



CHAPTER 8

ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定

IP バージョン 6 (IPv6) は、Cisco MDS NX-OS の IP Version 4 (IPv4; IP バージョン 4) のものより優れたアドレッシング機能を提供します。IPv6 のアーキテクチャでは、既存の IPv4 ユーザは、エンドツーエンドセキュリティ、Quality of Service (QoS) およびグローバルで一意的なアドレスなどのサービスを提供しつつ、IPv6 に簡単に移行できます。

この章の内容は、次のとおりです。

- 「IPv6 の概要」 (P.8-1)
- 「IPv6 用の基本的な接続の設定」 (P.8-11)
- 「IPv6 スタティック ルートの設定」 (P.8-13)
- 「ギガビットイーサネット IPv6-ACL の注意事項」 (P.8-14)
- 「IPv4 から IPv6 への移行」 (P.8-14)
- 「デフォルト設定」 (P.8-15)



(注) IP アドレッシングを使用する Cisco NX-OS 機能については、本書の該当する章で、IPv6 アドレッシングサポートに関するこれらの機能の説明を参照してください。



(注) ギガビットイーサネットインターフェイスで IP バージョン 4 (IPv4) を設定するには、第 7 章「ギガビットイーサネットインターフェイスの IP バージョン 4 (IPv4) の設定」を参照してください。

IPv6 の概要

IPv6 の IPv4 に対する機能強化は次のとおりです。

- ネットワークの拡張、およびグローバルな到達可能性の提供が可能になる。
- プライベートアドレスおよび Network Address Translation (NAT; ネットワークアドレス変換) が必要ない。
- アドレスの自動設定が簡単になる。

ここでは、Cisco MDS NX-OS での IPv6 機能について説明します。ここで説明する内容は、次のとおりです。

- 「一意なアドレスに対する拡張 IPv6 アドレス領域」 (P.8-2)
- 「IPv6 アドレスのフォーマット」 (P.8-2)
- 「IPv6 アドレス プレフィックスのフォーマット」 (P.8-3)
- 「IPv6 アドレス タイプ : ユニキャスト」 (P.8-3)
- 「IPv6 アドレス タイプ : マルチキャスト」 (P.8-5)
- 「IPv6 のインターネット制御メッセージプロトコル (ICMP)」 (P.8-6)
- 「IPv6 Path MTU Discovery」 (P.8-7)
- 「IPv6 近隣探索」 (P.8-7)
- 「ルータの検出」 (P.8-9)
- 「IPv6 ステートレス自動設定」 (P.8-9)
- 「IPv4 と IPv6 の二重プロトコルスタック」 (P.8-10)

一意なアドレスに対する拡張 IPv6 アドレス領域

IPv6 は、ネットワーク アドレス ビット数を 32 ビット (IPv4) から 128 ビットに 4 倍にすることで、アドレス領域を拡張します。これにより、さらに多くのグローバルで一意な IP アドレスを使用できます。IPv6 アドレスは、グローバルで一意になることで、ネットワーク デバイスのグローバルな到達可能性およびエンドツーエンドセキュリティや、さらに多くのアドレスが要求されるアプリケーションやサービスに重要な機能が実現されます。

IPv6 アドレスのフォーマット

IPv6 アドレスは、フォーマット `x:x:x:x:x:x` によりコロン (:) で区切った一連の 16 ビット 16 進数フィールドとして表されます。IPv6 アドレスの例は次のとおりです。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:3210
```

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

通常、IPv6 アドレスには、連続するゼロの 16 進数フィールドが含まれます。IPv6 アドレスを使いやすくするため、2 つのコロン (::) を使用して、IPv6 アドレスの先頭、中間、末尾で連続するゼロの 16 進数フィールドを圧縮できます (2 つのコロンは連続するゼロの 16 進数フィールドを表します)。

表 8-1 に、圧縮された IPv6 アドレスのフォーマットを示します。



(注) 2 つのコロン (::) は IPv6 アドレスで一度だけ使用でき、最も長い連続するゼロの 16 進数フィールドを表すことができます。



(注) IPv6 アドレスの 16 進数文字は大文字と小文字が区別されません。

表 8-1 圧縮された IPv6 アドレスのフォーマット

IPv6 アドレスのタイプ	通常のフォーマット	圧縮されたフォーマット
ユニキャスト	2001:0DB8:800:200C:0:0:0:417A	2001:0DB8:800:200C::417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101

IPv6 アドレス プレフィックスのフォーマット

IPv6 アドレス プレフィックス (フォーマット *ipv6-prefix/prefix-length*) を使用して、アドレス領域全体のビット単位の連続ブロックを表すことができます。*ipv6-prefix* は、コロンで囲まれた 16 ビット値を使用して 16 進数で指定されます。*prefix-length* は、アドレスの連続する高位何ビットがプレフィックス (アドレスのネットワーク部) を構成するかを示す 10 進値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 アドレス タイプ: ユニキャスト

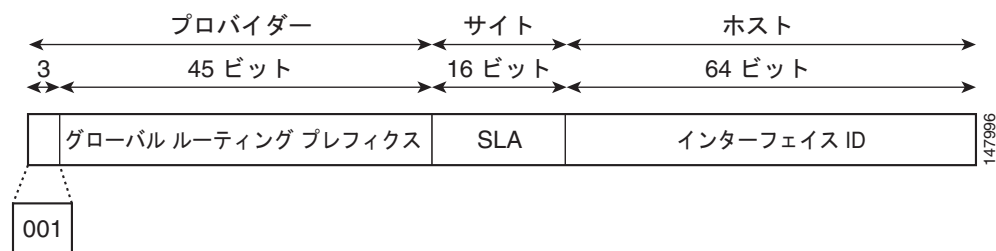
IPv6 ユニキャストアドレスは、シングルノードのシングルインターフェイスの ID です。ユニキャストアドレスに送信されるパケットは、そのアドレスで示されるインターフェイスに配信されます。Cisco MDS NX-OS は、次の IPv6 ユニキャストアドレスタイプをサポートします。

- グローバルアドレス
- リンクローカルアドレス

グローバルアドレス

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。図 8-1 に、グローバルアドレスの構造を示します。

図 8-1 グローバルアドレスのフォーマット



プレフィックス 2000::/3 (001) から E000::/3 (111) のアドレスには、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。Internet Assigned Numbers Authority (IANA; インターネット割り当て番号局) は、範囲 2000::/16 の IPv6 アドレス領域をリージョナルレジストリに割り当てます。

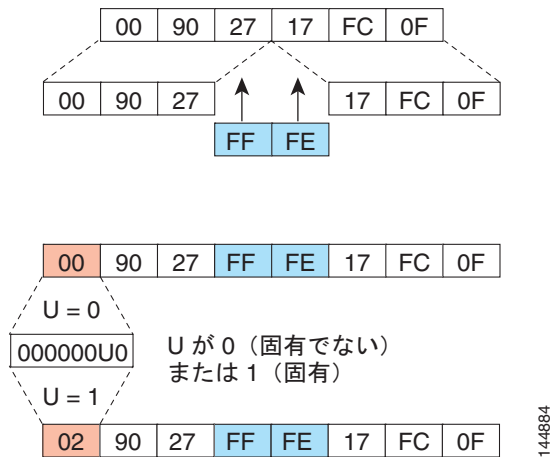
集約可能グローバルアドレスは、通常、48 ビットグローバルルーティングプレフィックスおよび 16 ビットサブネット ID または Site-Level Aggregator (SLA) で構成されます。IPv6 集約可能なグローバルユニキャストアドレスフォーマット文書 (RFC 2374) では、グローバルルーティングプレフィックスには、Top-Level Aggregator (TLA) および Next-Level Aggregator (NLA) という他の 2 つの階層構造のフィールドが含まれるとされていました。TLA フィールドおよび NLA フィールドはポリシーベースであるため、IETF 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、独自のローカルアドレス階層を作成したり、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 65,535 の個々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 はリンク上で一意でなければなりません。また、これより広い範囲で一意な場合もあります。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レイヤアドレスと同じか、リンクレイヤアドレスに基づいているため、グローバルで一意なインターフェイス ID になります。集約可能なグローバルユニキャストアドレスタイプおよびその他の IPv6 アドレスタイプで使用されるインターフェイス ID は、長さが 64 ビットの変更済み EUI-64 フォーマットでなければなりません。

Cisco MDS NX-OS は、IEEE 802 インターフェイスタイプ（たとえば、ギガビットイーサネットインターフェイス）をサポートします。この場合、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 ビットリンクレイヤアドレス（MAC アドレス）の Organizationally Unique Identifier (OUI; 組織固有識別子)、4 番目と 5 番目のオクテット（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。インターフェイス ID の構築は、最初のオクテットの 7 番目のビットである Universal/Local (U/L) ビットに値 0 または 1 を設定して完了します。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（図 8-2 を参照してください）。

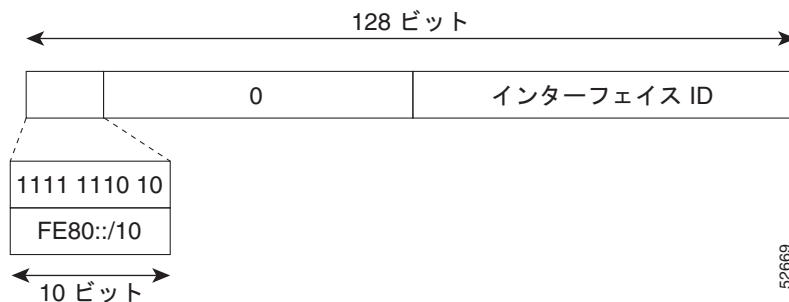
図 8-2 インターフェイス ID フォーマット



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 と、変更済み EUI-64 フォーマットのインターフェイス ID を使用するインターフェイスで自動的に設定される 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近隣探索プロトコルおよびステートレス自動設定処理で使用されます。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。図 8-3 に、リンクローカルアドレスの構造を示します。

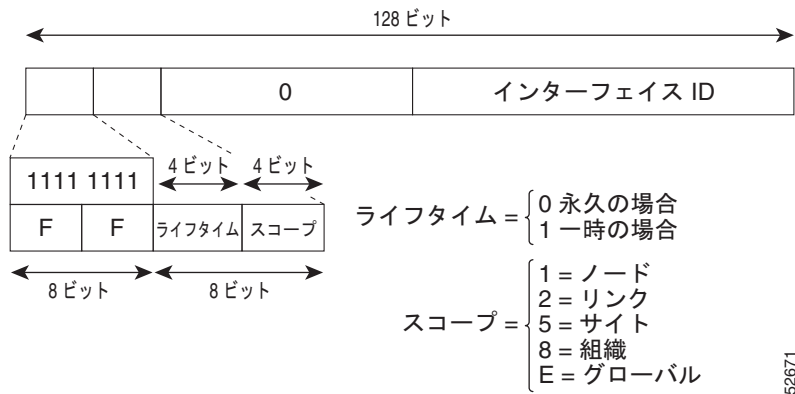
図 8-3 リンクローカルアドレスのフォーマット



IPv6 アドレス タイプ : マルチキャスト

IPv6 マルチキャスト アドレスとは、FF00::/8 (1111 1111) というプレフィクスを持つ IPv6 アドレスです。IPv6 マルチキャスト アドレスは、通常、異なるノードに属するインターフェイス一式の ID です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。プレフィクスに続く 2 番目のオクテットで、マルチキャスト アドレスのライフタイムとスコープが定義されます。永久マルチキャスト アドレスはライフタイム パラメータが 0 に等しく、一時マルチキャスト アドレスのライフタイム パラメータは 1 に等しくなっています。ノード、リンク、サイト、または組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータはそれぞれ、1、2、5、8、または E です。たとえば、FF02::/16 というプレフィクスを持つマルチキャスト アドレスは、リンク スコープを持つ永久マルチキャスト アドレスです。図 8-4 に、IPv6 マルチキャスト アドレスのフォーマットを示します。

図 8-4 IPv6 マルチキャスト アドレスのフォーマット

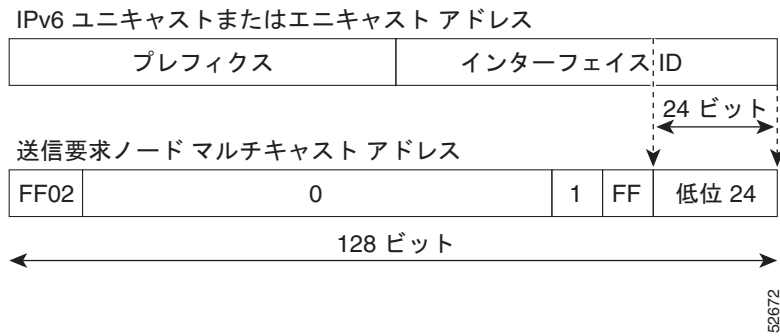


IPv6 ホストは、(受信パケットの宛先となる) 次のマルチキャスト グループに加入する必要があります。

- 全ノード マルチキャスト グループ FF02::1
- ユニキャスト アドレスの低位 24 ビットに連結された送信要求ノード マルチキャスト グループ FF02:0:0:0:1:FF00:0000/104

送信要求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているユニキャスト アドレスごとに、関連付けられた送信要求ノード マルチキャスト グループに加入する必要があります。IPv6 送信要求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレスの低位 24 ビットに連結されたプレフィクス FF02:0:0:0:1:FF00:0000/104 があります (図 8-5 を参照してください)。たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する送信要求ノード マルチキャスト アドレスは FF02::1:FF0E:8C6C です。送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

図 8-5 IPv6 送信要求ノードマルチキャストアドレスのフォーマット



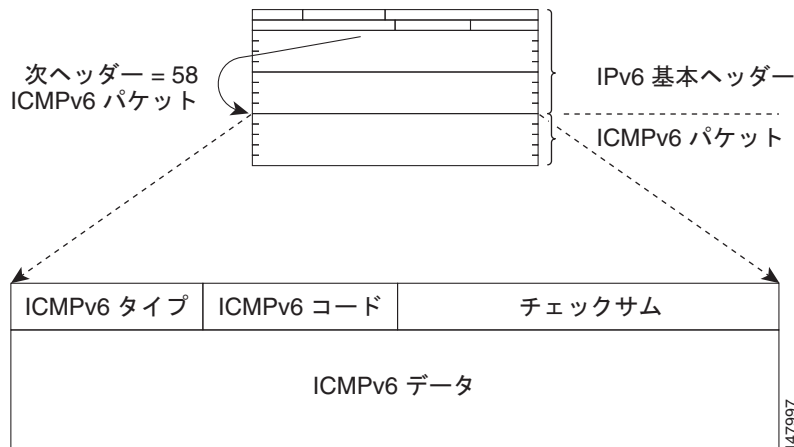
(注) IPv6 にはブロードキャストアドレスはありません。IPv6 マルチキャストアドレスがブロードキャストアドレスの代わりに使用されます。

IPv6 のインターネット制御メッセージ プロトコル (ICMP)

IPv6 のインターネット制御メッセージプロトコル (ICMP) は IPv4 の ICMP と同様に機能します。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、および ICMP エコー要求と応答要求などの情報メッセージを生成します。また、IPv6 の ICMP パケットは IPv6 近隣探索処理、Path MTU Discovery、IPv6 の Multicast Listener Discovery (MLD) プロトコルに使用されます。MLD は、IPv4 の Internet Group Management Protocol (IGMP; インターネットグループ管理プロトコル) のバージョン 2 に基づいています。

基本 IPv6 パケットヘッダーの次ヘッダーフィールドの 58 という値は、IPv6 ICMP パケットであることを示します。IPv6 の ICMP パケットは、すべての拡張ヘッダーの後に続く、ICMP パケット中の最後の情報部分であるという点で、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、IPv6 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。ICMPv6 データフィールドには、IP パケット処理に関するエラーまたは診断情報が含まれます。図 8-6 に、IPv6 ICMP パケットヘッダーのフォーマットを示します。

図 8-6 IPv6 ICMP パケットヘッダーのフォーマット



IPv6 Path MTU Discovery

IPv4 の場合と同様に、ホストが動的に、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に、IPv6 で Path MTU Discovery 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。



(注) IPv4 では、最小リンク MTU は 68 オクテットです。つまり、データパス上のすべてのリンクの MTU サイズは、少なくとも 68 オクテットの MTU サイズをサポートする必要があります。

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。

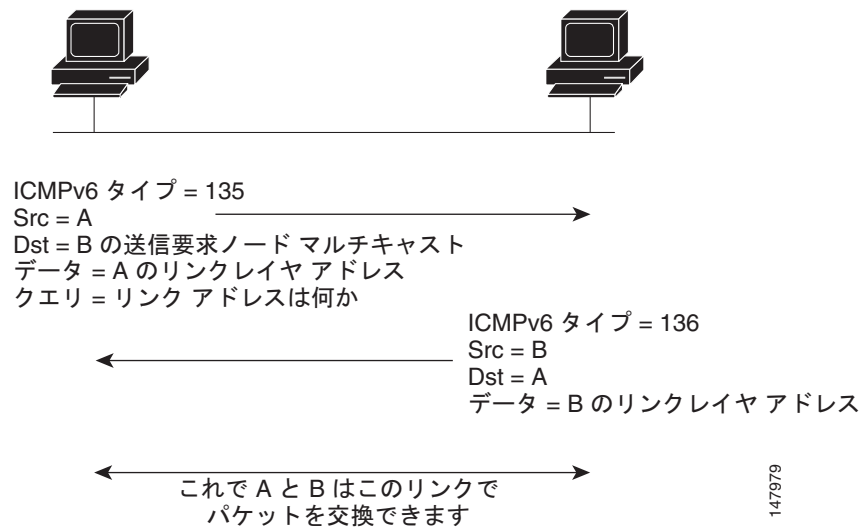
IPv6 近隣探索

IPv6 近隣探索プロセスは、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、同じネットワーク上のネイバーのアドレス（ローカルリンク）を決定し、ネイバーの到達可能性を検証して、ネイバー ルータを追跡します。

IPv6 ネイバー送信要求メッセージおよびアドバタイズメント 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 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レイヤ アドレスを決定するときに、ローカルリンクで送信されます（図 8-7 を参照してください）。ノードが別のノードのリンクレイヤ アドレスを決定する場合、ネイバー送信要求メッセージの送信元アドレスは、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。ネイバー送信要求メッセージの宛先アドレスは、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レイヤ アドレスも含まれます。

図 8-7 IPv6 近隣探索：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、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。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（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レイヤ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は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により、ネイバーのリンクレイヤアドレスが認識された後に、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。

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レイヤアドレスが変更されたときにも送信されます。変更があったときの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です。

ネイバー送信要求メッセージにより、ネイバーのリンクレイヤアドレスが認識された後に、ネイバーの到達可能性が確認できます。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、ホストと近隣ノード（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、そのノードから受諾の確認応答（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。受諾の確認応答は、接続が動作中（宛先に到達中）であることを示す Transmission Control Protocol (TCP; 伝送制御プロトコル) などの上位層プロトコルからの情報や、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は、送信元ノード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、転送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、転送パスがまだ機能しているという確認応答です（値 1 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す）。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、転送パスがまだ機能していることを示す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 アドレスをインターフェイスに割り当て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処理でも使用されます。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 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）はすべてリンクでの一意性を確認する必要があります。ただし、リンクローカルアドレスの一意性が確認されるまで、リンクローカルアドレスに関連付けられた他の 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。

ルータの検出

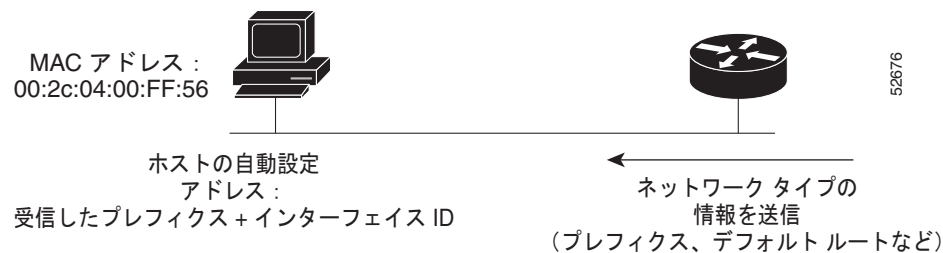
ルータの検出では、ルータ送信要求およびルータ アドバタイズの両方を実行します。ホストは、全ルータのマルチキャスト アドレスにルータ送信要求を送信します。ルータは、送信要求または非送信要求に対して、デフォルトのルータ情報および MTU やホップ制限などの追加パラメータを含むルータ アドバタイズを送信します。

IPv6 ステートレス自動設定

IPv6 ノードのすべてのインターフェイスには、インターフェイスの ID およびリンクローカルプレフィクス 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、ノードはリンク上の他のノードと通信できます。さらに、リンクローカルアドレスを使用して、ノードを設定することができます。

ノードは、ネットワークに接続して自動的にサイトローカルおよびグローバル IPv6 アドレスを生成できます。手動設定や DHCP サーバなどのサーバによる支援は必要はありません。IPv6 の場合、リンク上のルータは、Router Advertisement (RA; ルータ アドバタイズ) メッセージで、任意のサイトローカルプレフィクスやグローバルプレフィクスをアドバタイズしたり、リンクのデフォルトルータとして機能する意図をアドバタイズしたりします。RA メッセージには、定期的に送信されるメッセージと、システム起動時にホストが送信するルータ送信要求メッセージに対する応答として送信されるメッセージがあります（図 8-8 を参照してください）。

図 8-8 IPv6 ステートレス自動設定

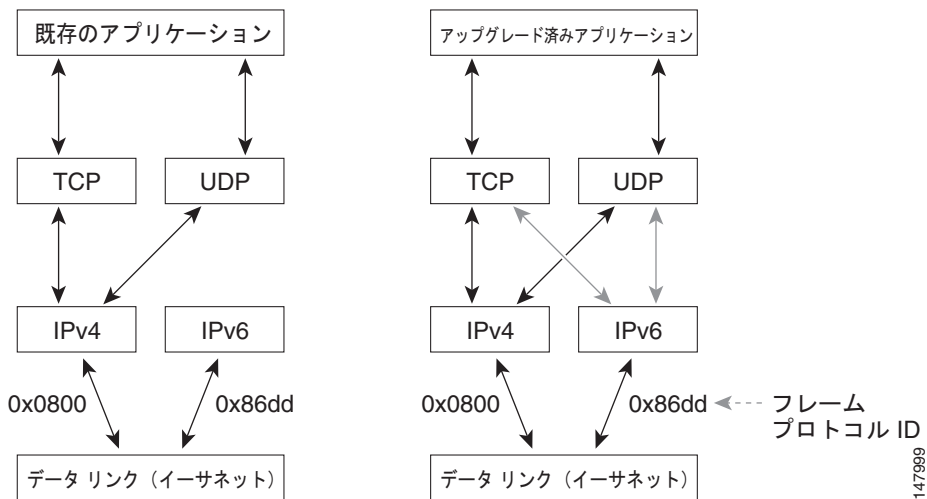


リンク上のノードは、RA メッセージに含まれるプレフィクス（64 ビット）にそのインターフェイス ID（64 ビット）を追加して、自動的にサイトローカルおよびグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、リンクでの一意性を保証するために、重複アドレス検出の対象になります。RA メッセージでアドバタイズされるプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意であることが保証されます。ホストはシステム起動時に ICMP パケットヘッダーのタイプフィールドの値が 133 のルータ送信要求メッセージを送信するため、スケジュールされた次の RA メッセージを待たずにただちに自動設定できます。

IPv4 と IPv6 の二重プロトコル スタック

IPv4 と IPv6 の二重プロトコル スタックは、IPv6 へ移行するための 1 つの方法です。この方法を使用すると、ノード上で稼動するアプリケーションを段階的にアップグレードできます。ノード上で稼動するアプリケーションは、IPv6 プロトコル スタックを利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（IPv4 プロトコル スタックしかサポートしない）アプリケーションは、同じノード上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およびアップグレードされたアプリケーションは、IPv4 および IPv6 の両方のプロトコル スタックを利用します（図 8-9 を参照してください）。

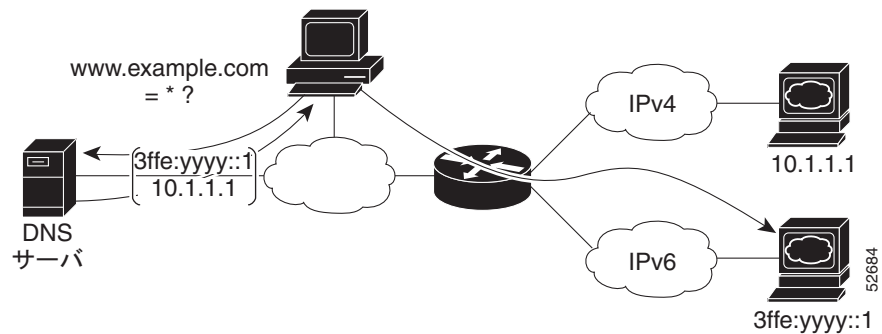
図 8-9 IPv4 と IPv6 の二重プロトコル スタック



IPv4 と IPv6 の両方のアドレスおよび DNS 要求をサポートするために、新しい API が定義されています。アプリケーションは新しい API へアップグレードできます。また、引き続き、IPv4 プロトコル スタックだけを使用できます。Cisco MDS NX-OS は、IPv4 と IPv6 の二重プロトコル スタックをサポートしています。インターフェイスに IPv4 アドレスと IPv6 アドレスの両方を設定すると、そのインターフェイスは、IPv4 トラフィックと IPv6 トラフィックの両方を受け入れ、処理します。

図 8-10 で、IPv4 と IPv6 の二重プロトコル スタックをサポートするアプリケーションは、DNS サーバから宛先ホスト名 `www.a.com` 用に使用できるすべてのアドレスを要求します。DNS サーバは、`www.a.com` に使用できるすべてのアドレス（IPv4 アドレスと IPv6 アドレスの両方）を返信します。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で選択されます）、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 8-10 IPv4 と IPv6 の二重プロトコル スタックをサポートするアプリケーション



IPv6 用の基本的な接続の設定

ここでは、IPv6 の基本的な接続を実装する方法について説明します。各作業には、必須またはオプションの指定があります。ここで説明する内容は、次のとおりです。

- 「IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化」(P.8-11)
- 「IPv4 および IPv6 プロトコルアドレスの設定」(P.8-13)

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化

ここでは、個々のルータ インターフェイスに IPv6 アドレスを割り当て、IPv6 トラフィックの処理をイネーブルにする方法を説明します。デフォルトでは、IPv6 アドレスは設定されておらず、IPv6 処理はディセーブルです。

次の種類のインターフェイスに IPv6 アドレスを設定できます。

- ギガビットイーサネット
- 管理
- VLAN (ギガビットイーサネットサブインターフェイス)
- VSAN



(注) IPv6 アドレスは、RFC 2373 に記述されているように、コロンで囲んだ 16 ビット値を使用して 16 進数で指定する必要があります。

IPv6 プレフィックスは、RFC 2373 に記述されているように、コロンで囲んだ 16 ビット値を使用して 16 進数で指定する必要があります。

IPv6 プレフィックス長アドレスの連続する高位何ビットがプレフィックス (アドレスのネットワーク部) を構成するかを示す 10 進値です。10 進値の前にスラッシュ記号を付ける必要があります。

インターフェイスにグローバル IPv6 アドレスを設定すると、自動的にリンクローカルアドレスが設定され、そのインターフェイスで IPv6 がアクティブになります。また、設定されたインターフェイスは、自動的にそのリンクに必要な次のマルチキャストグループに参加します。

- 送信要求ノードマルチキャストグループ FF02:0:0:0:0:1:FF00::/104 (インターフェイスに割り当てられた各ユニキャストアドレス用)

IPv6 用の基本的な接続の設定

- 全ノードリンクローカル マルチキャスト グループ FF02::1



(注) 送信要求ノードマルチキャストアドレスは、近隣探索プロセスで使用されます。

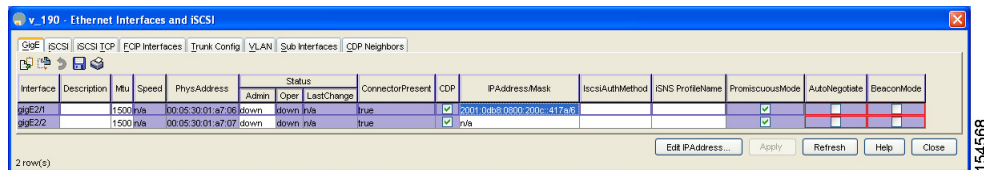


(注) 各インターフェイスには IPv6 アドレス (スタティックおよび自動設定) を最大 8 つまで設定できます。ただし、管理 (mgmt 0) インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定できません。

Device Manager を使用してインターフェイスの IPv6 アドレスを設定する手順は、次のとおりです。

- ステップ 1** [Interfaces] > [Gigabit Ethernet and iSCSI] を選択します。
[Gigabit Ethernet Configuration] ダイアログボックスが表示されます (図 8-11 を参照してください)。

図 8-11 Device Manager でのギガビットイーサネットの設定

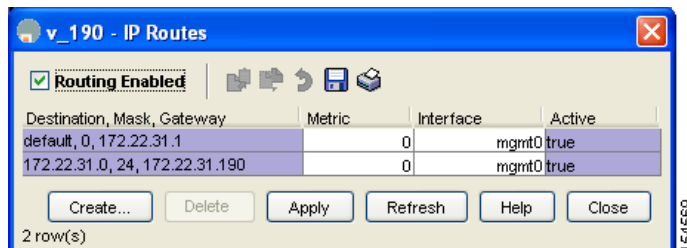


- ステップ 2** 設定する [IP Address] をクリックして、[Edit IP Address] をクリックします。
[IP Address] ダイアログボックスが表示されます。
- ステップ 3** [Create] をクリックし、IPv6 フォーマット (たとえば、2001:0DB8:800:200C::417A/64) を使用して、[IP Address/Mask] フィールドを設定します。
- ステップ 4** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

Device Manager を使用して IPv6 ルーティングをイネーブルにする手順は、次のとおりです。

- ステップ 1** [IP] > [Routing] を選択します。[IP Routing Configuration] ダイアログボックスが表示されます (図 8-12 を参照してください)。

図 8-12 Device Manager での IP ルーティングの設定



- ステップ 2** [Routing Enabled] チェックボックスをオンにします。
- ステップ 3** これらの変更を保存するには、[Apply] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。
-

IPv4 および IPv6 プロトコル アドレスの設定

シスコ ネットワーク デバイスのインターフェイスに IPv4 アドレスと IPv6 アドレスの両方を設定すると、インターフェイスは IPv4 ネットワークと IPv6 ネットワークの両方でデータを送受信できます。

Device Manager を使用して、IPv4 および IPv6 プロトコル スタックの両方をサポートするようにシスコ ネットワーク デバイスのインターフェイスを設定する手順は、次のとおりです。

- ステップ 1** [Interfaces] > [Gigabit Ethernet and iSCSI] を選択します。
[Gigabit Ethernet Configuration] ダイアログボックスが表示されます。
- ステップ 2** 設定する [IP Address] フィールドをクリックして、[Edit IP Address] をクリックします。
[IP Address] ダイアログボックスが表示されます。
- ステップ 3** [Create] をクリックし、IPv4 または IPv6 フォーマットを使用して、[IP Address/Mask] フィールドを設定します。
- ステップ 4** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。
-

IPv6 スタティック ルートの設定

Cisco MDS NX-OS は、IPv6 のスタティック ルートをサポートしています。ここで説明する内容は、次のとおりです。

- [「IPv6 スタティック ルートの設定」 \(P.8-13\)](#)

IPv6 スタティック ルートの設定

IPv6 スタティック ルートを手動で設定し、2 台のネットワーク デバイス間の明示的なパス定義する必要があります。IPv6 スタティック ルートは自動的に更新されないため、ネットワーク トポロジが変化した場合は、手動で再設定する必要があります。

Device Manager を使用して IPv6 スタティック ルートを設定する手順は、次のとおりです。

- ステップ 1** [IP] > [Routing] を選択します。
[IP Routing Configuration] ダイアログボックスが表示されます
- ステップ 2** [Create] をクリックします。
[Create IP Route] ダイアログボックスが表示されます。
- ステップ 3** [Dest] フィールドに IPv6 宛先アドレスを設定します。
- ステップ 4** [Mask] フィールドに IPv6 サブネット マスクを設定します。

- ステップ 5** [Gateway] フィールドに IPv6 デフォルト ゲートウェイを設定します。
- ステップ 6** (任意) [Metric] フィールドに必要なルート トリックを設定します。
- ステップ 7** [Interface] ドロップダウン メニューからインターフェイスを選択します。
- ステップ 8** これらの変更を保存するには、[Create] をクリックします。変更を保存せずに終了するには、[Close] をクリックします。

ギガビットイーサネット IPv6-ACL の注意事項



ヒント

IPv6-ACL がギガビットイーサネット インターフェイスにすでに含まれている場合、このインターフェイスをイーサネット PortChannel グループに追加することはできません。IPv6-ACL の設定については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

ギガビットイーサネット インターフェイスの IPv6-ACL を設定する場合、次の注意事項に従ってください。

- 伝送制御プロトコル (TCP) または Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) だけを使用します。



(注)

User Datagram Protocol (UDP; ユーザ データグラム プロトコル) および HTTP などのその他のプロトコルは、ギガビットイーサネット インターフェイスではサポートされていません。これらのプロトコルのルールを含む ACL をギガビットイーサネット インターフェイスに適用することはできますが、そのルールの効果はありません。

- インターフェイスをイネーブルにする前に IPv6-ACL をインターフェイスに適用します。これにより、トラフィック フローが開始される前に、フィルタが正常であることを確認できます。
- 次の条件に注意してください。
 - **log-deny** オプションを使用する場合、毎秒最大 50 のメッセージが記録されます。
 - **established** オプションは、このオプションを含む IPv6-ACL をギガビットイーサネット インターフェイスに適用する場合は無視されます。
 - IPv6-ACL ルールが既存の TCP 接続に適用される場合、ルールは無視されます。たとえば、A と B の間に既存の TCP 接続があり、発信元を A、宛先を B とするすべてのパケットの削除を指定する IPv6-ACL がその後で適用された場合、このルールの効果はありません。

IPv6-ACL のインターフェイスへの適用については、『Cisco Fabric Manager Security Configuration Guide』を参照してください。

IPv4 から IPv6 への移行

Cisco MDS NX-OS は、IPv4 から IPv6 への移行メカニズムをサポートしていません。ただし、IPv4 から IPv6 への移行には、シスコ ルータ製品の移行スキームを利用できます。ネットワークを移行するようにシスコ ルータを設定する方法の詳細については、『Cisco IOS IPv6 Configuration Guide』の「Implementing Tunneling for IPv6」の章を参照してください。

デフォルト設定

表 8-2 に、IPv6 パラメータのデフォルト設定を示します。

表 8-2 デフォルトの IPv6 パラメータ

パラメータ	デフォルト
IPv6 処理	ディセーブル
重複アドレス検出試行回数	0 (近隣探索ディセーブル)
到達可能性時間	1000 ミリ秒
再送信時間	30000 ミリ秒
IPv6-ACL	なし

