストアドレスは、1つのノード上の1つのインターフェイスのIDです。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。

集約可能グローバル アドレス

集約可能グローバル アドレスは、集約可能なグローバル ユニキャスト プレフィックスによる IPv6 アドレスです。集約可能グローバル ユニキャスト アドレスの構造により、グローバル ルーティング テーブル内のルーティング テーブル エントリ数を制限するルーティング プレフィックスの厳密な集約が可能になります。集約可能グローバル アドレスは、組織を上に向かって、最終的にインターネット サービス プロバイダー（ISP）まで集約されるリンク上で使用されます。

集約可能なグローバル IPv6 アドレスは、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID により定義されます。バイナリ 000 で始まるアドレスを除き、グローバル ユニキャスト アドレスはすべて 64 ビット インターフェイス ID を持ちます。IPv6 グローバル ユニキャスト アドレスの割り当てには、バイナリ値 001（2000::/3）から始まるアドレスの範囲が使用されます。次の図は、集約可能グローバルアドレスの構造を示しています。

図 *1*：集約可能グローバル アドレス形式



2000::/3（001）～ E000::/3（111）のプレフィックスを持つアドレスには、Extended Universal Identifier（EUI）64 形式の 64 ビット インターフェイス識別子が必要です。インターネット割り当て番号局（IANA）は、2000::/16 の範囲の IPv6 アドレス空間を地域レジストリに割り当てます。

集約可能なグローバル アドレスは、48 ビット グローバル ルーティング プレフィックスと、16 ビット サブネット ID または Site-Level Aggregator（SLA）で構成されます。IPv6 集約可能グローバル ユニキャスト アドレスの形式に関するドキュメント（RFC 2374）によると、グローバル ルーティング プレフィックスには、Top-Level Aggregator（TLA）と Next-Level Aggregator（NLA）という 2 つの階層構造のフィールドが含まれています。TLS フィールドおよび NLA フィールドはポリシーベースであるため、IETF は、これらのフィールドを RFC から削除することを決定しました。この変更以前に展開された既存の IPv6 ネットワークの中には、依然として、古いアーキテクチャ上のネットワークを使用しているものもあります。

個々の組織は、16 ビット サブネット フィールドであるサブネット ID を使用して、ローカル アドレス指定階層を作成したり、サブネットを識別したりできます。サブネット ID は IPv4 でのサブネットに似ていますが、IPv6 サブネット ID を持つ組織では最大 65,535 個のサブネットをサポートできるという点が異なります。

インターフェイス ID により、リンク上のインターフェイスが識別されます。インターフェイス ID は、リンク上では一意です。多くの場合、インターフェイス ID は、インターフェイスのリンク層アドレスと同じか、リンク層アドレスに基づいています。集約可能なグローバル ユニキャストやその他の IPv6 アドレス タイプで使用されるインターフェイス ID は 64 ビットであり、形式は変更済み EUI-64 フォーマットです。

インターフェイス ID は、次のいずれかに該当する修正 EUI-64 形式です。

- すべての IEEE 802 インターフェイス タイプ（イーサネット、およびファイバ分散データ インターフェイスなど）の場合は、最初の 3 オクテット（24 ビット）がそのインターフェイスの 48 ビット リンク層アドレス（MAC アドレス）の Organizationally Unique Identifier（OUI）、4 番めと 5 番めのオクテット（16 ビット）が FFFE の固定 16 進数値、そして、最後の 3 オクテット（24 ビット）が MAC アドレスの最後の 3 オクテットです。最初のオクテットの 7 番めのビットである Universal/Local（U/L）ビットの値は 0 または 1 です。ゼロはローカルに管理されている ID を表し、1 はグローバルに一意の IPv6 インターフェイス ID を表します。

- その他すべてのインターフェイス タイプ（シリアル、ループバック、ATM、フレーム リレー、トンネル インターフェイス タイプなど、IPv6 オーバーレイ トンネルで使用されるトンネル インターフェイスを除く）の場合、インターフェイス ID は IEEE 802 インターフェイス タイプのインターフェイス ID に似ていますが、ルータの MAC アドレス プールの最初の MAC アドレスが識別子として使用されます（インターフェイスには MAC アドレスがないため）。

- IPv6 オーバーレイ トンネルで使用されるトンネル インターフェイス タイプの場合、インターフェイス ID は、識別子の上位 32 ビットがすべてゼロであるトンネル インターフェイスに割り当てられた IPv4 アドレスです。

（注） PPP（ポイントツーポイントプロトコル）を使用するインターフェイスの場合は、接続の両端のインターフェイスが同じMACアドレスを持つため、接続の両端のインターフェイスIDが、両方の ID が一意となるまでネゴシエートされます（ランダムに選択され、必要に応じて再構築されます）。ルータの最初のMACアドレスが、PPPを使用するインターフェイスのIDとして使用されます。

ルータに IEEE 802 インターフェイス タイプがない場合は、ルータのインターフェイスでリンクローカル IPv6 アドレスが次のシーケンスで生成されます。

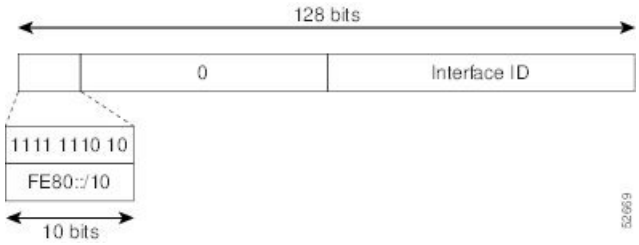
1. ルータに MAC アドレスが（ルータの MAC アドレス プールから）照会されます。
2. 使用可能な MAC アドレスがルータにない場合は、ルータのシリアル番号を使用してリンクローカル アドレスが作成されます。
3. リンクローカル アドレスの作成にルータのシリアル番号を使用できない場合、ルータは MD5 ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

リンクローカル アドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコル（NDP）で使用されます。ローカル リンク上のノードは、リンクローカル アドレスを使用して通信できます。ノードの通信にグローバルに一意のアドレスは不要です。次の図は、以下のリンクローカル アドレスの構造を示しています。

IPv6 ルータは、送信元または宛先がリンクローカル アドレスであるパケットを他のリンクに転送できません。

図 *2:* リンクローカル アドレス形式

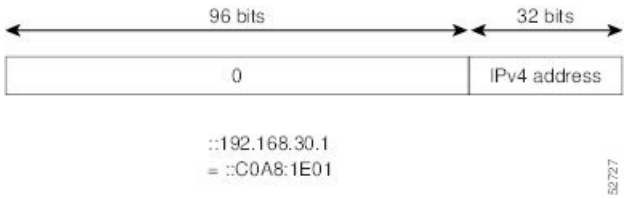


IPv4 互換 IPv6 アドレス

IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットがゼロであり、アドレスの下位 32 ビットが IPv4 アドレスである IPv6 ユニキャスト アドレスです。IPv4 互換 IPv6 アドレスの形式は、0:0:0:0:0:0:A.B.C.D または ::A.B.C.D です。IPv4 互換 IPv6 アドレスの 128 ビット全体がノードの IPv6 アドレスとして使用され、下位 32 ビットに埋め込まれた IPv4 アドレスがノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 と IPv6 の両方のプロトコル

スタックをサポートするノードに割り当てられ、自動トンネルで使用されます。次の図に、IPv4 互換 IPv6 アドレスの構造と、許容されるいくつかのアドレス形式を示します。

図 *3: IPv4* 互換 *IPv6* アドレス形式



ユニーク ローカル アドレス

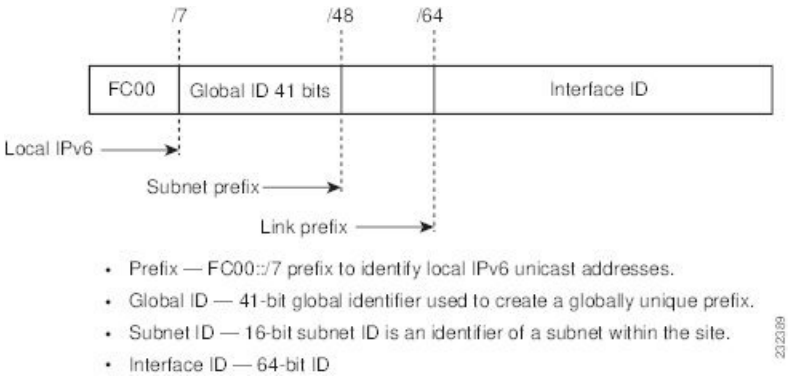
一意のローカル アドレスは、グローバルに一意であり、ローカル通信を目的とした IPv6 ユニキャスト アドレスです。グローバルなインターネット上でのルーティングには対応しておらず、サイトなどの限られたエリア内だけでルーティング可能です。限られた複数のサイト間もルーティングできる場合もあります。アプリケーションは、ユニーク ローカル アドレスをグローバル スコープのアドレスのように扱うことができます。

一意のローカル アドレスには、次の特性があります。

- グローバルに一意のプレフィックスを持っている（一意である可能性が大）。
- 既知のプレフィックスがあるため、サイト境界で簡単にフィルタリングできる。
- アドレス競合を発生させたり、これらのプレフィックスを使用するインターフェイスのリナンバリングを必要としたりすることなく、サイトを結合またはプライベートに相互接続できる。
- ISP に依存せず、永続的または断続的なインターネット接続がなくてもサイト内での通信に使用できる。
- ルーティングやドメイン ネーム サーバ（DNS）を通して誤ってサイト外に漏れても、他のどのアドレスとも競合しない。

次の図に、一意のローカル アドレスの構造を示します。

図 *4:* ユニーク ローカル アドレスの構造



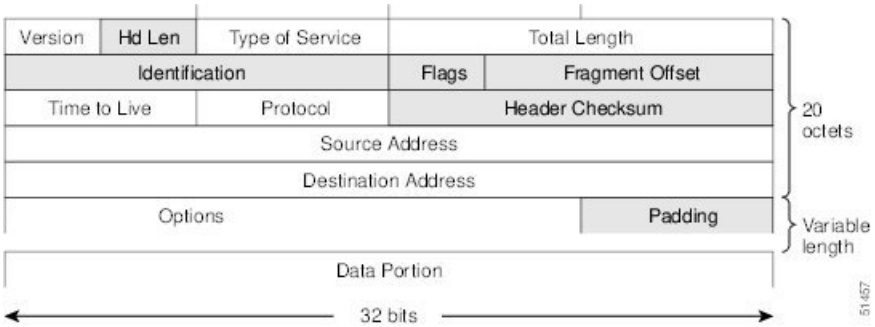
サイトローカル アドレス

RFC 3879 によりサイトローカル アドレスの使用が廃止されたため、プライベート IPv6 アドレスの設定時には、RFC 4193 で推奨されるユニーク ローカル アドレス（UCA）を使用する必要があります。

IPv4 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（以下の図を参照）。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。IPv4 パケット ヘッダーのグレーの部分のフィールドは、IPv6 パケット ヘッダーに含まれません。

図 *5 : IPv4* パケット ヘッダー形式



簡易 IPv6 パケット ヘッダー

base 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 のフィールドがあります（次の図を参照）。フラグメンテーションはパケットの送信元により処理され、データリンク層のチェックサムとトランスポート層が使用されます。ユーザ データグラム プロトコル（UDP）チェックサムにより、内部パケットと基本 IPv6 パケット ヘッダーの整合性がチェックされ、オプション フィールドが 64 ビットに揃えられるため、IPv6 パケットの処理が容易になります。

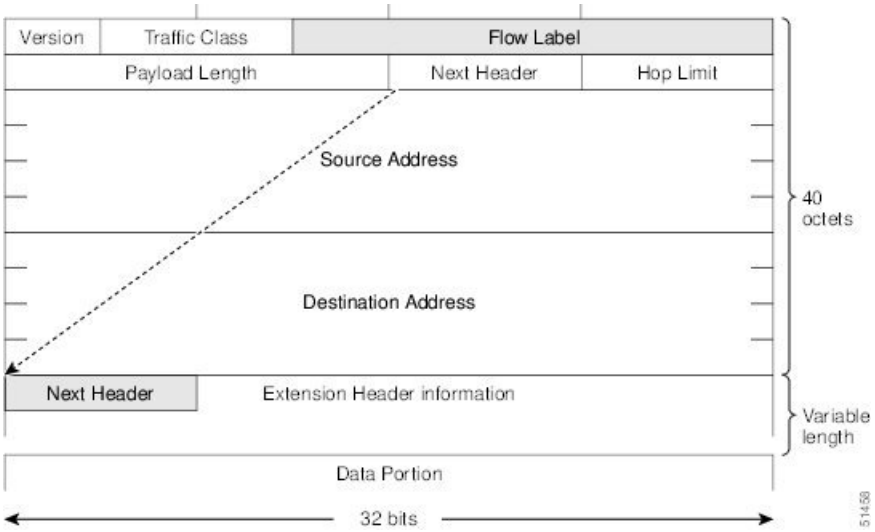
次の表に、基本 IPv6 パケット ヘッダーのフィールドをリストします。

表 *2 :* 表 *3-2* 基本 *IPv6* パケット ヘッダーのフィールド

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。

フィールド	説明
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 ヘッダーの新規フィールドです。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。
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、次の図に示すように、TCP パケット、UDP パケット、または拡張ヘッダーなどのトランスポート層パケットです。
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ルータの最大数です。各ルータを通過するたびに、この値が 1 つずつ減少します。IPv6 ヘッダーにはチェックサムがないため、ルータ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。

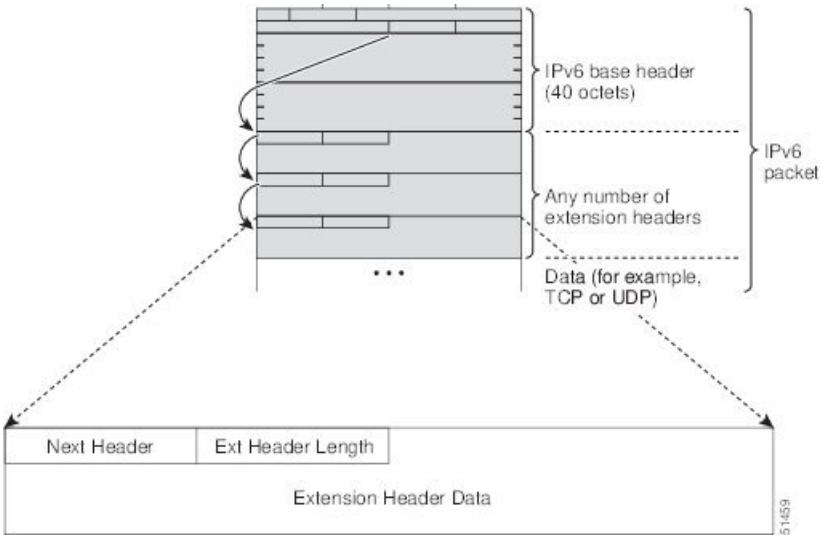
図 *6 : IPv6* パケット ヘッダー形式



IPv6 拡張ヘッダー

任意に使用できる拡張ヘッダーおよびパケットのデータ部分は、基本 IPv6 パケット ヘッダーの 8 つのフィールドのあとに続きます。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。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。次の図は、IPv6 拡張ヘッダーの形式を示しています。

図 *7 : 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	パケットのパス上のすべてのホップで処理されるヘッダー。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	任意のホップバイホップ オプション ヘッダーのあとに続くことのあるヘッダー。このヘッダーは、最終の宛先、およびルーティング ヘッダーで指定された各通過アドレスで処理されます。または、接続先オプション ヘッダーを任意のカプセル化セキュリティ ペイロード（ESP）ヘッダーの後に続けることができます。接続先オプション ヘッダーは、最終接続先でのみ処理されます。
ルーティング ヘッダー	43	送信元ルーティングに使用されるヘッダー。
フラグメント ヘッダー	44	送信元が、送信元と宛先の間のパスの最大伝送単位（MTU）より大きいパケットをフラグメント化するときに使用されるヘッダー。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。
上位層ヘッダー	6（TCP） 17（UDP）	データ転送のためにパケット内で使用されるヘッダー。2 つの主要なトランスポート プロトコルは TCP と UDP です。

（注） 一部のスイッチモデルは、IPv6 拡張ヘッダー タイプのサブセットのみをサポートします。次のリストに、Cisco Nexus 3600 プラットフォーム スイッチ（N3K-C36180YC-R および N3K-C3636C-R）、および N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R ライン カードを搭載した Cisco Nexus 9504 および 9508 モジュラ シャーシでサポートされる拡張ヘッダー タイプを示します。 。

サポート対象：宛先オプション（60）、ルーティング（43）、フラグメント（44）、モビリティ（135）、ホスト アイデンティティ プロトコル（HIP）（139）、シム 6（140）。

サポート対象外：ホップバイホップ オプション（0）、カプセル化セキュリティ ペイロード（50）、認証ヘッダー（51）、および試験的ヘッダー（253 および 254）。

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。必要な設定手順については、NX-OS リリース 9.3(x) 以降の『*Cisco Nexus 3600 NX-OS Security Configuration Guide*』の「Configuring an ACL for IPv6 Extension Headers」を参照してください。

IPv6 の DNS

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 タイプは IPv6 アドレスをサポートしています（次の表を参照）。

（注） 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。

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（**Format**）
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）。	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

IPv6 のパス MTU ディスカバリ

IPv4 の場合と同様に、ホストがダイナミックに、データ パス上のすべてのリンクの MTU サイズの差を検出し、それに合わせて調整できるよう、IPv6 でパス MTU ディスカバリを使用できます。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 ルータ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。ICMP の Too Big メッセージの到着によってパス MTU が削減されると、Cisco NX-OS はその低い値を保持します。この接続では、スループットを測定するためにセグメント サイズが増加することはありません。

（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 値の使用を推奨します。

CDP IPv6 アドレスのサポート

ネイバー情報機能用の Cisco Discovery Protocol（CDP）IPv6 アドレスのサポートを使用して、2 台のシスコ デバイス間で IPv6 アドレス指定情報を転送できます。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 の ICMP

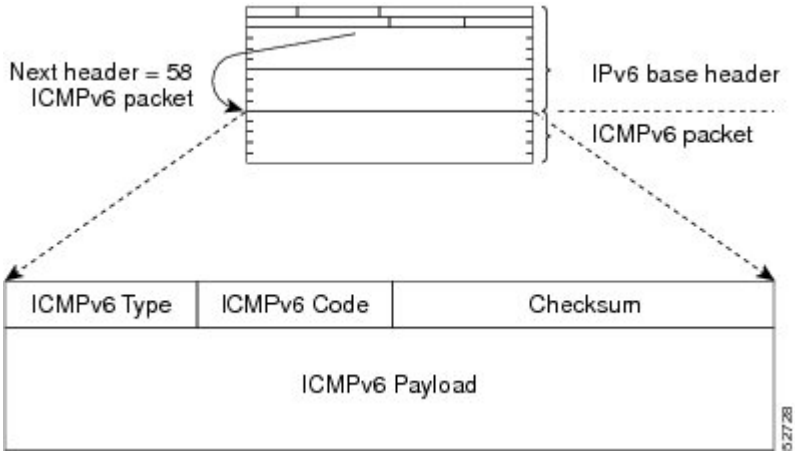
IPv6 の ICMP を使用して、ネットワークのヘルスの情報について説明します。IPv6 で動作する ICMPv6 は、パケットを正しく処理できない場合にエラーを報告し、ネットワークのステータスに関する情報メッセージを送信します。たとえば、パケットが大きすぎて別のネットワークに送信できないためにルータがパケットを転送できない場合、ルータは発信元ホストに ICMPv6 メッセージを送信します。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索およびパス MTU ディスカバリに使用されます。パス MTU ディスカバリ プロセスでは、特定のルートでサポートされる最大サイズを使用してパケットが送信されます。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値が 58 の場合は、IPv6 ICMP パケットであることを意味します。ICMP パケットは、すべての拡張ヘッダーの後に続き、IPv6 パケットの最後の情報です。IPv6 ICMP パケット内の [ICMPv6 タイプ（ICMPv6 Type）] フィールドと [ICMPv6 コード（ICMPv6 Code）] フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を識別します。[チェックサム（ Checksum ）] フィールドの値は、送信側で計算され、IPv6 ICMP パケットと IPv6 疑似ヘッダーのフィールドから受信者によって確認されます。

（注） IPv6 ヘッダーにはチェックサムがありません。ただし、トランスポート層上のチェックサムにより、パケットが正しく配信されていないかどうかを判定できます。計算に IP アドレスを含むすべてのチェックサム計算は、新しい 128 ビット アドレスに対応するように IPv6 用に変更する必要があります。チェックサムは、疑似ヘッダーを使用して生成されます。

ICMPv6 ペイロード 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。次の図は、IPv6 ICMP パケット ヘッダーの形式を示しています。

図 *8 : IPv6 ICMP* パケット ヘッダーの形式



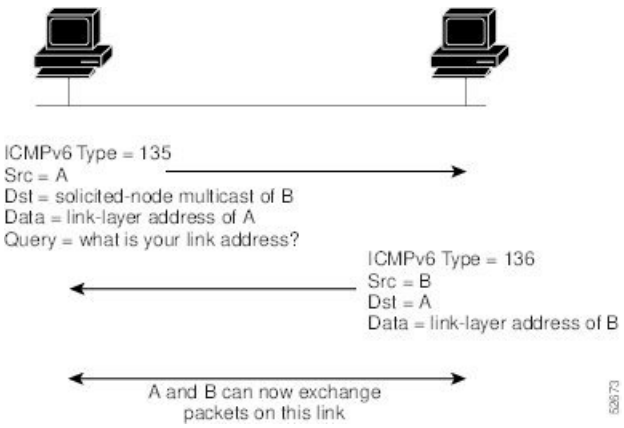
IPv6 ネイバー探索

IPv6 ネイバー探索プロトコル（NDP）を使用して、ネイバー ルータが到達可能かどうかを判断できます。IPv6 ノードは、ネイバー探索を使用して、同じネットワーク（ローカル リンク）上のノードのアドレスを決定し、パケットを転送できるネイバー ルータを見つけ、ネイバー ルータが到達可能かどうかを確認し、リンク層アドレスの変更を検出します。NDP は、ICMP メッセージを使用して、到達不能な隣接ルータにパケットが送信されたかどうかを検出します。

IPv6 ネイバー送信要求メッセージ

ノードは、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決定するときに、ICMP パケット ヘッダーのタイプ フィールドの値が 135 であるネイバー送信要求メッセージをローカル リンクで送信します（次の図を参照）。送信元アドレスは、ネイバー送信要求メッセージを送信するノードの IPv6 アドレスです。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 *9 : 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。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（ノード インターフェイスの IPv6 アドレス）です。宛先アドレスは、ネイバー送信要求メッセージを送信するノードの IPv6 アドレスです。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、ノードがネイバーのリンク層アドレスを識別した後に、ネイバーの到達可能性を確認できます。ノードがあるネイバーの到達可能性を検証する場合、そのネイバーのユニキャストアドレスとして、ネイバー送信要求メッセージ内の宛先アドレスを使用します。

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。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（ホストまたはルータ）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。肯定確認応答（TCP などの上位層プロトコルからの）は、接続が順調に進んでいる（接続先に到達しつつある）ことを示します。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。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 ルータ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。

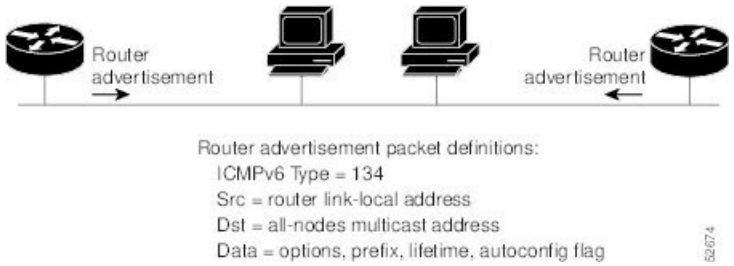
（注） 送信要求フラグが値 0 に設定されたネイバー アドバタイズメント メッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

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 ルータの構成済みの各インターフェイスへ定期的に送信されます。

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（以下の図を参照）。

図 *10 : IPv6* ネイバー検出：*RA* メッセージ



RA メッセージには、通常次の情報が含まれています。

- 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
- 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、および、その場合は、ルータがデフォルト ルータとして使用される秒単位の時間）
- 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応答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。通常、送信元アドレスは未指定の 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。宛先アドレスは、リンク範囲の全ルータ マルチキャスト アドレス。ルータ送信

要求に応答してRAが送信される場合、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 パラメータを構成できます。

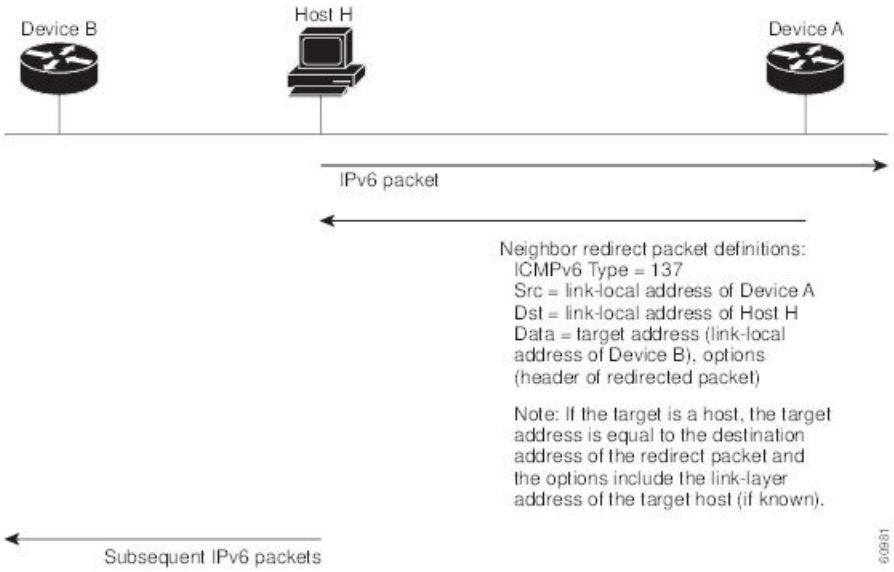
- RA メッセージの定期的な時間間隔
- （特定のリンク上のすべてのノードで使用される）デフォルト ルータとしてのルータの実用性を示す「ルータ ライフタイム」値
- 特定のリンクで使用されているネットワーク プレフィックス
- （特定のリンクで）ネイバー送信要求メッセージが再送信される時間の間隔
- ノードによってネイバーが到達可能である（特定のリンク上のすべてのノードで使用できる）と見なされるまでの時間

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、イーサネットとインターフェイス上では自動的にイネーブルになります。他のインターフェイス タイプの場合は、**no ipv6 nd suppress-ra** コマンドを入力して RA メッセージを送信する必要があります。個々のインターフェイスでは、**ipv6 nd suppress-ra** コマンドを入力して、RA メッセージ機能を無効にできます。

IPv6 ネイバー リダイレクト メッセージ

ルータは、ネイバー リダイレクト メッセージを送信して、接続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）。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。

図 *11 : 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）によって隣接ルータのリンクローカル アドレスが確実に識別されるように、ルータは各隣接ルータのリンクローカル アドレスを判断できる必要があります。静的ルーティングの場合は、ルータのリンクローカル アドレスを使用してネクストホップ ルータのアドレスを指定する必要があります。動的ルーティングの場合、隣接ルータのリンクローカルアドレスを交換するように、すべてのIPv6ルーティング プロトコルを構成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、ルータはパケットの送信元にリダイレクト メッセージを送信します。

- 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。
- パケットがルータ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。
- ルータが、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。

仮想化のサポート

IPv6 は、仮想ルーティング/転送（VRF）インスタンスをサポートします。

ECMP を使用した IPv6 ルート

ルートのすべてのネクストホップが収集、ドロップ、またはパントの場合、すべてのネクストホップはマルチパス ハードウェア テーブルにそのままプログラムされます。

ルートの一部のネクストホップがグリーニング、ドロップ、またはパントであり、残りのネクストホップがそうでない場合、非グリーニング、ドロップ、またはパントのネクストホップのみがマルチパス ハードウェア テーブルにプログラムされます。

ECMPルートの特定のネクストホップが解決されると（ARP/IPV6 NDが解決されると）、それに応じてマルチパス ハードウェア テーブルが更新されます。

IPv6の前提条件

IPv6 には、次の前提条件があります。

- IPv6 アドレッシング、IPv6 ヘッダー情報、ICMPv6、IPv6 Neighbor Discovery（ND）プロトコルなど、IPv6 の基本を理解している必要があります。

- デバイスをデュアルスタック デバイス（IPv4/IPv6）にする場合は、必ずメモリ/処理の注意事項に従ってください。

IPv6 の注意事項および制約事項

IPv6 設定時の注意事項および制約事項は、次のとおりです。

- 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。IPv6 ホストは、レイヤ 2 LAN スイッチに直接接続できます。
- インターフェイスの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。ただし、1 つのインターフェイス上での複数の IPv6 リンクローカル アドレスはサポートされません。
- RFC 3879 によりサイトローカル アドレスの使用が廃止されたため、RFC 4193 のユニークローカル アドレス（UCA）の推奨に従って、プライベート IPv6 アドレスを設定する必要があります。
- Cisco Nexus 3600-R プラットフォーム スイッチの場合、インターネット ピアリング モードは、グローバル インターネット ルーティング テーブルで配信されるプレフィックス パターンでのみ使用されます。このモードでは、他のプレフィックス配布またはパターンは動作できますが、予測できません。その結果、プレフィックス パターンが実際のインターネット プレフィックス パターンである場合にのみ、達成可能な最大 LPM/LEM スケールが信頼できます。インターネット ピアリング モードでは、グローバル インターネット ルーティング テーブル内のルート プレフィックス パターン以外のルート プレフィックス パターンが使用されている場合、スイッチは文書化されたスケーラビリティの数値を正常に達成できない可能性があります。

デフォルト設定

次の表に、IPv6 パラメータのデフォルト設定を示します。

表 *5:* デフォルト *IPv6* パラメータ

パラメータ	デフォルト
ND reachable time	0 ミリ秒
ネイバー要求再送信間隔	1000 ミリ秒

IPv6 の設定

IPv6 アドレッシングの設定

インターフェイスの IPv6 アドレスを設定して、インターフェイスが IPv6 トラフィックを転送できるようにします。インターフェイスでグローバル IPv6 アドレスを設定すると、リンクローカル アドレスが自動的に設定され、そのインターフェイスで IPv6 が有効となります。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3.
4. （任意） **show ipv6 interface**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet number**
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3		

オプション	説明
コマンド	目的
ipv6 address { *addr* [**eui64**] [**route-preference** *preference*] [**secondary**] **tag** *tag-id*]	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。 **ipv6 address** コマンドを入力すると、IPv6 アドレスの下位 64 ビットにインターフェイス ID を含む

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td>
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td></td><td>グローバル IPv6 アドレスが設定されます。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。</td></tr>
<tr><td>ipv6 address ipv6-address use-link-local-only</td><td>ipv6 address use-link-local-only コマンドを入力すると、インターフェイスのリンクローカル アドレスが設定されます。このアドレスは、IPv6 がインターフェイスでイネーブルになっているとき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ます。

このコマンドは、IPv6 アドレスを設定せずに、インターフェイス上で IPv6 処理をイネーブルにします。</td></tr>
</table>
例：
<code>switch(config-if)# ipv6 address 2001:0DB8::1/10</code>
または
<code>switch(config-if)# ipv6 address use-link-local-only</code>
</td><td></td></tr>
<tr><td>ステップ 4</td><td>（任意） show ipv6 interface
例：
<code>switch(config-if)# show ipv6 interface</code></td><td>IPv6 用に設定されたインターフェイスを表示します。</td></tr>
<tr><td>ステップ 5</td><td>（任意） copy running-config startup-config
例：
<code>switch(config-if)# copy running-config startup-config</code></td><td>この設定変更を保存します。</td></tr>
</table>

例

次に、IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# ipv6 address ?
A:B::C:D/LEN IPv6 prefix format: xxxx:xxxx/ml, xxxx:xxxx::/ml,
xxxx::xx/128
use-link-local-only Enable IPv6 on interface using only a single link-local
address
switch(config-if)# ipv6 address 2001:db8::/64 eui64
```

次に、IPv6 インターフェイスを表示する例を示します。

```
switch(config-if)# show ipv6 interface ethernet 3/1
Ethernet3/1, Interface status: protocol-down/link-down/admin-down, iod: 36
IPv6 address: 0dc3:0dc3:0000:0000:0218:baff:fed8:239d
IPv6 subnet: 0dc3:0dc3:0000:0000:0000:0000:0000:0000/64
IPv6 link-local address: fe80::0218:baff:fed8:239d (default)
IPv6 multicast routing: disabled
IPv6 multicast groups locally joined:
ff02::0001:ffd8:239d ff02::0002 ff02::0001 ff02::0001:ffd8:239d
IPv6 multicast (S,G) entries joined: none
IPv6 MTU: 1500 (using link MTU)
IPv6 RP inbound packet-filtering policy: none
IPv6 RP outbound packet-filtering policy: none
IPv6 inbound packet-filtering policy: none
IPv6 outbound packet-filtering policy: none
IPv6 interface statistics last reset: never
IPv6 interface RP-traffic statistics: (forwarded/originated/consumed)
Unicast packets: 0/0/0
Unicast bytes: 0/0/0
Multicast packets: 0/0/0
Multicast bytes: 0/0/0
```

LPM インターネット ピアリング ルーティング モードの設定

Cisco NX-OS リリース9.3(1) 以降では、IPv4 および IPv6 LPM インターネット ルート エントリをサポートするために LPM インターネット ピアリング ルーティング モードを設定できます。このモードは、IPv4 プレフィックス（/32 までのプレフィックス長）および IPv6 プレフィックス（/83 までのプレフィックス長）のダイナミック トライ（ツリー ビット ルックアップ）をサポートします。このルーティング モードをサポートするのは、Cisco Nexus 3600-R プラットフォーム スイッチです。

（注） この設定は、IPv4 および IPv6 両方のアドレス ファミリに影響を及ぼします。

（注） LPM インターネット ピアリング ルーティング モードのスケール数については、『Cisco Nexus 3600 Series NX-OS Verified Scalability Guide』を参照してください。LPM インターネット ピアリング モードの Cisco Nexus 3600-R プラットフォーム スイッチは、インターネット ピアリング プレフィックスを使用する場合にのみ、予測どおりにスケールアウトします。Cisco Nexus 3600-R プラットフォーム スイッチが他のプレフィックス パターンを使用している場合は、文書化されたスケーラビリティの数値を達成できない可能性があります。

手順の概要

1. **configure terminal**
2. [**no**] **system routing template-internet-peering**
3. （任意） **show system routing mode**
4. **copy running-config startup-config**
5. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **system routing template-internet-peering** 例： `switch(config)# system routing template-internet-peering`	デバイスを LPM インターネット ピア ルーティング モードにして、IPv4 および IPv6 LPMインターネット ルート エントリをサポートします。

ステップ 3	（任意） **show system routing mode**
	例：
	`switch(config)# show system routing mode`
	`Configured System Routing Mode: Internet Peering`
	`Applied System Routing Mode: Internet Peering`
		LPM ルーティング モードを表示します。

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。
ステップ 5	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

LPM インターネット ピアリング ルーティング モードの追加設定

大規模ルーティング環境でLPMインターネット ピアリング ルーティング モードでCisco Nexusスイッチを導入する場合、またはネクストホップ数が増加するルートの場合は、VDC リソース テンプレートで IPv4 のメモリ制限を増やす必要があります。

手順の概要

1. **configure terminal**

2. （任意） **show routing ipv4 memory estimate routes routes next-hops hops**
3. **vdc switch id id**
4. **limit-resource u4route-mem minimum min-limit maximum max-limit**
5. **exit**
6. **copy running-config startup-config**
7. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	（任意） **show routing ipv4 memory estimate routes routes next-hops hops**
	例：
	`switch(config)# show routing ipv4 memory estimate routes 262144 next-hops 32`
	`Shared memory estimates:`
	`Current max 512 MB; 78438 routes with 64 nhs`
	`in-use 2 MB; 2642 routes with 1 nhs (average)`
	`Configured max 512 MB; 78438 routes with 64 nhs`
	`Estimate memory with fixed overhead: 1007 MB; 262144 routes with 32 nhs`
	`Estimate with variable overhead included:`
	`- With MVPN enabled VRF: 1136 MB`
	`- With OSPF route (PE-CE protocol): 1375 MB`
	`- With EIGRP route (PE-CE protocol): 1651 M`
		共有メモリの見積もりを表示して、ルートのメモリ要件を判断します。

ステップ 3	**vdc switch id id**
	例：
	`switch(config)# vdc switch id 1`
	`switch(config-vdc)#`
		VDC スイッチ ID を指定します。

ステップ 4	**limit-resource u4route-mem minimum min-limit maximum max-limit** 例： `switch(config-vdc)# limit-resource u4route-mem minimum 1024 maximum 1024`	IPv4 メモリの制限をメガバイト単位で指定します。

ステップ 5	**exit**
	例：
	`switch(config-vdc)# exit`
	`switch(config)#`
		VDC 設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。
ステップ 7	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

IPv6 ネイバー探索の構成

ルータで IPv6 ネイバー探索を構成できます。NDP は、IPv6 ノードとルータを有効にして、同じリンク上のネイバーのリンク層アドレスを特定し、隣接ルータを見つけ、ネイバーの動向を把握します。

始める前に

最初にインターフェイスで IPv6 を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **ipv6 nd** [**hop-limit** *hop-limit* | **managed-config-flag** | **mtu** *mtu* | **ns-interval** *interval* | **other-config-flag** | **prefix** | **ra-interval** *interval* | **ra-lifetime** *lifetime* | **reachable-time** *time* | **redirects** | **retrans-timer** *time* | **suppress-ra**]
4. （任意） **show ipv6 nd interface**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet number**
	例：
	`switch(config)# interface ethernet 2/31`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 nd** [**hop-limit** *hop-limit* | **managed-config-flag** | **mtu** *mtu* | **ns-interval** *interval* | **other-config-flag** | **prefix** | **ra-interval** *interval* | **ra-lifetime** *lifetime* | **reachable-time** *time* | **redirects** | **retrans-timer** *time* | **suppress-ra**] 例： `switch(config-if)# ipv6 nd prefix`	IPv6 アドレスを設定する場合は、ネイバー探索が自動的に有効になります。このコマンドにより、インターフェイスで次の追加の IPv6 ネイバー探索オプションが有効になります。 • **hop-limit** *hop-limit*：IPv6 ネイバー検出パケットでホップ リミットをアドバタイズします。値の範囲は 0 ～ 255 です。 • **managed-config-flag**：ステートフル アドレス自動構成を使用してアドレス情報を取得するために、ICMPv6 ルータ アドバタイズメント メッセージ内でアドバタイズします。 • **mtu** *mtu*：このリンク上で ICMPv6 ルータ アドバタイズメント メッセージで最大伝送単位（MTU）をアドバタイズします。範囲は 1280 ～ 65535 バイトです。 • **ns-interval** *interval*：IPv6 ネイバー送信要求メッセージ間の再送信間隔を構成します。範囲は 1000 ～ 3600000 ミリ秒です。 • **other-config-flag**：ICMPv6 ルータ アドバタイズメント メッセージで、ホストがアドレス以外の関連情報を取得するためにステートフル自動構成を使用することを示します。 • **prefix**：ルータ アドバタイズメント メッセージで IPv6 プレフィックスをアドバタイズします。 • **ra-interval** *interval*：ICMPv6 ルータ アドバタイズメント メッセージの送信間の間隔を構成します。範囲は 4 ～ 1800 秒です。 • **ra-lifetime** *lifetime*：ICMPv6 ルータ アドバタイズメント メッセージで、デフォルト ルータのライフタイムをアドバタイズします。範囲は 0 ～ 9000 秒です。 • **reachable-time** *time*：ICMPv6 ルータ アドバタイズメント メッセージで、ノードが到達可能性確認を受信したあとにネイバーをアップしていると見なした時間をアドバタイズします。範囲は 0 ～ 9000 秒です。 • **redirects**：ICMPv6 リダイレクト メッセージの送信を有効化します。

	コマンドまたはアクション	目的
		• **retrans-timer** *time*：ICMPv6 ルータ アドバタイズメントメッセージで、ネイバー送信要求メッセージ間の時間をアドバタイズします。範囲は 0 ～ 9000 秒です。 • **suppress-ra**：ICMPv6 ルータ アドバタイズメント メッセージの送信を無効にします。
ステップ 4	（任意） **show ipv6 nd interface** 例： `switch(config-if)# show ipv6 nd interface`	IPv6 ネイバー検出に構成されたインターフェイスを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

例

次に、IPv6 ネイバー探索到達可能時間を構成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# ipv6 nd reachable-time 10
```

次に、IPv6 ネイバー探索インターフェイスを表示する例を示します。

```
switch(config-if)# show ipv6 nd interface ethernet 3/1
ICMPv6 ND Interfaces for VRF "default"
Ethernet3/1, Interface status: protocol-down/link-down/admin-down
IPv6 address: 0dc3:0dc3:0000:0000:0218:baff:fed8:239d
ICMPv6 active timers:
Last Neighbor-Solicitation sent: never
Last Neighbor-Advertisement sent: never
Last Router-Advertisement sent:never
Next Router-Advertisement sent in: 0.000000
Router-Advertisement parameters:
Periodic interval: 200 to 600 seconds
Send "Managed Address Configuration" flag: false
Send "Other Stateful Configuration" flag: false
Send "Current Hop Limit" field: 64
Send "MTU" option value: 1500
Send "Router Lifetime" field: 1800 secs
Send "Reachable Time" field: 10 ms
Send "Retrans Timer" field: 0 ms
Neighbor-Solicitation parameters:
NS retransmit interval: 1000 ms
ICMPv6 error message parameters:
Send redirects: false
Send unreachables: false
```

オプションの IPv6 ネイバー探索

次のオプションの IPv6 ネイバー探索コマンドを使用できます。

コマンド	目的
ipv6 nd hop-limit	ルータ アドバタイズメントおよびルータから発信されるすべての IPv6 パケットで使用されるホップの最大数を構成します。
ipv6 nd managed-config-flag	「managed address configuration flag」フラグは、IPv6 ルータ アドバタイズメントで設定されません。
ipv6 nd mtu	各インターフェイスにおいて送信される IPv6 パケットの最大伝送単位（MTU）サイズを設定します。
ipv6 nd ns-interval	インターフェイスで IPv6 ネイバー再送信要求メッセージが送信される時間間隔を設定します。
ipv6 nd other-config-flag	IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを構成します。
ipv6 nd ra-interval	インターフェイスで IPv6 ルータ アドバタイズメント（RA）メッセージが送信される時間間隔を構成します。
ipv6 nd ra-lifetime	インターフェイス上の IPv6 ルータ アドバタイズメントに含まれるルータのライフタイム値を構成します。
ipv6 nd reachable-time	到達可能性確認イベントがいくつか発生した後、リモート IPv6 ノードが到達可能と見なされる時間を構成します。
ipv6 nd redirects	ICMPv6 リダイレクト メッセージの送信を有効にします。
ipv6 nd retrans-timer	ルータ アドバタイズメントのネイバー送信要求メッセージ間のアドバタイズ時間を構成します。
ipv6 nd suppress-ra	LAN インターフェイス上で IPv6 ルータ アドバタイズメントの送信を抑制します。

IPv6 パケット検証の構成

Cisco NX-OS は、IPv6 パケットの検証をチェックする侵入検知システム（IDS）をサポートしています。これらの IDS チェックは有効または無効にできます。

（注） Cisco Nexus 3600 プラットフォーム スイッチは、送信元 IP アドレスが 0.0.0.0 のパケットを除外しません。

IDS チェックを有効にするには、グローバル構成モードで次のコマンドを使用します。

コマンド	目的
hardware ip verify address { **destination zero** | **identical** | **reserved** | **source multicast** }	IPv6 アドレスに対して次の IDS チェックを実行します。 • **destination zero**：宛先 IP アドレスが :: である場合は IPv6 パケットをドロップします。 • **identical**：送信元 IPv6 アドレスが宛先 IPv6 アドレスと同じである場合は IPv6 パケットをドロップします。 • **reserved**：IPv6 アドレスが ::1 である場合は、IPv6 パケットをドロップします。 • **source multicast**：送信元 IPv6 アドレスが FF00::/8 の範囲内（マルチキャスト）である場合は IPv6 パケットをドロップします。
hardware ipv6 verify length { **consistent** | **maximum** { max-frag | **max-tcp** | **udp** }}	IPv6 アドレスに対して次の IDS チェックを実行します。 • **consistent** ：イーサネット フレーム サイズが、IPv6 パケット長にイーサネット ヘッダーを加えた値以上の場合には、IPv6 パケットをドロップします。 • **maximum max-frag**：計算式（IPv6 ペイロード長 - IPv6 拡張ヘッダー バイト数）+（フラグメント オフセット * 8）の値が 65536 より大きい場合には、IPv6 パケットをドロップします。 • **maximum max-tcp**：TCP 長が IP ペイロード長より長い場合は、IP パケットをドロップします。 • **maximum udp**：IPv6 ペイロード長が UDP パケット長を下回る場合には、IPv6 パケットをドロップします。
hardware ipv6 verify tcp tiny-frag	IPv6 フラグメント オフセットが 1 の場合、または IPv6 フラグメント オフセットが 0 で IP ペイロード長が 16 未満の場合、TCP パケットをドロップします。
hardware ipv6 verify version	EtherType が 6（IPv6）に設定されていない場合、IPv6 パケットをドロップします。

IPv6 パケット検証の構成を表示するには、**show hardware forwarding ip verify** コマンドを使用します。

IPv6 設定の確認

IPv6 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hardware forwarding ip verify	IPv4 および IPv6 パケット検証の構成を表示します。
show ipv6 interface	IPv6-related インターフェイスの情報を表示します。
show ipv6 adjacency	隣接関係テーブルを表示します。
show ipv6 icmp	ICMPv6 情報を表示します。
show ipv6 nd	IPv6 ネイバー探索インターフェイス情報を表示します。
show ipv6 neighbor	IPv6 ネイバー エントリを表示します。

IPv6 の設定例

次に、IPv6 を構成する例を示します。

```
configure terminal
interface ethernet 3/1
ipv6 address 2001:db8::/64 eui64
ipv6 nd reachable-time 10
```

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