



IPv6 の設定

この章では、Cisco NX-OS デバイス上で、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)、およびインターネット制御メッセージプロトコルバージョン 6 (ICMPv6) を設定する方法について説明します。

この章では、次の内容について説明します。

- 「IPv6 について」 (P.3-1)
- 「IPv6 のライセンス要件」 (P.3-16)
- 「IPv6 の前提条件」 (P.3-16)
- 「IPv6 の注意事項および制約事項」 (P.3-16)
- 「デフォルト設定」 (P.3-16)
- 「IPv6 の設定」 (P.3-17)
- 「IPv6 コンフィギュレーションの確認」 (P.3-23)
- 「IPv6 の設定例」 (P.3-23)
- 「その他の関連資料」 (P.3-24)

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、ネットワークの拡張が可能となり、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 フォーマットにより、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和、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 Network Address Translation (NAT; ネットワーク アドレス変換) 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有効になります。

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 の Open Shortest Path First (OSPF) およびマルチプロトコル 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。

ここでは、次の内容について説明します。

- 「IPv6 アドレス フォーマット」 (P.3-2)
- 「IPv6 ユニキャスト アドレス」 (P.3-3)
- 「IPv4 パケット ヘッダー」 (P.3-7)
- 「IPv4 パケット ヘッダー」 (P.3-7)
- 「簡易 IPv6 パケット ヘッダー」 (P.3-7)
- 「IPv6 の DNS」 (P.3-10)
- 「IPv6 のパス MTU 探索」 (P.3-10)
- 「CDP IPv6 アドレスのサポート」 (P.3-11)
- 「IPv6 の ICMP」 (P.3-11)
- 「IPv6 ネイバー探索」 (P.3-12)
- 「IPv6 ネイバー送信要求メッセージ」 (P.3-12)
- 「IPv6 ルータ アドバタイズメント メッセージ」 (P.3-13)
- 「IPv6 ネイバー リダイレクト メッセージ」 (P.3-15)
- 「仮想化のサポート」 (P.3-16)

IPv6 アドレス フォーマット

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 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:BA98:7654:3210
2001:0DB8:0:0:8:800:200C: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。表 3-1 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 3-1 圧縮された IPv6 アドレス フォーマット

| IPv6 アドレス タイプ | 元のフォーマット | 圧縮されたフォーマット |
|---------------|-------------------------------|--------------------------|
| 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 | FF01:0:0:0:0:0:101 | 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 3-1 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、第 1 章「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は割り当てられません。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、送信元アドレスまたは宛先アドレスに IPv6 ループバック アドレスを持つ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は割り当てられません。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、プレフィックスを構成するアドレスの上位の連続ビット（アドレスのネットワーク部分）の桁数を示す 10 進数の値です。たとえば、2001:0DB8:8086:6502::/32 は IPv6 プレフィックスとして有効です。

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宛てに送信されたパケットは、そのアドレスを持つインターフェイスに配信されます。ここでは、次の内容について説明します。

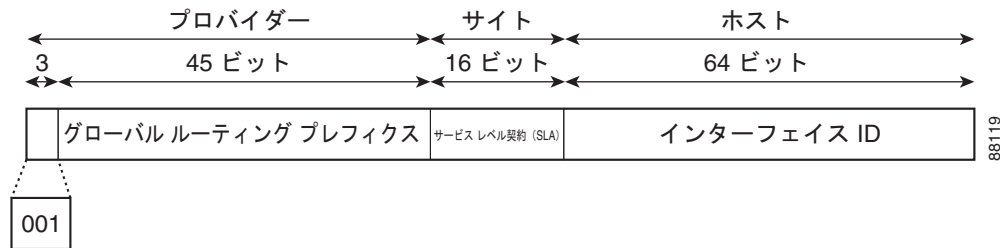
- 「集約可能グローバル アドレス」(P.3-3)
- 「リンクローカル アドレス」(P.3-5)
- 「IPv4 互換 IPv6 アドレス」(P.3-5)
- 「ユニーク ローカル アドレス」(P.3-6)
- 「サイトローカル アドレス」(P.3-7)

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となります。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せん。図 3-1 は、集約可能グローバル アドレスの構造を示します。

図 3-1 集約可能グローバルアドレスのフォーマット



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 フォーマットの 64 ビット インターフェイス ID 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 集約可能なグローバルユニキャストアドレスフォーマット文書 (RFC 2374) では、グローバルルーティングプレフィックスには、Top-Level Aggregator (TLA) および Next-Level Aggregator (NLA) という他の 2 つの階層構造のフィールドが含まれるとされていました。TLA 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。

個々の組織では、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構造を作成したり、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 のサブネットをサポートできるという点で異なります。

インターフェイス ID で、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変更済みの EUI-64 フォーマットです。

- 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。
- その他の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。ただし、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 アドレスプールからの最初の MAC アドレスが ID として使用される点が異なります (インターフェイスが MAC アドレスを持たないため)。
- 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、ID の高位 32 ビットがすべての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) ポイントツーポイント プロトコル (PPP) 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 (ルータ内の MAC アドレス プールの) が照会されます。
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 Message Digest 5 (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。

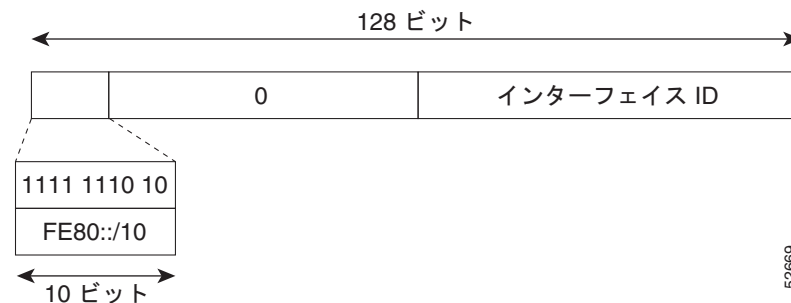
リンクローカル アドレス

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、変更済み EUI-64 フォーマットのインターフェイス ID を使用するどのインターフェイスでも自動設定が可能な IPv6 ユニキャスト アドレスです。ネイバー探索プロトコル (NDP) およびステートレス自動設定プロセスでは、リンクローカル アドレスが使用されます。ローカル リンク上のノードは、リンクローカル アドレスを使用して通信でき、通信するためにはグローバルに一意のアドレスを必要としません。

図 3-2 は、リンクローカル アドレスの構造を示します。

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 3-2 リンクローカル アドレス フォーマット

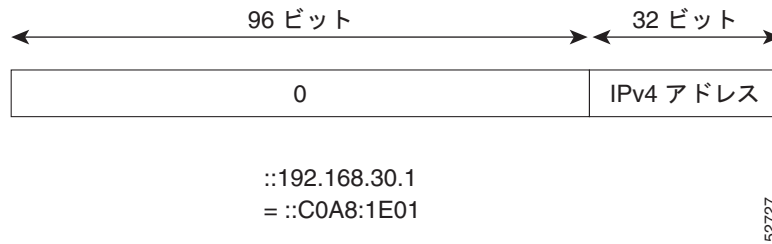


52669

IPv4 互換 IPv6 アドレス

IPv4 互換 IPv6 アドレスとは、アドレスの高位 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 アドレスのフォーマットは 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 ビット全体はノードの 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 アドレスはノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 および IPv6 の両プロトコル 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。図 3-3 は、IPv4 互換 IPv6 アドレスの構造と、許容されるアドレス フォーマットのいくつかを示します。

図 3-3 IPv4 互換 IPv6 アドレスのフォーマット



ユニーク ローカル アドレス

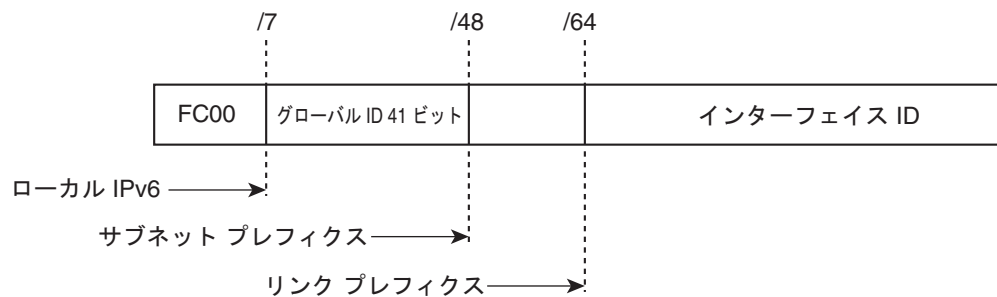
ユニーク ローカル アドレスは、グローバルに一意であり、ローカルでの通信のための IPv6 ユニキャストアドレスです。グローバルなインターネット上でのルーティングには対応しておらず、サイトなどの限られたエリア内だけでルーティング可能です。限られた複数のサイト間もルーティングできる場合もあります。アプリケーションは、ユニーク ローカル アドレスをグローバルなスコープのアドレスとして扱う場合があります。

ユニーク ローカル アドレスには次の特徴があります。

- 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）。
- 周知のプレフィックスを持つため、サイトの境界でフィルタリングが容易。
- アドレスの競合が発生せず、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再番号割り当てでも必要とせず、サイトを結合したり、プライベートに相互接続したりできる。
- ISP に依存せず、永久的または断続的なインターネット接続を使用することなく、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。

図 3-4 は、ユニーク ローカル アドレスの構造を示します。

図 3-4 ユニーク ローカル アドレスの構造



- プレフィックス：ローカル IPv6 ユニキャスト アドレスを識別するための FC00::/7 プレフィックス。
- グローバル ID：グローバルに一意なプレフィックスの作成に使用される 41 ビット グローバル ID。
- サブネット ID：16 ビット サブネット ID はサイト内のサブネットの ID。
- インターフェイス ID：64 ビット IID

232389

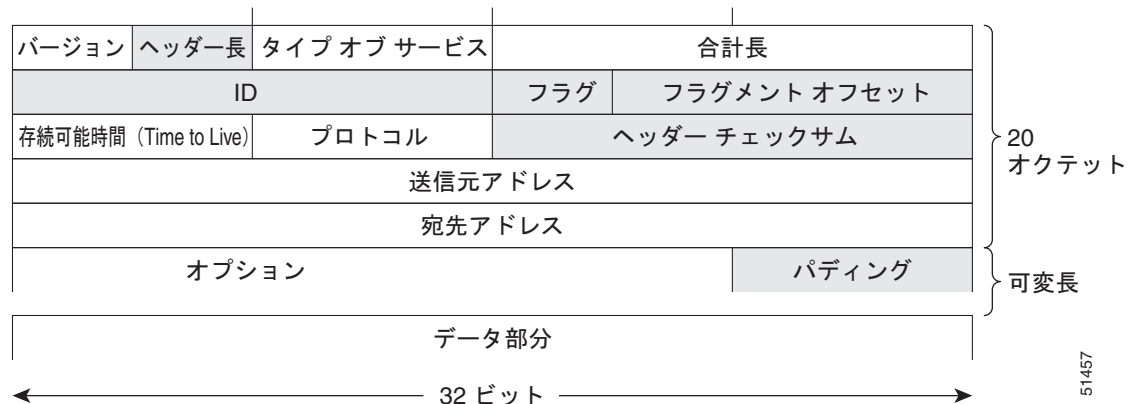
サイトローカル アドレス

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 (図 3-5 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層パケットであるデータ部分が続く場合があります。オプション フィールドの可変長部分は、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 3-5 IPv4 パケット ヘッダーのフォーマット



簡易 IPv6 パケット ヘッダー

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 (図 3-6 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。

表 3-2 は、基本 IPv6 パケット ヘッダー内のフィールドの一覧です。

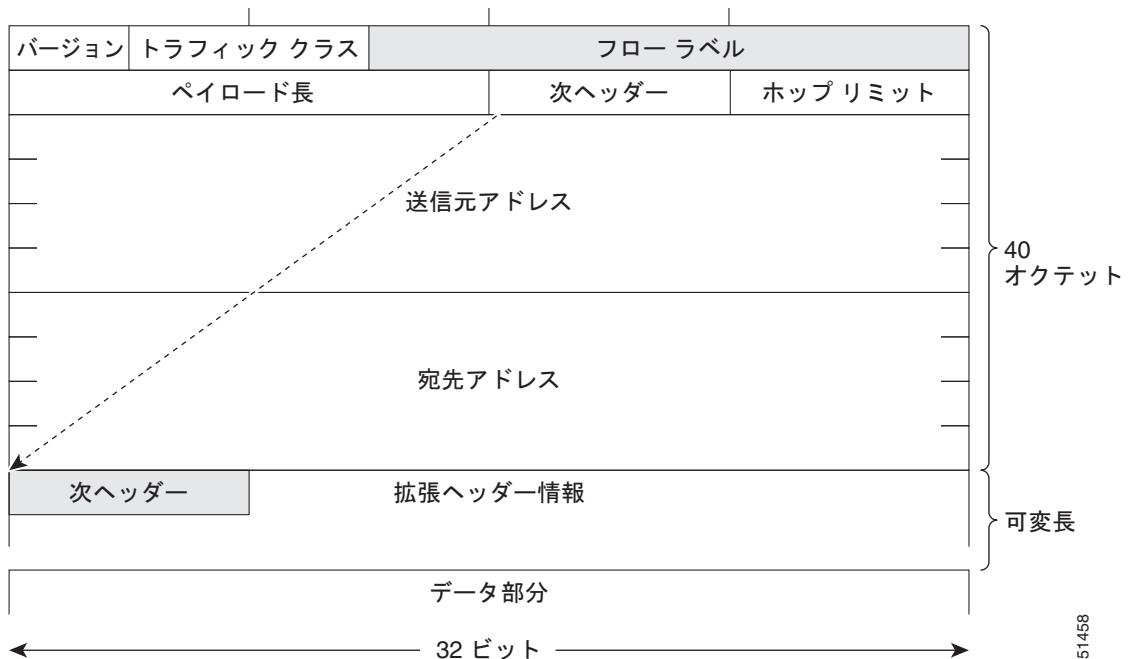
表 3-2 基本 IPv6 パケット ヘッダー フィールド

| 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 フィールドに該当します。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。 |

表 3-2 基本 IPv6 パケット ヘッダー フィールド (続き)

| フィールド | 説明 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ペイロード長 | IPv4 パケット ヘッダーのペイロード長フィールドに該当します。ペイロード長フィールドは、パケットのデータ部分の長さの合計を示します。 |
| 次ヘッダー | IPv4 パケット ヘッダーの Protocol フィールドに該当します。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、 図 3-6 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 ヘッダーの生存時間フィールドに該当します。ホップ リミット フィールドは、IPv6 パケットが無効になる前に通過できるルータの最大数を指定します。各ルータを通過するたびに、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、ルータは、値が減少するたびにチェックサムを再計算する必要がなく、処理リソースの節約となります。 |
| 送信元アドレス | IPv4 パケット ヘッダーの送信元アドレス フィールドに該当しますが、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 フィールドに該当しますが、IPv4 の 32 ビット宛先アドレスの代わりに、IPv6 では 128 ビット宛先アドレスが含まれます。 |

図 3-6 IPv6 パケット ヘッダーのフォーマット



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。拡張ヘッダーがある場合は、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決められていません。各拡張ヘッダーは、前のヘッダーの次ヘッダー フィールドに示されます。通常は、最後の拡張ヘッダーに、TCP または UDP などのトラン

スポーツ層プロトコルの次ヘッダー フィールドがあります。図 3-7 は、IPv6 拡張ヘッダーのフォーマットを示します。

図 3-7 IPv6 拡張ヘッダーのフォーマット

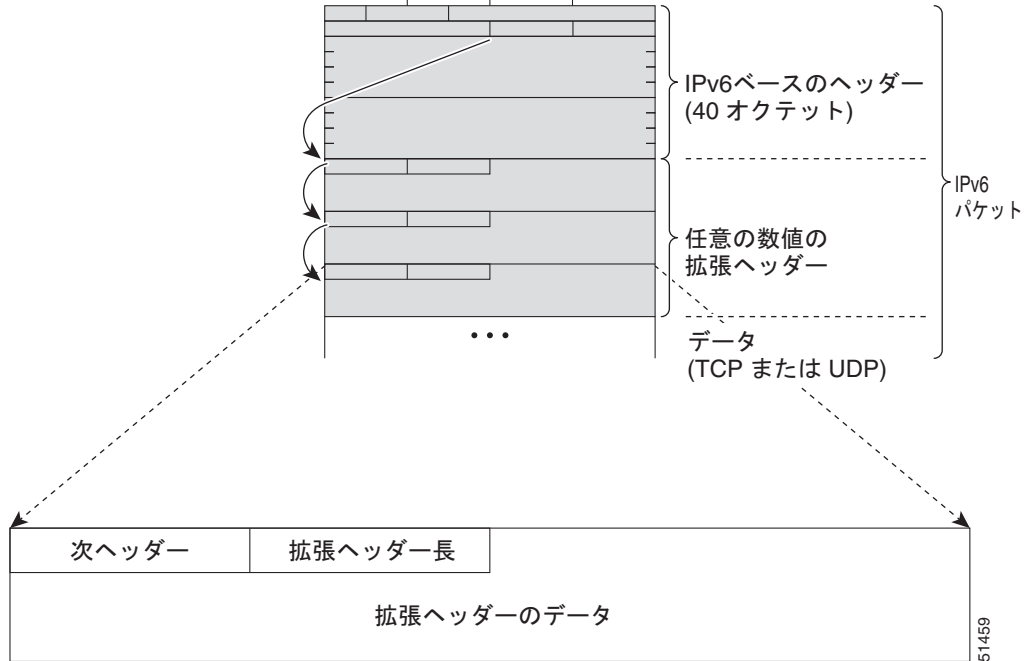


表 3-3 は、拡張ヘッダーのタイプとその次ヘッダー フィールドの値の一覧です。

表 3-3 IPv6 拡張ヘッダーのタイプ

| ヘッダーのタイプ | 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、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) ヘッダーのあとに続く場合もあります。この場合の宛先オプションヘッダーは、最終の宛先だけで処理されます。 |
| ルーティングヘッダー | 43 | 送信元のルーティングに使用されるヘッダー。 |

表 3-3 IPv6 拡張ヘッダーのタイプ (続き)

| ヘッダーのタイプ | 次ヘッダーの値 | 説明 |
|------------|-----------------------------|--------------------------------------------------------------------------------------------------|
| フラグメントヘッダー | 44 | 送信元が、送信元と宛先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 の場合) 17 (UDP の場合) | データ転送のためにパケット内で使用されるヘッダー。おもな転送プロトコルは TCP と UDP の 2 つです。 |

IPv6 の DNS

IPv6 は、DNS 名前/アドレスおよびアドレス/名前のルックアップ処理でサポートされる DNS レコードタイプをサポートしています。DNS レコードタイプは IPv6 アドレスをサポートしています (表 3-4 を参照)。



(注) IPv6 は、IPv6 アドレスから DNS 名への逆マッピングもサポートしています。

表 3-4 IPv6 DNS レコードタイプ

| レコードタイプ | 説明 | 形式 |
|---------|----------------------------------------------|----------------------------------------------------------------------------------------|
| AAAA | ホスト名を IPv6 アドレスにマッピングします (IPv4 の A レコードに該当) | 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 レコードに該当) | 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.e.f.f.3.ip6.int PTR www.abc.test |

IPv6 のパス MTU 探索

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 探索を使用できます。ただし、IPv6 では、データパス上のリンクのパス MTU が小さすぎてパケットを処理できない場合は、パケットの送信元によりフラグメンテーションが処理されます。IPv6 ホストにパケットのフラグメンテーションを処理させると、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

ネイバー情報機能向けの 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 で ICMP を使用して、ネットワークの状態に関する情報を提供できます。IPv6 で使用できるバージョンである ICMPv6 は、パケットが正しく処理されない場合にエラーを報告し、ネットワークの状態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は、ルータにより、送信元のホストに ICMPv6 メッセージが送信されます。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索およびパス MTU 探索に使用されます。パス MTU 探索処理により、パケットが確実に、特定のルートでサポートされる最大のサイズで送信されます。

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あとに続く、IPv6 パケット中の最後の情報部分です。IPv6 ICMP パケットでは、ICMPv6 タイプ フィールドと ICMPv6 コード フィールドに、ICMP メッセージ タイプなどの IPv6 ICMP パケット情報が示されます。チェックサム フィールドの値は送信側で計算され、受信側により、ICMP パケット内および IPv6 疑似ヘッダー内のフィールドでチェックされます。

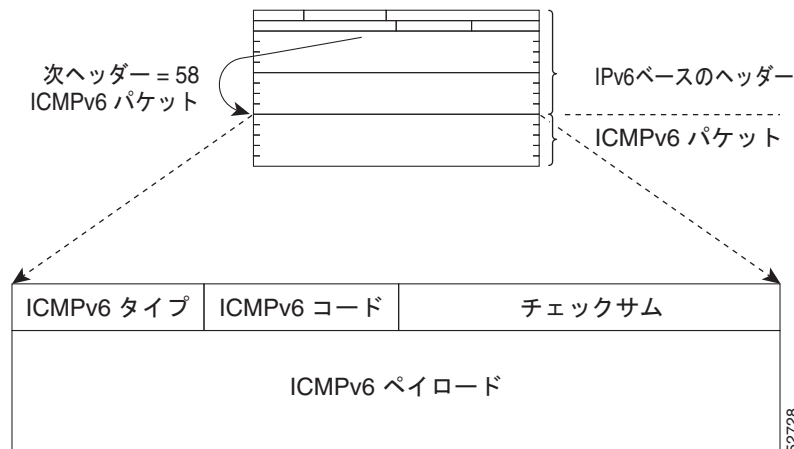


(注)

IPv6 ヘッダーには、チェックサムはありません。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 アドレスが含まれるすべてのチェックサム計算は、新しい 128 ビット アドレスを処理できるように、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。図 3-8 は、IPv6 ICMP パケット ヘッダーのフォーマットを示します。

図 3-8 IPv6 ICMP パケット ヘッダーのフォーマット



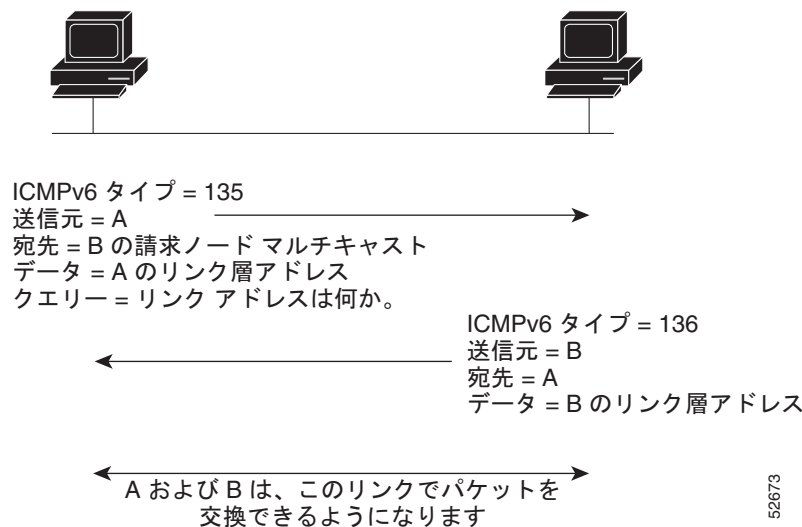
IPv6 ネイバー探索

IPv6 ネイバー探索プロトコル (NDP) を使用して、隣接ルータが到達可能かどうかを判定できます。IPv6 ノードは、ネイバー探索を使用して、同じネットワーク上のノードのアドレス (ローカルリンク) を決定します。そして、ノード自身からのパケットを転送できる隣接ルータを見つけ、その隣接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、パケットが到達不可能な隣接ルータに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 (図 3-9 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 3-9 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あとに、宛先ノードは返信として、ICMP パケットヘッダーのタイプフィールドの値が 136 のネイバー アドバタイズメントメッセージをローカルリンクで送信します。送信元アドレスは、ノードの IPv6 アドレス (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。

送信元ノードと宛先ノードが通信できるのは、送信元ノードがネイバー アドバタイズメントを受信したあとです。

ネイバー送信要求メッセージにより、ノードがネイバーのリンク層アドレスを認識したあとに、ネイバーの到達可能性が確認できます。ノードは、ネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスを、ネイバーのユニキャストアドレスとして使用します。

ローカルリンク上のノードのリンク層アドレスに変更がある場合も、ネイバー アドバタイズメントメッセージが送信されます。変更があったときのネイバー アドバタイズメントメッセージの宛先アドレスは、全ノードマルチキャストアドレスです。

ネイバー到達不能検出により、ネイバーの障害またはネイバーへの転送パスの障害が特定されます。また、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）の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だけ実行され、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、そのノードから肯定確認応答（以前にそのノード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）が返されると、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（宛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。順調に進んでいることで、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 リンクにない宛先の場合は、順調に進んでいることで、ファーストホップ ルータが到達可能であることがわかります。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、宛先へのパスがまだ機能しているかどうかを確認します。ネイバーから返信された送信要求ネイバー アドバタイズメント メッセージは、宛先へのパスがまだ機能しているという肯定確認応答です（1 という値が設定された送信要求フラグを持つネイバー アドバタイズメント メッセージは、ネイバー送信要求メッセージへの返信としてだけ送信されません）。非送信要求メッセージが返信された場合は、送信元ノードから宛先ノードまでの片道のパスだけが確認されています。送信要求ネイバー アドバタイズメント メッセージは、往復のパスがいずれも機能していることを示します。



(注)

0 という値が設定された送信要求フラグを持つネイバー アドバタイズメント メッセージは、宛先への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。

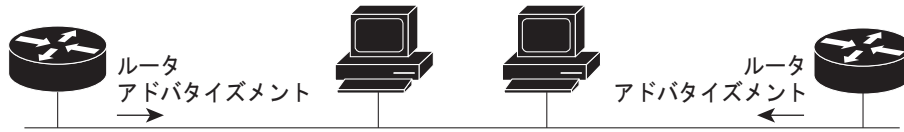
ネイバー送信要求メッセージは、ユニキャスト IPv6 アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。新規のリンクローカル IPv6 アドレスに対しては、インターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（新規アドレスは、重複アドレス検出の実行中は一時的なアドレスのままです）。ノードは、未指定の送信元アドレスと一時的なリンクローカル アドレスがメッセージ本文に含まれるネイバー送信要求メッセージを送信します。そのアドレスがすでに他のノードによって使用されている場合、ノードは、一時的なリンクローカル アドレスを含むネイバー アドバタイズメント メッセージを返信します。他のノードが同時に、同じアドレスが一意であることを確認している場合は、そのノードも、ネイバー送信要求メッセージを返信します。ネイバー送信要求メッセージの返信としてのネイバー アドバタイズメント メッセージも、同じ一時的アドレスを確認中の他のノードからのネイバー送信要求メッセージも受信しない場合、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 アドレスが一意であると判断し、そのアドレスをインターフェイスに割り当てます。

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 フィールドの値が 134 であり、IPv6 ルータの設定済みの各インターフェイスへと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 (図 3-10 を参照)。

図 3-10 IPv6 ネイバー探索 - RA メッセージ



ルータ アドバタイズメント パケット定義：

ICMPv6 タイプ = 134

送信元 = ルータ リンクローカル アドレス

宛先 = すべてのノードのマルチキャスト アドレス

データ = オプション、プレフィクス、有効期間、自動設定フラグ

52674

RA メッセージには通常、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 リミットと MTU などの、ホストの詳細情報

RA は、ルータ送信要求メッセージ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。送信元アドレスは通常、未指定 IPv6 アドレス (0:0:0:0:0:0:0) です。ホストでユニキャスト アドレスが設定されている場合は、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、メッセージで送信元アドレスとして使用されます。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 がルータ送信要求の返信として送信されるとき RA メッセージの宛先アドレスは、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。

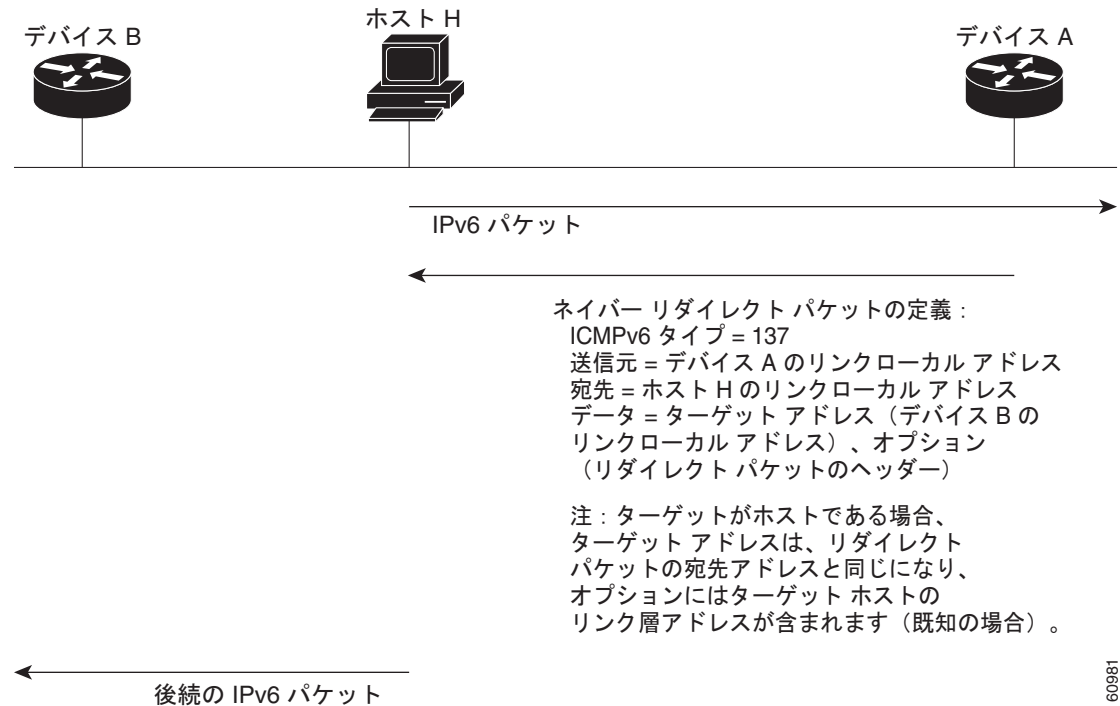
- RA メッセージが定期的に送信される時間の間隔
- デフォルト ルータ（リンクのすべてのノードが使用する）としてのルータの実用性を示すルータのライフタイム値
- リンクで使用されているネットワーク プレフィックス
- (リンクで) ネイバー送信要求メッセージが再送される時間の間隔
- ネイバーが到達可能である（リンク上のすべてのノードが使用できる）とノードが判断するまでの時間

設定されたパラメータは、各インターフェイス固有のパラメータです。RA メッセージ（デフォルト値を含む）の送信は、自動的にイーサネット インターフェイス上で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 メッセージ機能をディセーブルにできます。

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、パス上の宛先へ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 (図 3-11 を参照)。IPv6 ネイバー リダイレクト メッセージは、ICMPv6 パケット ヘッダーのタイプ フィールドの値が 137 となっています。

図 3-11 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 メッセージの目的のアドレス (最終の宛先) により、確実に隣接ルータのリンクローカルアドレスが特定されるよう、ルータは、その各隣接ルータのリンクローカルアドレスを決定可能である必要があります。スタティック 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。ダイナミック ルーティングの場合は、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 プロトコルを設定する必要があります。

パケットの転送後に、次の条件を満たす場合は、ルータが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。
- パケットがそのルータ宛てではなかった。
- パケットが、パケットを受信したインターフェイスから、まもなく送信される。
- 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決定した。
- 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。

IPv6 のライセンス要件

次の表に、この機能のライセンス要件を示します。

| 製品 | ライセンス要件 |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco NX-OS | IPv6 にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』を参照してください。 |

IPv6 の前提条件

IPv6 には、次の前提条件があります。

- IPv6 アドレス指定、IPv6 ヘッダー情報、ICMPv6、IPv6 ネイバー探索 (ND) プロトコルなどの IPv6 の基礎に精通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 の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、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。
- 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。

デフォルト設定

表 3-5 は、IPv6 パラメータのデフォルト設定の一覧です。

表 3-5 デフォルト IPv6 パラメータ

| パラメータ | デフォルト |
|---------------|----------|
| ND 到達可能時間 | 0 ミリ秒 |
| ネイバー送信要求再送信間隔 | 1000 ミリ秒 |

IPv6 の設定

ここでは、次の内容について説明します。

- 「IPv6 アドレス指定の設定」(P.3-17)
- 「IPv6 ネイバー探索の設定」(P.3-19)
- 「IPv6 パケット検証の設定」(P.3-22)



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

IPv6 アドレス指定の設定

インターフェイスで IPv6 トラフィックを転送できるように、インターフェイス上で IPv6 アドレスを設定する必要があります。インターフェイスでグローバル 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. **ipv6 address {addr [eui64] [route-preference preference] [secondary] tag tag-id]}**

または

1. **ipv6 address ipv6-address use-link-local-only**
4. (任意) **show ipv6 interface**
5. (任意) **copy running-config startup-config**

手順の詳細

| | コマンド | 目的 |
|-------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| ステップ1 | configure terminal Example: switch# configure terminal switch(config)# | 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 Example: switch(config)# interface ethernet 2/3 switch(config-if)# | 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。 |

| | コマンド | 目的 |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ3 | <pre> ipv6 address {addr [eui64] [route-preference preference] [secondary] tag tag-id] or ipv6 address ipv6-address use-link-local-only Example: switch(config-if)# ipv6 address 2001:0DB8::1/10 or switch(config-if)# ipv6 address use-link-local-only </pre> | <p>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。</p> <p>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、このアドレスの 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 から自動計算されます。</p> <p>ipv6 address use-link-local-only コマンドを入力すると、インターフェイス上で IPv6 がイネーブルになった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るリンクローカルアドレスがインターフェイス上に設定されます。</p> <p>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。</p> |
| ステップ4 | <pre> show ipv6 interface Example: switch(config-if)# show ipv6 interface </pre> | (任意) IPv6 に設定されたインターフェイスを表示します。 |
| ステップ5 | <pre> copy running-config startup-config Example: switch(config-if)# copy running-config startup-config </pre> | (任意) この設定の変更を保存します。 |

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: 0dc3:0dc3:0000:0000:0000:0000:0000/64
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
```

IPv6 ネイバー探索の設定

ルータで、IPv6 ネイバー探索を設定できます。NDP は、IPv6 ノードとルータをイネーブルにして、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。

はじめる前に

最初に、インターフェイスで IPv6 をイネーブルにする必要があります。

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

| | コマンド | 目的 |
|-------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| ステップ1 | configure terminal Example: switch# configure terminal switch(config)# | 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 Example: switch(config)# interface ethernet 2/31 switch(config-if)# | 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。 |

| コマンド | 目的 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステップ3</p> <pre> ipv6 nd [hop-limit <i>hop-limit</i> managed-config-flag mtu <i>mtu</i> ns-interval <i>interval</i> other-config-flag prefix ra-interval <i>interval</i> ra-lifetime <i>lifetime</i> reachable-time <i>time</i> redirects retrans-timer <i>time</i> suppress-ra] Example: switch(config-if)# ipv6 nd prefix </pre> | <p>ネイバー探索は、IPv6 アドレスを設定すると自動的にイネーブルになります。このコマンドは、インターフェイス上で次の追加の IPv6 ネイバー探索オプションをイネーブルにします。</p> <ul style="list-style-type: none"> • hop-limit <i>hop-limit</i> : IPv6 ネイバー探索パケットでホップリミットをアドバタイズします。有効な範囲は 0 ~ 255 です。 • managed-config-flag : ステートフルアドレス自動設定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 <i>mtu</i> : 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 <i>interval</i> : IPv6 ネイバー送信要求メッセージ間の再送信間隔を設定します。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設定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 <i>interval</i> : 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設定します。範囲は 4 ~ 1800 秒です。 • ra-lifetime <i>lifetime</i> : 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 <i>time</i> : 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イネーブルにします。 • retrans-timer <i>time</i> : 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ディセーブルにします。 |

| | コマンド | 目的 |
|-------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| ステップ4 | show ipv6 nd interface Example: switch(config-if)# show ipv6 nd interface | (任意) IPv6 ネイバー探索に設定されたインターフェイスを表示します。 |
| ステップ5 | copy running-config startup-config Example: switch(config-if)# copy running-config startup-config | (任意) この設定の変更を保存します。 |

次に、IPv6 ネイバー探索の到達可能時間の設定例を示します。

```
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 unreachable: false
```

選択可能なその他の IPv6 ネイバー探索

次の IPv6 ネイバー探索コマンドを任意で使用できます。

| 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、ルータにより発信されたすべての IPv6 パケットで使用される最大ホップ数を設定します。 |
| ipv6 nd managed-config-flag | IPv6 ルータ アドバタイズメントに、管理されたアドレス設定フラグを設定します。 |

| コマンド | 目的 |
|----------------------------------------|------------------------------------------------------------------------------|
| <code>ipv6 nd mtu</code> | インターフェイスで送信される IPv6 パケットの Maximum Transmission Unit (MTU; 最大伝送単位) サイズを設定します。 |
| <code>ipv6 nd ns-interval</code> | インターフェイスで IPv6 ネイバー送信要求メッセージが再送信される時間間隔を設定します。 |
| <code>ipv6 nd other-config-flag</code> | IPv6 ルータ アドバタイズメントに、別のステートフル設定フラグを設定します。 |
| <code>ipv6 nd ra-interval</code> | 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設定します。 |
| <code>ipv6 nd ra-lifetime</code> | インターフェイス上の IPv6 RA メッセージのルータのライフタイム値を設定します。 |
| <code>ipv6 nd reachable-time</code> | 何らかの到達可能確認イベントが発生したあとで、リモート IPv6 ノードが到達可能であると判断されるまでの時間を設定します。 |
| <code>ipv6 nd redirects</code> | ICMPv6 リダイレクト メッセージの送信をイネーブルにします。 |
| <code>ipv6 nd retrans-timer</code> | RA のネイバー送信要求メッセージ間のアドバタイズされる時間を設定します。 |
| <code>ipv6 nd suppress-ra</code> | LAN インターフェイス上で IPv6 RA が送信されないようにします。 |

IPv6 パケット検証の設定

Cisco NX-OS は、IPv6 パケット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、イネーブルまたはディセーブルにすることができます。

IDS チェックをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

| コマンド | 目的 |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>hardware ip verify address {destination zero identical reserved source multicast}</code> | IPv6 アドレスに対して次の IDS チェックを実行します。 <ul style="list-style-type: none"> destination zero : 宛先 IP アドレスが <code>::</code> 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 <code>::1</code> 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 <code>FF00::/8</code> 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。 |

| コマンド | 目的 |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>hardware ipv6 verify length {consistent maximum {max-frag max-tcp udp}}</code> | IPv6 アドレスに対して次の IDS チェックを実行します。 <ul style="list-style-type: none"> 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である場合は、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) が 65536 より大きい場合は IPv6 パケットをドロップします。 maximum max-tcp : TCP 長が IP ペイロード長より大きい場合は IPv6 パケットをドロップします。 maximum udp : IPv6 ペイロード長が UDP パケット長より小さい場合は IPv6 パケットをドロップします。 |
| <code>hardware ipv6 verify tcp tiny-frag</code> | 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 未満の場合は、TCP パケットをドロップします。 |
| <code>hardware ipv6 verify version</code> | Ethertype が 6 (IPv6) に設定されていない場合には、IPv6 パケットをドロップします。 |

IPv6 パケット検証の設定を表示するには、`show hardware forwarding ip verify` コマンドを使用します。

IPv6 コンフィギュレーションの確認

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 |
|-------------------------------------------------|--------------------------------|
| <code>show hardware forwarding ip verify</code> | IPv4 および IPv6 パケット検証の設定を表示します。 |
| <code>show ipv6 interface</code> | IPv6 関連のインターフェイス情報を表示します。 |
| <code>show ipv6 adjacency</code> | 隣接関係テーブルを表示します。 |
| <code>show ipv6 icmp</code> | ICMPv6 情報を表示します。 |
| <code>show ipv6 nd</code> | IPv6 ネイバー探索インターフェイス情報を表示します。 |
| <code>show ipv6 neighbor</code> | IPv6 ネイバー エントリを表示します。 |

IPv6 の設定例

次に、IPv6 を設定する例を示します。

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

その他の関連資料

IPv6 の実装に関する詳細情報については、次のページを参照してください。

- 「関連資料」(P.3-24)
- 「標準」(P.3-24)

関連資料

| 関連項目 | マニュアル名 |
|---------------|--------------------------------------------------------------------------------|
| IPv6 CLI コマンド | 『Cisco Nexus 3000 Series NX-OS Unicast Routing Command Reference, Release 6.x』 |

標準

| 標準 | タイトル |
|------------------------------------------------------------------|------|
| この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。 | — |