



CHAPTER 47

ギガビットイーサネットインターフェイスでの IPv6 の設定

Cisco MDS SAN-OS で IP バージョン 6 (IPv6) は IP バージョン 4 (IPv4) よりも拡張さ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。

この章は、次の項で構成されています。

- 「IPv6 の概要」 (P.47-1)
- 「IPv6 用の基本的な接続の設定」 (P.47-11)
- 「ネイバー探索パラメータの設定」 (P.47-15)
- 「IPv6 スタティック ルートの設定」 (P.47-17)
- 「ギガビットイーサネットの IPv6-ACL に関する注意事項」 (P.47-19)
- 「IPv4 から IPv6 への移行」 (P.47-19)
- 「IPv6 情報の表示」 (P.47-19)
- 「デフォルト設定」 (P.47-21)



(注) IP アドレッシングを使用する Cisco SAN-OS 機能の IPv6 アドレッシングのサポートについては、このガイドの該当する章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) を設定する場合は、[第 46 章「ギガビットイーサネットインターフェイスでの IPv4 の設定」](#)を参照してください。

IPv6 の概要

IPv6 の IPv4 に対する改良点は、次のとおりです。

- ネットワークの拡張性およびグローバルな到達可能性の実現
- プライベートアドレスおよびネットワークアドレス変換 (NAT) が不要
- アドレスの自動設定の簡素化

ここでは、Cisco MDS SAN-OS がサポートしている IPv6 機能について説明します。内容は次のとおりです。

- 「IPv6 アドレス空間の拡張による一意アドレスの確保」 (P.47-2)
- 「IPv6 アドレス フォーマット」 (P.47-2)
- 「IPv6 アドレス プレフィックスの形式」 (P.47-3)
- 「IPv6 アドレスの種類：ユニキャスト」 (P.47-3)
- 「IPv6 アドレスの種類：マルチキャスト」 (P.47-5)
- 「IPv6 の ICMP」 (P.47-6)
- 「IPv6 のパス MTU 検出」 (P.47-7)
- 「IPv6 ネイバー探索」 (P.47-7)
- 「ルータの検出」 (P.47-9)
- 「IPv6 ステートレス自動設定」 (P.47-9)
- 「IPv4 と IPv6 の二重プロトコルスタック」 (P.47-10)

IPv6 アドレス空間の拡張による一意アドレスの確保

IPv6 では、ネットワークアドレスのビット数を (IPv4 の) 32 ビットから 4 倍の 128 ビットに増やしてアドレス空間を拡張しています。これにより、利用できるグローバルに一意な IP アドレスの数が大幅に増加しています。グローバルに一意な IPv6 アドレスを利用すると、ネットワーク接続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を実現できます。これは、より多くのアドレスを必要とするアプリケーションやサービスに不可欠な機能です。

IPv6 アドレス フォーマット

IPv6 アドレスは、16 ビットの 16 進フィールドをコロン (:) で続けた x:x:x:x:x:x:x という形式で表現されます。次に、IPv6 アドレスの例を示します。

```
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、または末尾にある連続した 0 の 16 進フィールドを 2 つのコロン (::) を使用して圧縮すると、IPv6 アドレスが使いやすくなります (2 つのコロンは連続した 0 の 16 進フィールドを表します)。表 47-1 に、圧縮された IPv6 アドレスの形式をリストします。



(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。



(注)

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 47-1 圧縮された IPv6 アドレス形式

IPv6 アドレス タイプ	非圧縮形式	圧縮形式
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	FF01:0:0:0:0:0:101	FF01::101

IPv6 アドレス プレフィックスの形式

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、16 進の 16 ビット値をコロンで区切って指定します。*prefix-length* は、アドレスの連続する上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 アドレスの種類：ユニキャスト

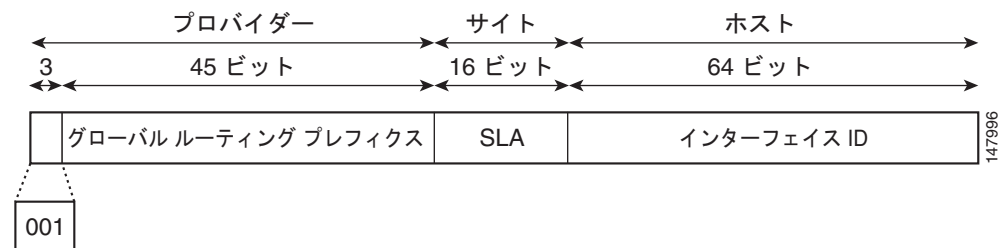
IPv6 ユニキャストアドレスは、1 つのノード上の 1 つのインターフェイスの ID です。ユニキャストアドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。Cisco MDS SAN-OS は、次の種類の IPv6 ユニキャストアドレスをサポートしています。

- 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 で定義されます。図 47-1 に、グローバルアドレスの構造を示します。

図 47-1 グローバルアドレスの形式



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。

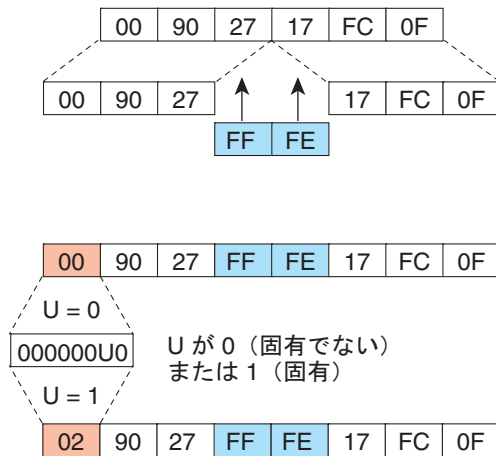
集約可能グローバルアドレスは、通常、48 ビットのグローバルルーティングプレフィックスと、16 ビットのサブネット ID またはサイトレベル集約 (SLA) で構成されます。RFC 2374 (IPv6 集約可能グローバルユニキャストアドレス形式) では、グローバルルーティングプレフィックスに Top-Level Aggregator (TLA) と Next-Level Aggregator (NLA) という他の 2 つの階層構造フィールドが含まれていました。IETF は、TLS フィールドと NLA フィールドがポリシーベースのフィールドであるため、これらのフィールドを RFC から削除することに決定しました。この変更の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に基づく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、サブネット ID と呼ばれる 16 ビットのサブネットフィールドを使用して、独自のローカルアドレスリング階層を作成したり、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 は、リンク上のインターフェイスの識別に使用されます。インターフェイス ID は、リンク上で一意である必要があります。また、より広い範囲で一意にすることもできます。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層アドレスと同じか、それに基づいているため、グローバルに一意になります。集約可能グローバルユニキャストおよびその他の 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 ビットの変更された EUI-64 形式で構築されている必要があります。

Cisco MDS SAN-OS は、IEEE 802 インターフェイス（たとえば、ギガビット イーサネット インターフェイス）をサポートしています。最初の 3 オクテット（24 ビット）は、インターフェイスの 48 ビットのリンク層アドレス（MAC アドレス）の Organizationally Unique Identifier（OUI）から取得され、4 番めと 5 番めのオクテット（16 ビット）は、FFFE の固定 16 進値であり、最後の 3 オクテット（24 ビット）は、MAC アドレスの最後の 3 オクテットから取得されます。インターフェイス ID の構成は、最初のオクテットの 7 番めのビットである Universal/Local（U/L）ビットを 0 または 1 の値に設定することで完成します。0 の値はローカルに管理される ID を表し、1 の値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 47-2 を参照）。

図 47-2 インターフェイス ID の形式

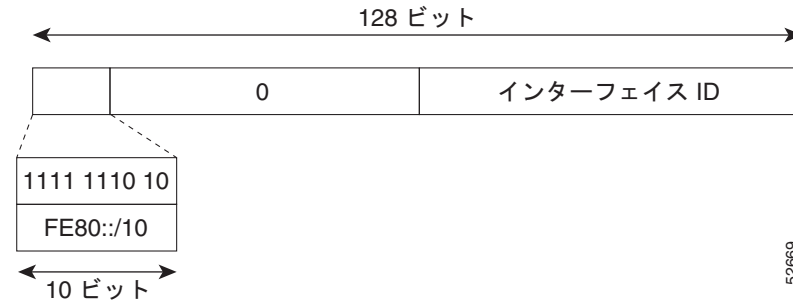


144884

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 Modified EUI-64 形式のインターフェイス ID を使用して自動的にインターフェイスに設定される 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、ネイバー探索プロトコルとステータス自動設定プロセスで使用されます。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 47-3 に、リンクローカルアドレスの構造を示します。

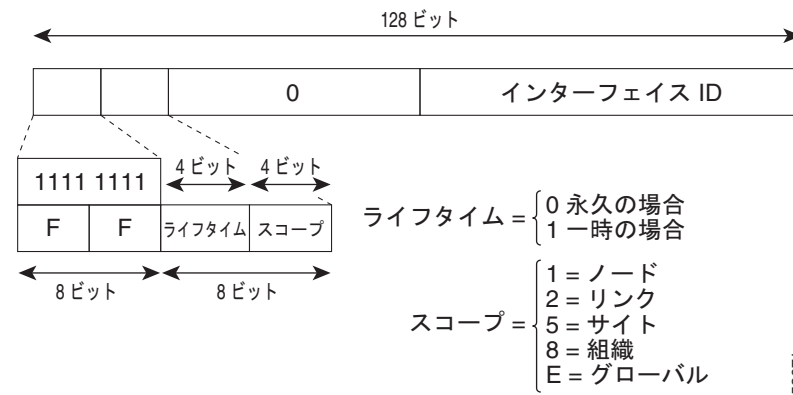
図 47-3 リンクローカルアドレスの形式



IPv6 アドレスの種類：マルチキャスト

IPv6 マルチキャストアドレスは、FF00::/8 (1111 1111) というプレフィックスを持つ IPv6 アドレスです。IPv6 マルチキャストアドレスは、通常は異なるノードに属するインターフェイスセットの識別子です。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。プレフィックスに続く 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。永続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 と等しく、一時マルチキャストアドレスはライフタイムパラメータが 1 と等しくなっています。ノード、リンク、サイト、組織、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、および E です。たとえば、プレフィックスが FF02::/16 のマルチキャストアドレスは、リンクスコープを持つ永続マルチキャストアドレスです。図 47-4 に、IPv6 マルチキャストアドレスの形式を示します。

図 47-4 IPv6 マルチキャストアドレスの形式



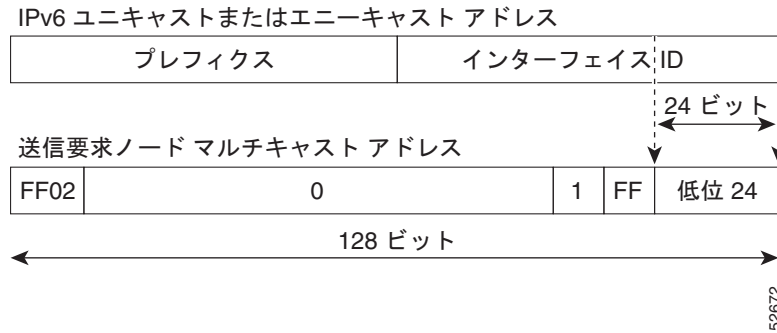
IPv6 ホストは、次のマルチキャストグループに参加して、各マルチキャストグループ宛のパケットを受信する必要があります。

- 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下位 24 ビットと連結した送信要求ノードマルチキャストグループ FFF02:0:0:0:1: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すべてのユニキャストアドレスについて、関連する送信要求ノードマルチキャストグループに参加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は、対応する IPv6 ユニキャストアドレスの下位 24 ビットと連結され

るプレフィックス FF02:0:0:0:1:FF00:0000/104 を持ちます。(図 47-5 を参照)。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 47-5 IPv6 送信要求ノード マルチキャスト アドレスの形式



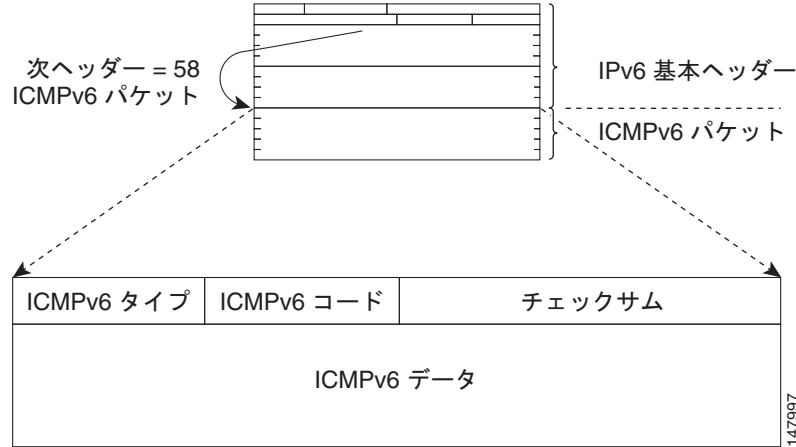
(注) IPv6 にはブロードキャストアドレスはありません。IPv6 マルチキャストアドレスがブロードキャストアドレスの代わりに使用されます。

IPv6 の ICMP

IPv6 の Internet Control Message Protocol (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のようなエラーメッセージ、および ICMP エコー要求や応答メッセージのような情報メッセージを生成します。また、IPv6 の ICMP 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、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。IPv6 の ICMP 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。図 47-6 に、IPv6 ICMP パケットヘッダーの形式を示します。

図 47-6 IPv6 ICMP パケット ヘッダーの形式



IPv6 のパス MTU 検出

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 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 が 68 オクテットであるため、特定のデータパスに沿うすべてのリンクの MTU サイズが少なくとも 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 リンクでは、1500 オクテットの最大伝送単位 (MTU) を使用することを推奨します。

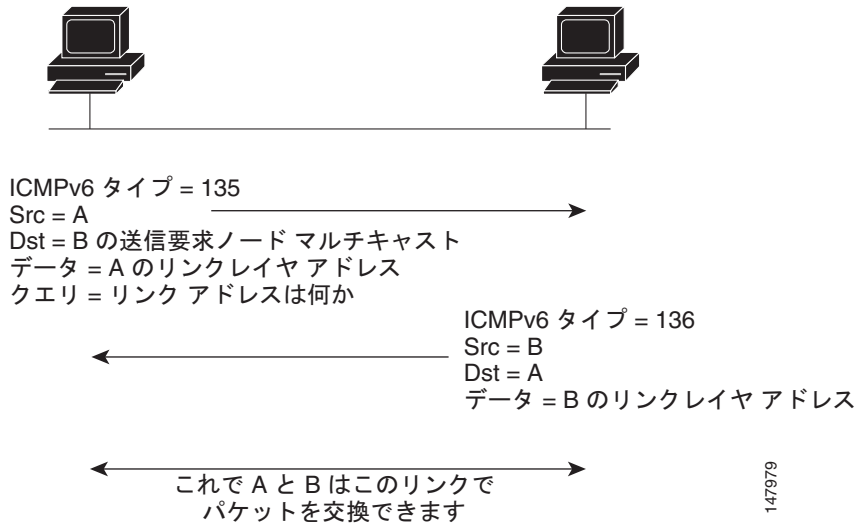
IPv6 ネイバー探索

IPv6 のネイバー探索プロセスは、ICMP メッセージと送信要求ノード 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別し、ネイバーの到達可能性を確認して、近隣ルータの状況を把握します。

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決定するときに、ローカルリンク上で送信されます (図 47-7 を参照)。ノードで別のノードのリンク層アドレスを特定する必要がある場合、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 アドレスになります。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 47-7 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。ノードが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。このような変更がある場合、ネイバー アドバタイズの宛先アドレスは、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。

直近にネイバーに送信したパケットがネイバーで受信され、処理されたことが確認できた場合、ネイバーは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 TCP 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、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 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。ネイバー送信要求メッセージに対する応答としてネイバー アドバタイズメント メッセージを受け取った場

合、中継パスが動作していることが確認できます（送信要求フラグが 1 にセットされたネイバー アドバタイズメッセージは、ネイバー送信要求メッセージに対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。

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

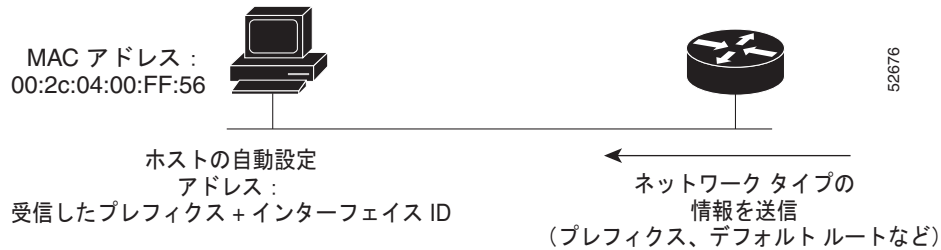
ルータの検出では、ルータ送信要求およびルータ アドバタイズの両方を実行します。ホストは、全ルータのマルチキャストアドレスにルータ送信要求を送信します。ルータは、送信要求または割り込みに対して、デフォルトのルータ情報および MTU やホップ制限などの追加パラメータを含むルータアドバタイズを送信します。

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を持つ必要があります。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、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、ルータ アドバタイズ (RA) メッセージで、任意のサイトローカルプレフィックスやグローバルプレフィッ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 メッセージは、定期的送信される場合と、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場合があります。(図 47-8 を参照)。

図 47-8 IPv6 ステートレス自動設定

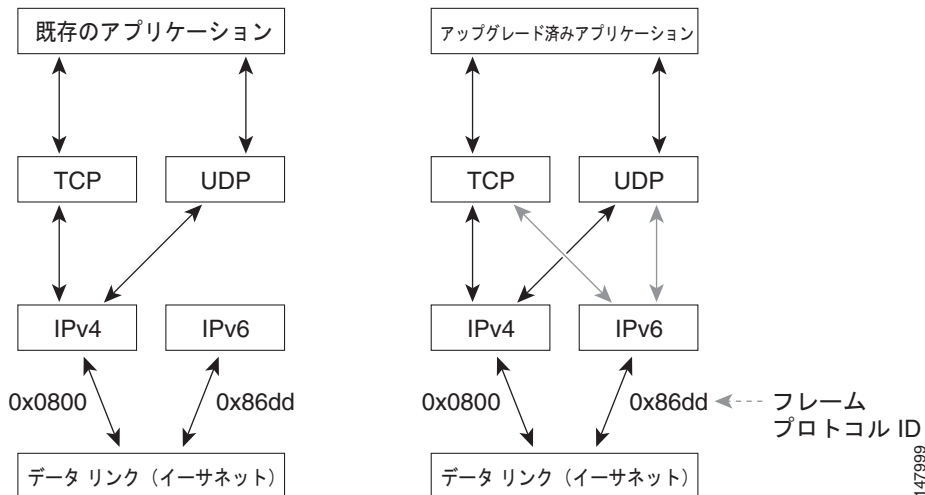


リンク上のノードは、RA メッセージに含まれるプレフィックス（64 ビット）にそのインターフェイス ID（64 ビット）を追加して、自動的にサイトローカルおよびグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動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。

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（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 47-9 を参照）。

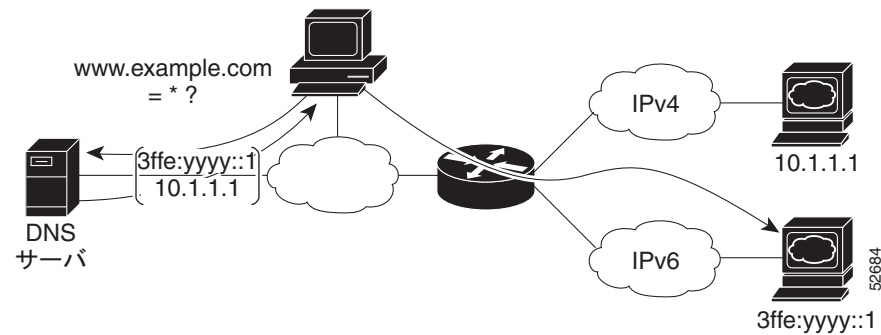
図 47-9 デュアル IPv4 および IPv6 プロトコル スタック手法



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。Cisco MDS SAN-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 47-10 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 `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 47-10 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 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。一覧内の各作業は、必須と任意に分けています。この項では、次のトピックについて取り上げます。

- 「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.47-11)
- 「IPv4 および IPv6 プロトコルアドレスの設定」 (P.47-13)
- 「基本的な IPv6 接続の設定と動作の確認」 (P.47-14)
- 「IPv6 のネイバー探索キャッシュのクリア」 (P.47-15)

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 address** コマンドの *ipv6-address* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。

ipv6 address コマンドの *ipv6-prefix* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。

ipv6 address コマンドの *prefix-length* 引数は、アドレスのうち連続する上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 進数値です。10 進数値の前にスラッシュ記号が必要です。

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、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に対して 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、そのリンクに必要な次のマルチキャスト グループに自動的に加入します。

- 送信要求ノード マルチキャスト グループ FF02:0:0:0:1: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）
- 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、ネイバー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。

インターフェイスの IPv6 アドレスを設定し、IPv6 ルーティングをイネーブルにするには、次の手順を実行します。

	コマンドまたはアクション	目的
ステップ1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ2	switch(config)# interface gigabitethernet 1/1 switch(config-if)#	ギガビット イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。
	switch(config)# interface mgmt 0 switch(config-if)#	管理インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。
	switch(config)# interface gigabitethernet 2/2.100 switch(config-if)#	ギガビット イーサネット サブインターフェイス (VLAN ID) を指定し、インターフェイス コンフィギュレーション サブモードを開始します。
	switch(config)# interface vsan 10 switch(config-if)#	VSAN インターフェイスを指定し、インターフェイス コンフィギュレーション サブ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	switch(config-if)# ipv6 address 2001:0DB8:800:200C::417A/64	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、そのインターフェイスの IPv6 リンクローカルアドレスを設定し、インターフェイスの IPv6 処理をイネーブルにします。
	switch(config-if)# ipv6 address autoconfig	インターフェイスの IPv6 リンクローカルアドレスとユニキャストアドレスの自動設定をイネーブルにし、インターフェイスの IPv6 処理をイネーブルにします。
	switch(config-if)# ipv6 enable	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。
ステップ 4	switch(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 5	switch(config-if)# exit switch(config)	インターフェイス コンフィギュレーション サブモードを終了して、コンフィギュレーションモードに戻ります。
ステップ 6	switch(config)# ipv6 routing	IPv6 ユニキャスト データグラムの処理をイネーブルにします。

IPv4 および IPv6 プロトコルアドレスの設定

シスコ製ネットワーク 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。

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製ネットワーク デバイスのインターフェイスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# interface gigabitethernet 1/1 switch(config-if)#	インターフェイスを指定し、インターフェイス コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-if)# ip address 192.168.99.1 255.255.255.0	インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。
ステップ 4	switch(config-if)# ipv6 address 2001:0DB8:c18:1::3/64	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。 (注) IPv6 アドレスの設定の詳細については、「 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 」を参照してください。
ステップ 5	switch(config-if)# no shutdown	インターフェイスをイネーブルにします。

	コマンド	目的
ステップ6	switch(config-if)# exit switch(config)	インターフェイス コンフィギュレーション サブモードを終了して、コンフィギュレーションモードに戻ります。
ステップ7	switch(config)# ipv6 routing	IPv6 ユニキャスト データグラムの処理をイネーブルにします。

基本的な IPv6 接続の設定と動作の確認

情報を表示して、基本的な IPv6 接続の設定および動作を確認できます。

ここでは、次の **show ipv6** コマンドの出力例を示します。

- [show ipv6 interface](#) コマンドの出力例
- [show ipv6 neighbours](#) コマンドの出力例
- [show ipv6 traffic](#) コマンドの出力例

show ipv6 interface コマンドの出力例

次の例では、**show ipv6 interface** 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 6/1 インターフェイスに対して正しく設定されていることを確認します。

```
switch# show ipv6 interface mgmt 0
mgmt0 is up
  IPv6 is enabled
  Global address(es):
    2172:22::180/64
  Link-local address(es):
    fe80::b8db:adff:feba:d074
  ND DAD is disabled
  ND reachable time is 30000 milliseconds
  ND retransmission time is 1000 milliseconds
  Stateless autoconfig for addresses disabled
  MTU is 1500 bytes
```

show ipv6 neighbours コマンドの出力例

次の例では、**show ipv6 neighbours** コマンドは、すべてのインターフェイスの IPv6 ネイバー探索 キャッシュ情報を表示します。

```
switch# show ipv6 neighbours
R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe, D - Delay
IPv6 Address                               Age  State Link-layer Addr      Interface
fe80::211:5dff:fe53:500a                   0    S    0011.5d53.500a        GigE6/1
fe80::211:5dff:fe53:500a                   0    S    0011.5d53.500a        GigE6/2
5000:1::250                                 0    S    0011.5d53.500a        po 4
fe80::211:5dff:fe53:500a                   0    S    0011.5d53.500a        po 4
fe80::211:5dff:fe53:500a                   0    S    0011.5d53.500a        po 4
fe80::2d0:3ff:fe61:4800                     184  S    00d0.0361.4800        mgmt0
```

次の例では、**show ipv6 neighbours interface** コマンドは、ギガビット イーサネット 6/1 インターフェイスの IPv6 ネイバー探索 キャッシュ情報を表示します。

```
switch# show ipv6 neighbours interface gigabitethernet 6/1
R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe, D - Delay
```

IPv6 Address	Age	State	Link-layer Addr	Interface
fe80::211:5dff:fe53:500a	0	S	0011.5d53.500a	GigE6/1

show ipv6 traffic コマンドの出力例

show ipv6 traffic コマンドは、IPv6 および ICMP の統計情報を表示します。

```
switch# show ipv6 traffic
IPv6 Statistics:
Rcvd: 100 total, 0 local destination
      0 errors, 0 truncated, 0 too big
      0 unknown protocol, 0 dropped
      0 fragments, 0 reassembled
      0 couldn't reassemble, 0 reassembly timeouts
Sent: 0 generated, 0 forwarded 0 dropped
      0 fragmented, 0 fragments created, 0 couldn't fragment

ICMPv6 Statistics:
Rcvd: 100 total, 0 errors, 0 unreachable, 0 time exceeded
      0 too big, 0 param probs, 0 admin prohibits
      0 echos, 0 echo reply, 0 redirects
      0 group query, 0 group report, 0 group reduce
      0 router solicit, 69 router advert
      0 neighbor solicit, 31 neighbor advert
Sent: 55 total, 0 errors, 0 unreachable, 0 time exceeded
      0 too big, 0 param probs, 0 admin prohibits
      0 echos, 0 echo reply, 0 redirects
      0 group query, 20 group report, 2 group reduce
      0 router solicit, 0 router advert
      0 neighbor solicit, 33 neighbor advert
```

IPv6 のネイバー探索キャッシュのクリア

EXEC モードで **clear ipv6 neighbor** コマンドを使用して、IPv6 ネイバー探索キャッシュをクリアできます。

```
switch# clear ipv6 neighbor
```

ネイバー探索パラメータの設定

次のネイバー探索パラメータを設定できます。

- 重複アドレス検出試行回数
- 到達可能性時間
- 再送信タイマー



(注) これらのパラメータに、工場出荷時に定義されたデフォルトを使用することを推奨します。

この項では、次のトピックについて取り上げます。

- 「[重複アドレス検出試行回数](#)」(P.47-16)

- 「到達可能性時間」 (P.47-16)
- 「再送信時間」 (P.47-16)
- 「ネイバー探索パラメータ設定の確認」 (P.47-17)

重複アドレス検出試行回数

重複アドレス検出試行回数を設定するには、次の手順を実行します。

	コマンドまたはアクション	目的
ステップ1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ2	switch(config)# interface gigabitethernet 3/1 switch(config-if)#	インターフェイスを指定し、インターフェイスコンフィギュレーションサブモードを開始します。
ステップ3	switch(config-if)# ipv6 nd dad attempts 3	重複アドレス検出試行回数を 100 に設定します。範囲は 0 ~ 15 です。
ステップ4	switch(config-if)# no ipv6 nd dad attempts	デフォルト値 (0) に戻します。 (注) 試行回数を 0 に設定すると、ネイバー探索はディセーブルになります。

到達可能性時間

到達可能性時間を設定するには、次の手順を実行します。

	コマンドまたはアクション	目的
ステップ1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ2	switch(config)# interface gigabitethernet 3/1 switch(config-if)#	インターフェイスを指定し、インターフェイスコンフィギュレーションサブモードを開始します。
ステップ3	switch(config-if)# ipv6 nd reachability-time 10000	到達可能性時間を 10000 ミリ秒に設定します。範囲は 1000 ~ 3600000 ミリ秒です。
ステップ4	switch(config-if)# no ipv6 nd reachability-time	デフォルト値 (30000 ミリ秒) に戻します。

再送信時間

再送信時間を設定するには、次の手順を実行します。

	コマンドまたはアクション	目的
ステップ1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ2	switch(config)# interface gigabitethernet 3/1 switch(config-if)#	インターフェイスを指定し、インターフェイスコンフィギュレーションサブ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	switch(config-if)# ipv6 nd retransmission-timer 20000	再送信時間を 20000 ミリ秒に設定します。範囲は 1000 ~ 3600000 ミリ秒です。
ステップ 4	switch(config-if)# no ipv6 nd retransmission-timer	デフォルト値 (1000 ミリ秒) に戻します。

ネイバー探索パラメータ設定の確認

show ipv6 interface コマンドは、ネイバー探索パラメータの設定を表示します。

```
switch# show ipv6 interface mgmt 0
mgmt0 is up
IPv6 is enabled
Global address(es):
  2003::1/64
Link-local address(es):
  fe80::205:30ff:fe00:533e
ND DAD is enabled, number of DAD attempts: 5
ND reachable time is 50000 milliseconds
ND retransmission time is 3000 milliseconds
Stateless autoconfig for addresses disabled
```

IPv6 スタティック ルートの設定

Cisco MDS SAN-OS は、IPv6 のスタティック ルートをサポートしています。この項では、次のトピックについて取り上げます。

- 「IPv6 スタティック ルートの設定」 (P.47-17)
- 「IPv6 スタティック ルートの設定と動作の確認」 (P.47-18)

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を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。

IPv6 スタティック ルートを設定するには、次の手順を実行します。

	コマンドまたはアクション	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ipv6 route ::/0 gigabitethernet 3/1	ギガビットイーサネットインターフェイスのデフォルトのスタティック IPv6 ルートを設定します。
ステップ 3	switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 3/2	ギガビットイーサネットインターフェイスの完全指定 IPv6 スタティック ルートを設定します。

IPv6 スタティック ルートの設定と動作の確認

show ipv6 route コマンドは、スイッチの IPv6 ルート テーブルを表示します。

```
switch# show ipv6 route

IPv6 Routing Table
Codes: C - Connected, L - Local, S - Static G - Gateway
G   ::/0
    via fe80::211:5dff:fe53:500a, GigabitEthernet6/1, distance 2
G   ::/0
    via fe80::2d0:3ff:fe61:4800, mgmt0, distance 2
C   2000::/64
    via ::, mgmt0
C   2172:22::/64
    via ::, mgmt0, distance 2
C   3000:3::/64
    via fe80::205:30ff:fe01:7ed6, GigabitEthernet4/1
C   3000:4::/64
    via fe80::205:30ff:fe01:7ed6, GigabitEthernet4/1.250
C   3000:5::/64
    via fe80::213:1aff:fee5:e69b, GigabitEthernet5/4
C   3000:6::/64
    via fe80::213:1aff:fee5:e69b, GigabitEthernet5/4.250
C   3000:7::/64
    via fe80::205:30ff:fe01:7ed7, GigabitEthernet4/2
C   3000:8::/64
    via fe80::205:30ff:fe01:7ed7, GigabitEthernet4/2.250
C   3000:9::/64
    via fe80::213:1aff:fee5:e69e, port-channel 3
C   3000:10::/64
    via fe80::213:1aff:fee5:e69e, port-channel 3.250
C   5000:1::/64
    via fe80::205:30ff:fe01:3917, GigabitEthernet6/2
C   5000:1::/64
    via fe80::205:30ff:fe01:3918, port-channel 4
C   6000:1:1:1::/64
    via fe80::205:30ff:fe01:3916, GigabitEthernet6/1
C   7000:1::/64
    via fe80::205:30ff:fe01:3917, GigabitEthernet6/2.250
C   7000:1::/64
    via fe80::205:30ff:fe01:3918, port-channel 4.250
C   7000:1:1:1::/64
    via fe80::205:30ff:fe01:3917, GigabitEthernet6/2, distance 2
L   fe80::/10
    via ::
L   ff00::/8
    via ::
```

ギガビットイーサネットの IPv6-ACL に関する注意事項



ヒント

ギガビットイーサネットインターフェイスに IPv6-ACL がすでに設定されている場合、このインターフェイスをイーサネット PortChannel グループに追加できません。IPv6-ACL の設定については、[第 35 章「IPv4 および IPv6 のアクセスコントロールリストの設定」](#)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で IPv6-ACL を設定する際には、次の注意事項に従ってください。

- Transmission Control Protocol (TCP) または Internet Control Message Protocol (ICMP) だけを使用します。



(注) ユーザ データグラム プロトコル (UDP) や HTTP など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に関するルールを含む 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可能ですが、これらのルールは無効になります。

- インターフェイスをイネーブルにする前に、インターフェイスに IPv6-ACL を適用します。このようにすれば、トラフィックが流れ始める前にフィルタを適用できます。
- 次の条件を確認します。
 - **log-deny** オプションを使用する場合、1 秒ごとに記録されるメッセージ数は最大 50 です。
 - ギガビットイーサネットインターフェイスに **established** オプションを含む IPv6-ACL を適用すると、このオプションは無視されます。
 - 前から存在している TCP 接続に IPv6-ACL のルールを適用しても、このルールは無視されません。たとえば、A と B の間に既存の TCP 接続がある場合に、送信元が A で送信先が B のパケットをすべて廃棄する IPv6-ACL を適用しても、このルールは無効になります。

インターフェイスに対する IPv6-ACL の適用については、[第 35 章「IPv4 および IPv6 のアクセスコントロールリストの設定」](#)を参照してください。

IPv4 から IPv6 への移行

Cisco MDS SAN-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。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製ルータを設定する方法の詳細については、[Cisco IOS IPv6 Configuration Library](#)にある「[Implementing Tunneling for IPv6](#)」を参照してください。

IPv6 情報の表示

インターフェイスの IPv6 ネイバーについては、`show ips ipv6 neighbours interface` コマンドを使用します。

```
switch# show ips ipv6 neighbours interface gigabitethernet 6/1
IPv6 Address                               Age (min)  Link-layer Addr  State  Interface
fe80::211:5dff:fe53:500a                   0          0011.5d53.500a   S      Gigabi tEthernet6/1
```

インターフェイスの IPv6 プレフィックスについては、**show ips ipv6 prefix-list interface** コマンドを使用します。

```
switch# show ips ipv6 prefix-list interface gigabitethernet 6/1
Prefix                               Prefix-len  Addr
Valid Preferred
6000:1:1:1::                          64         ::
      2592000      604800
```

インターフェイスの IPv6 ルートについては、**show ips ipv6 interface** コマンドを使用します。

```
switch# show ips ipv6 route interface gigabitethernet 6/1
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, G - Gateway, M - Multicast
C 6000:1:1:1::/64 is directly connected, GigabitEthernet6/1
C 6000:1:1:1::/64 is directly connected, GigabitEthernet6/1
C fe80::/64 is directly connected, GigabitEthernet6/1
M ff02::/32 is multicast, GigabitEthernet6/1
G ::/0 via fe80::211:5dff:fe53:500a, GigabitEthernet6/1
```

インターフェイスの IPv6 ルータについては、**show ips ipv6 routers interface** コマンドを使用します。

```
switch# show ips ipv6 routers interface gigabitethernet 6/1
Addr                               Lifetime  Expire
fe80::211:5dff:fe53:500a          1800     1781
```

インターフェイスの IPv6 トラフィック統計情報については、**show ips ipv6 traffic interface** コマンドを使用します。

```
switch# show ips ipv6 traffic interface gigabitethernet 6/1
IPv6 statistics:
Rcvd: 5094 total
      0 bad header, 0 unknown option, 0 unknown protocol
      0 fragments, 0 total reassembled
      0 reassembly timeouts, 0 reassembly failures
Sent: 13625 generated
      0 fragmented into 0 fragments, 0 failed
      2 no route

ICMP statistics:
Rcvd: 1264 input, 0 checksum errors, 0 too short
      0 unknown info type, 0 unknown error type
      unreachable: 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
      734 group query, 0 group report, 0 group reduce
      0 router solicit, 528 router advert, 0 redirects
      0 neighbor solicit, 2 neighbor advert
Sent: 6045 output, 0 rate-limited
      unreachable: 0 routing, 0 admin, 0 neighbor, 1160 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, 1466 group report, 0 group reduce
      1 router solicit, 0 router advert, 0 redirects
      3412 neighbor solicit, 6 neighbor advert
```

デフォルト設定

表 47-2 は、IPv6 パラメータのデフォルト設定の一覧です。

表 47-2 デフォルト 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 (ネイバー探索はディセーブル)
到達可能性時間	1000 ミリ秒
再送信時間	30000 ミリ秒
IPv6-ACL	なし

