IPv6 の設定

この章は次のトピック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、Routing Information Protocol（RIP）、Integrated Intermediate System-to-Intermediate System（IS-IS）、IPv6 向け Open Shortest Path First（OSPF）、マルチプロトコル Border Gateway Protocol（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:BA98:7654:3210
```

```
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。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	2001:0:0:0:0:DB8:800:200C: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

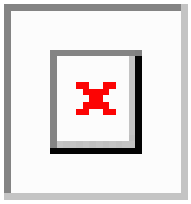
IPv6 ユニキャスト アドレスは、1 つのノード上の 1 つのインターフェイスの ID です。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。

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 リレー種別など）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）。

（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。

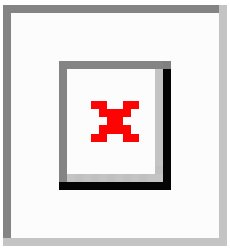
3. リンクローカル アドレスの作成にルータのシリアル番号を使用できない場合、ルータは MD5 ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

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。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。

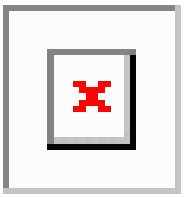
図 *2:* リンクローカル アドレス形式



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。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

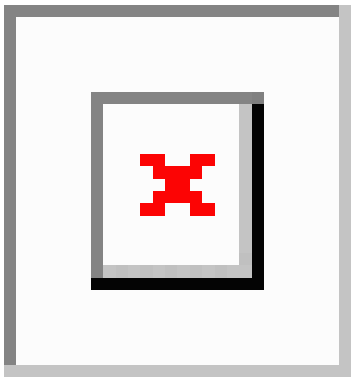
グできる場合もあります。アプリケーションは、一意のローカルアドレスをグローバルスコープのアドレスのように扱うことができます。

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。

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



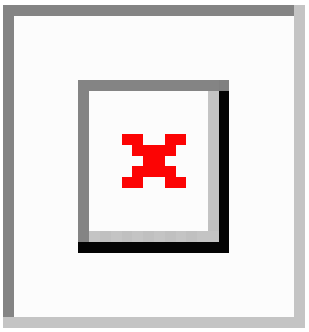
サイト ローカル アドレス

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。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。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。

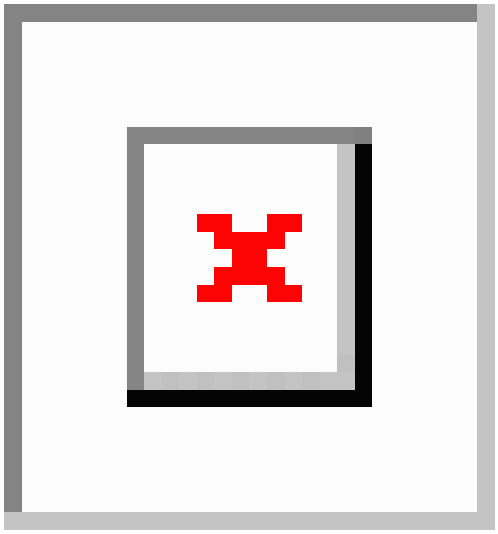
次の表に、基本 IPv6 パケット ヘッダーのフィールドをリストします。

表 *2 : base IPv6* パケット ヘッダー フィールド

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

フィールド	説明
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、下の図に示すように、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

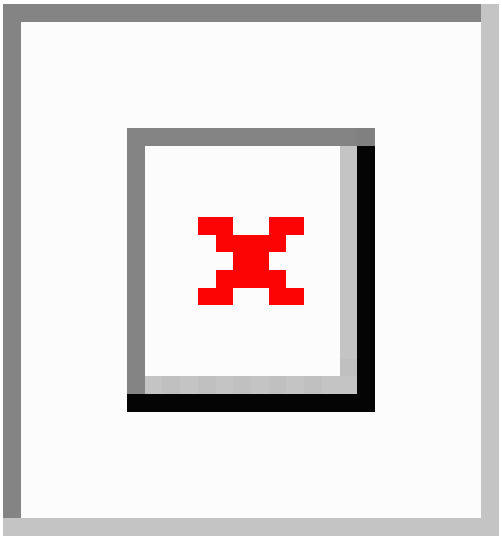


IPv6 拡張ヘッダー

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



下表に、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	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	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。
ルーティング	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	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。
認証	51	パケットのコネクションレス型整合性およびデータ発信元認証を提供するために使用されるヘッダー。

ヘッダー タイプ	次ヘッダーの値	説明
Encapsulation Security Payload	50	このヘッダーに続くすべての情報は暗号化されます。
モビリティ	135	モバイルIPv6サービスのサポートで使用されるヘッダー。
ホスト識別プロトコル	139	Host Identity Protocol バージョン 2（HIPv2）に使用されるヘッダー。IPマルチホーミングとモバイルコンピューティングをセキュアな方法で実現できるようにします。
シム 6	140	IPマルチホーミングに使用されるヘッダー。これにより、ホストを複数のネットワークに接続できます。
上位レイヤ 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 9000 Series 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（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

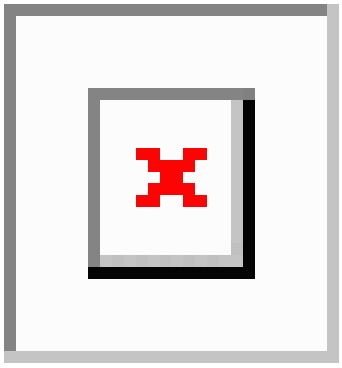
できないためにルータがパケットを転送できない場合、ルータは発信元ホストにICMPv6メッセージを送信します。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索およびパス MTU ディスカバリに使用されます。パス MTU ディスカバリ プロセスでは、特定のルートでサポートされる最大サイズを使用してパケットが送信されます。

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（下記の図を参照）。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（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、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。

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）。ノードは未指定の送信元アドレスと一時的なリンクローカル アドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカル アドレスを含むネイバーアドバタイズメントメッセージを返します。別のノードが同じアドレスの一意性を同時に検証している場合は、そのノードもネイバー送信要求メッセージを返します。ネイバー送信要求メッセージの返信としてネイバーアドバタイズメントメッセージが受信されず、同じ一時アドレスの検証を試行している他のノードからのネイバー送信要求メッセージも受信されない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンクローカル アドレスを一意であると見なし、そのアドレスをインターフェイスに割り当てます。

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。

IPv6 ステートレスアドレス自動構成（SLAAC）は、管理インターフェイスでのみ実行されます。たとえば、SLAAC が管理インターフェイスで有効になっている場合、リンク ローカル アドレス（LLA）が生成され、リンク ローカルアドレスに対して重複アドレス検出（DAD）が実行されます。重複アドレス検出プロセスが成功すると、インターフェイスは ICMPv6 ルータ要請（RS）パケットを送信します。RS パケットを受信するアップストリーム ルータは、ICMPv6 ルータ アドバタイズメント（RA）で応答します。RA パケットには、インターフェイスの MAC 情報と RA パケット内のアドバタイズされたプレフィックスを使用して、ダウンストリーム NX-OS スイッチがアドレスを自動生成するサブネットを伝送するプレフィックス TLV オプションがあります。Cisco NX-OS スイッチは、EUI-64 形式でアドレスを自動生成し、新しい自動生成されたアドレスで DAD を実行します。

IPv6 アドレスは、特定の時間だけインターフェイスに割り当てられます。各アドレスには、アドレスがインターフェイスに接続されている期間を示すライフタイムがあります。アップストリーム ルータから送信される RA パケットの TLV プレフィックスには、有効なライフタイムと優先ライフタイムに関する情報が含まれています。インターフェイスに割り当てられたアドレスは、2 つの異なるフェーズを通過します。最初は、アドレスは優先状態になります。これは、アドレスが任意の通信での使用に制限されないことを意味します。現在のインターフェイス バインディン

グが無効になると、アドレスは廃止状態になります。廃止状態では、アドレスの使用は推奨されません。必ずしも禁止されているわけではありません。サービスを中断せずに別のアドレスに切り替えることが困難なアプリケーションのみが、廃止されたアドレスを使用する必要があります。

IPv6 コンピューティング ノード IP 自動構成

K8s クラスタにオンボードし、スイッチとコンピューティング ノード間で eBGP ピアリングを確立する前に、接続されたコンピューティング ノードをノード IP を接続されたコンピューティング ノードに割り当てる必要があります。

Cisco NX-OS リリース 10.3(3)F 以降では、Cisco NX-OS 9000 シリーズ プラットフォーム スイッチで IPv6 コンピューティング ノード IP 自動構成のサポートが提供され、マルチホーム コンピューティング ノードにノード IP アドレスを割り当てて配布し、割り当てられたノードIPを使用して K8s クラスタに到達可能性を確立します。

（注） ただし、ノードアドレスの割り当てはSLAAC とは異なります。これは、SLAAC を介して実行されるレイヤ 3 インターフェイス サブネットでのインターフェイス アドレス プロビジョニングと直交する、ループバック インターフェイスに固有の IPv6 アドレスを割り当てる方法です。

この機能は、8505/6775 で定義されている標準に準拠しています。

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。ステートレス自動構成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（以下の図を参照）。

図 *10 : IPv6* ネイバー検出：*RA* メッセージ

RA メッセージは、全ノード マルチキャスト アドレスに送信されます。

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
- 完成可能な自動設定のタイプ（ステートレスまたはステートフル）を示すフラグのセット

- デフォルトルータ情報（アドバタイズメントを送信しているルータをデフォルトルータとして使用する必要があるかどうか、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、宛先へのパス上のより適切なファーストホップ ノードをホストに通知します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。

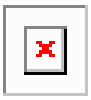
IPv6 エニーキャスト アドレス

エニーキャスト アドレスとは、異なるノードに属するインターフェイス一式に割り当てられたアドレスです。エニーキャストアドレスに送信されたパケットは、使用しているルーティングプロトコルの定義に従って、そのエニーキャスト アドレスが示す最も近いインターフェイスに送信されます。エニーキャストアドレスは、ユニキャストアドレス空間から割り当てられるため、その構文ではユニキャストアドレスと区別できません。ユニキャストアドレスを複数のインターフェイスに割り当てると、ユニキャスト アドレスがエニーキャスト アドレスとなります。属するエニーキャストアドレスが割り当てられたノードは、アドレスがエニーキャストアドレスであることを認識できるよう、設定する必要があります。

（注） エニーキャストアドレスを使用できるのは、ルータだけです。ホストはエニーキャストアドレスを使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスには使用できません。

次の図は、サブネット ルータ エニーキャスト アドレスのフォーマットを示します。このアドレスには、連続するゼロに連結されたプレフィックス（インターフェイス ID）があります。サブネット ルータ エニーキャスト アドレスを使用すると、サブネット ルータ エニーキャスト アドレスのプレフィックスが示すリンク上のルータに到達できます。

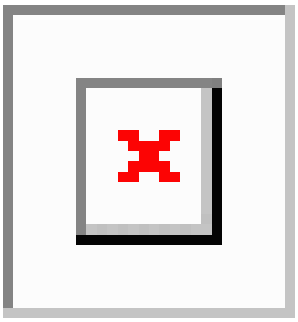
図 *12* : サブネット ルータ エニーキャスト アドレスの形式



IPv6 マルチキャスト アドレス

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、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。プレフィックスに続く 2 番めのオクテットで、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、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。次の図に、IPv6マルチキャストアドレスの形式を示します。

図 *13* : *IPv6* マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）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。

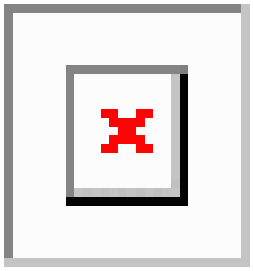
- 全ノード マルチキャスト グループ FF02:0:0:0:0:0:0:1（スコープはリンクローカル）
- 割り当てられたユニキャストアドレスおよびエニーキャストアドレスごとの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00:0000/104

IPv6 ルータは、全ルータ マルチキャスト グループ FF02:0:0:0:0:0:0:2（スコープはリンクローカル）にも加入する必要があります。

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 アドレスまたはエニー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およびエニー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 アドレスまたは IPv6 エニーキャスト アドレスの下位 24 ビットに連結されたプレフィックス FF02:0:0:0:0:1:FF00:0000/104 があります（下図を参照）。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 *14 : IPv6* 送信要求ノード マルチキャスト アドレス形式



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

LPMルーティングモード

デフォルトでは、Cisco NX-OSは、デバイス上で最長プレフィックス一致（LPM）を許可するように階層的にルーティングします。ただし、より多くの LPM ルート エントリをサポートするために、異なるルーティング モード用にデバイスを設定できます。

次の表に、Cisco Nexus 9300 シリーズおよび 9500 シリーズ スイッチでサポートされている LPM ルーティング モードを示します。

表 *5 : Cisco Nexus 9200* シリーズ スイッチ用の *LPM* ルーティング モード

LPM ルーティング モード	CLI コマンド
デフォルトのシステム ルーティング モード	
LPM デュアルホスト ルーティング モード	**system routing template-dual-stack-host-scale**
LPM ヘビー ルーティング モード	**system routing template-lpm-heavy**

（注） Cisco Nexus 9200 プラットフォーム スイッチは、IPv4 マルチキャスト ルートの **system routing template-lpm-heavy** モードをサポートしていません。LPM の上限を 0 にリセットしてください。

表 *6 : Cisco Nexus 9300* シリーズ スイッチ用の *LPM* ルーティング モード

LPM ルーティング モード	Broadcom T2モード	CLI コマンド
デフォルトのシステム ルーティング モード	3	
ALPM ルーティング モード	4	**system routing max-mode l3**

表 *7 : Cisco Nexus 9300-EX/FX/FX2/FX3/GX* プラットフォーム スイッチ用の *LPM* ルーティング モード

LPM ルーティング モード	CLI コマンド
LPM デュアルホスト ルーティング モード	**system routing template-dual-stack-host-scale**
LPM ヘビー ルーティング モード	**system routing template-lpm-heavy**
LPM インターネットピアリング モード)	**system routing template-internet-peering**

表 *8 : 9700-EX* および *9700-FX* ラインカードを搭載した *Cisco Nexus 9500* プラットフォーム スイッチ用 *LPM* ルーティング モード

LPM ルーティング モード	Broadcom T2モード	CLI コマンド
デフォルトのシステムルーティング モード	3（ラインカード用）。 4（ファブリック モジュール用）	
最大-ホスト ルーティング モード	2（ラインカード用）。 3（ファブリック モジュール用）	**system routing max-mode host**
非階層ルーティングモード	3（ラインカード用）。 max-l3-modeオプション付き4（ラインカード用）	**system routing non-hierarchical-routing [max-l3-mode]**
64 ビット ALPM ルーティング モード	モード4のサブモード（ファブリックモジュール用）	**system routing mode hierarchical 64b-alpm**

LPM ルーティング モード	Broadcom T2モード	CLI コマンド
LPM ヘビー ルーティング モード		**system routing template-lpm-heavy** （注） このモードは、9732C-EX ライン カードを搭載した Cisco Nexus 9508 スイッチでのみサポートされます。
LPMインターネットピアリング モード)		**system routing template-internet-peering** （注） このモードは、次の Cisco Nexus 9500 プラットフォーム スイッチでのみサポートされています。 • 9700-EX ライン カード搭載の Cisco Nexus 9500 プラットフォーム スイッチ • Cisco Nexus 9500-FX プラットフォーム スイッチ（Cisco NX-OS リリース 7.0(3)I7(4) 以降） • Cisco 9500-R プラットフォーム スイッチ（Cisco NX-OS リリース 9.3(1) 以降）
LPM デュアルホスト ルーティング モード		

表 *9 : 9600-R* ライン カードを搭載した *Cisco Nexus 9500-R* プラットフォーム スイッチの *LPM* ルーティング モード

LPM ルーティング モード	CLI コマンド
LPMインターネットピアリング モード)	**system routing template-internet-peering** （Cisco NX-OS リリース 9.3(1) 以降 ）

ホストから LPM へのスピルオーバー

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、ホストルートを LPM テーブルに保存して、より大きなホスト スケールを実現できます。ALPM モードでは、スイッチはより少ないホスト ルートを許可します。サポートされるスケールよりも多くのホストルートを追加すると、ホストテーブルからこぼれたルートは LPM テーブルの LPM ルートのスペースを使用します。このモードで許可される LPM ルートの総数は、保存されているホスト ルートの数だけ減少します。この機能は、Cisco Nexus 9300 および 9300 プラットフォーム スイッチではサポートされていません。

デフォルトのシステム ルーティング モードでは、Cisco Nexus 9300 プラットフォーム スイッチは、より高いホスト スケールとより少ない LPM ルート用に設定され、より多くのホスト ルートを保存するために LPM スペースを使用できます。Cisco Nexus 9500 プラットフォーム スイッチでは、デフォルトのシステム ルーティング モードと非階層型ルーティング モードのみがライン カードでこの機能をサポートします。ファブリック モジュールはこの機能をサポートしていません。

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 アドレッシングおよび IPv6 ヘッダー情報などの IPv6 の基本に関する詳しい知識が必要です。
- 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。

- インターネット ピアリング モードに設定された Cisco Nexus 9300-EX および Cisco Nexus 9300-FX2 プラットフォーム スイッチには、完全な IPv4 および IPv6 インターネット ルートを同時にインストールするための十分なハードウェア容量がない場合があります。
- 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。
- IPv6 LLA を使用するには、 **ing-sup** の TCAM リージョンをデフォルト値の 512 から 768 に再分割する必要があります。この手順では、コピー実行の開始とリロードが必要です。
- IPv6 スタティック ルートのネクストホップ リンクローカル アドレスは、どのローカル インターフェイスでも設定できません。
- リンク ローカル IPv6 アドレスを使用する場合は、BGP 更新ソースを定義する必要があります。
- 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 9500-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/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。
- LPM の重いルーティングモードは、**9700**-EX、-FX、および-GX シリーズモジュールを搭載した Cisco Nexus **9500** シリーズスイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3)F 以降、設定された間隔に基づいて IPv6 リダイレクト メッセージがトリガーされると、syslog が出力されます。
- Cisco NX-OS リリース 10.3(1)F 以降、スタティック ルーティングが Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、静的ルーティングが Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(1)F 以降、ダイナミック ルーティングが Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、ダイナミック ルーティングが Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(3)F 以降、IPv6 コンピューティング ノード IP 自動構成機能は、次の制限付きで Cisco NX-OS 9000 シリーズ プラットフォーム スイッチでサポートされます。
  - RA プレフィックスは、プレフィックス長が 64 のオフリンクとして構成する必要があります。

- マルチホーム コンピューティング ノードがある場合は、L1 スイッチと L2 スイッチの両方で同じ RA プレフィックスを構成する必要があります。

- Cisco NX-OS リリース 10.4(1)F 以降、ダイナミック ルーティングは、9808 および 9804 スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、スタティック ルーティングは、9808 および 9804 スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。

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. **ipv6 address** {*address* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*] or **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

手順

	コマンドまたはアクション	目的

Step 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。

Step 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。

	コマンドまたはアクション	目的

Step 3	**ipv6 address** {*address* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*] or **ipv6 address** *ipv6-address* **use-link-local-only**
	例：
	`switch(config-if)# ipv6 address 2001:0DB8::1/10`
	または
	`switch(config-if)# ipv6 address use-link-local-only`
		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。
		ipv6 address use-link-local-only を入力します。 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。

Step 4	（任意） **show ipv6 interface** 例： `switch(config-if)# show ipv6 interface`	IPv6 用に設定されたインターフェイスを表示します。
Step 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 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: 2001:db8:0000:0000:0218:baff:fed8:239d
     IPv6 subnet: 2001:db8::/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
```

最大ホスト ルーティング モードの設定（Cisco Nexus 9500 プラットフォーム スイッチのみ）

デフォルトでは、デバイスは階層方式で（モード4になるように設定されたファブリック モジュールとモード 3 になるように設定されたラインカード モジュールで）ルートをプログラミングし、デバイス上での最長プレフィクス照合（LPM）とホスト スケールが可能になります。

デフォルトの LPM およびホスト スケールを変更してシステム内のホストをさらにプログラミングできます。これは、ノードをレイヤ 2 ～ レイヤ 3 の境界ノードとして位置付けるときに必要になる場合があります。

（注） LPM テーブルのエントリをさらに拡大したい場合は、「非階層ルーティング モードの設定（Configuring Nonhierarchical Routing Mode (Cisco Nexus 9500 シリーズ スイッチのみ）」の項を参照して、ライン カード上のレイヤ 3 IPv4 および IPv6 ルートすべてをプログラミングしてファブリック モジュール上のルートはそのままにするようデバイスを設定します。

（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） 最大ホスト ルーティング モードのスケール数については、『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] system routing max-mode host**
3. （任意） **show forwarding route summary**
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

Step 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。

Step 2	[**no**] **system routing max-mode host** 例： `switch(config)# system routing max-mode host`	ライン カードを Broadcom T2 モード 2 に、ファブリック モジュールを Broadcom T2 モード 3 にして、サポートされるホスト数を増やします。
Step 3	（任意） **show forwarding route summary** 例： `switch(config)# show forwarding route summary`	LPM ルーティング モードを表示します。
Step 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。
Step 5	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

非階層ルーティング モードの設定（Cisco Nexus 9500 シリーズ スイッチのみ）

ホストの規模が小さい場合（純粋なレイヤ 3 配置の場合など）、コンバージェンス パフォーマンスを向上させるために、ラインカードの最長プレフィクス照合（LPM）のルートをプログラミングすることを推奨します。そうすることによって、ラインカードのルートおよびホストがプログラミングされ、ファブリック モジュールのルートはプログラミングされません。

（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。

手順の概要

1. **configure terminal**

2. [**no**] **system routing non-hierarchical-routing** [**max-l3-mode**]
3. （任意） **show forwarding route summary**
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

Step 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。

Step 2	[**no**] **system routing non-hierarchical-routing** [**max-l3-mode**] 例： `switch(config)# system routing non-hierarchical-routing max-l3-mode`	ラインカードを Broadcom T2モード 3（または **max-l3-mode** オプションを使用している場合は Broadcom T2 モード 4）にし、より大きな LPM スケールをサポートします。その結果、IPv4 および IPv6 ルートのすべてが、ファブリック モジュールではなくラインカードでプログラミングされます。

Step 3	（任意） **show forwarding route summary**
	例：
	`switch(config)# show forwarding route summary`
	`Mode 3:`
	`120K IPv4 Host table`
	`16k LPM table (> 65 < 127 1k entry reserved)`
	`Mode 4:`
	`16k V4 host/4k V6 host`
	`128k v4 LPM/20K V6 LPM`
		LPM モードを表示します。

Step 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。
Step 5	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

64 ビット ALPM ルーティング モードの設定（Cisco Nexus 9500 プラットフォーム スイッチのみ）

64 ビットアルゴリズム最長プレフィックス一致（ALPM）機能を使用して、IPv4 および IPv6 ルートテーブルエントリを管理できます。64 ビット ALPM ルーティング モードでは、デバイスに保存できるルート エントリの数が増加します。このモードでは、次のいずれかをプログラムできます。

- 80,000 IPv6 エントリ、IPv4 エントリなし
- IPv6 エントリなし、128,000 の IPv4 エントリ
- *x* 個の IPv6 エントリと IPv4 エントリ（2*x* + *y* の場合）

（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） 64 ビット ALPM ルーティング モードのスケール数については、『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] system routing mode hierarchical 64b-alpm**
3. （任意） **show forwarding route summary**
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

Step 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。

Step 2	**[no] system routing mode hierarchical 64b-alpm** 例： `switch(config)# system routing mode hierarchical 64b-alpm`	マスク長が 64 以下のすべての IPv4 および IPv6 LPM ルートをファブリック モジュールにプログラミングします。IPv4 および IPv6 のすべてのホスト ルート、

	コマンドまたはアクション	目的
		およびマスク長が 65 ～ 127 であるすべての LPM ルートがライン カードでプログラミングされます。
Step 3	（任意） **show forwarding route summary** 例： `switch(config)# show forwarding route summary`	LPM モードを表示します。
Step 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。
Step 5	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

ALPM ルーティング モードの設定（Cisco Nexus 9300 プラットフォーム スイッチのみ）

Cisco Nexus 9300 プラットフォーム スイッチは、多数の LPM ルート エントリをサポートするように設定できます。

（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） ALPM ルーティング モードのスケール数については、『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] system routing max-mode l3**
3. （任意） **show forwarding route summary**
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

Step 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。

Step 2	[**no**] **system routing max-mode l3** 例： `switch(config)# system routing max-mode l3`	デバイスを Broadcom T2 モード 4にして、より大きな LPM スケールをサポートします。
Step 3	（任意） **show forwarding route summary** 例： `switch(config)# show forwarding route summary`	LPM モードを表示します。
Step 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。
Step 5	**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 ip 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

Step 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。

Step 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。

Step 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`	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。 • **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**：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**：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。

	コマンドまたはアクション	目的
		• **ra-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**：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にします。 （注） IPv6 リダイレクトを無効にする場合は、一部の IPv6 パケットが CPU にリークされる可能性があるため、IPv4 リダイレクトも無効にする必要があります。 • **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。
Step 4	（任意） **show ip nd interface** 例： `switch(config-if)# show ip 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。
Step 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 インターフェイスを表示する例を示します。

```
switch# configure terminal
switch(config)# 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。

表 10：

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。

コマンド	目的
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。

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。

表 *11*:

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 ステートレス自動構成の定義

手順の概要

1. **configure terminal**
2. **interface management** *number*
3. **ipv6 address autoconfig**
4. **ipv6 address autoconfig default**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	**configure terminal** 例: `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
Step 2	**interface management** *number* 例: `switch(config)# interface mgmt0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
Step 3	**ipv6 address autoconfig** 例: `switch(config-if)# ipv6 address autoconfig`	管理インターフェイスでステートレス自動構成を使用して、IPv6 アドレスの自動構成を有効にします。
Step 4	**ipv6 address autoconfig default** 例: `switch(config-if)# ipv6 address autoconfig default`	管理インターフェイスでステートレス自動構成を使用して IPv6 アドレスの自動構成を有効にし、ルータ アドバタイズメントで受信したリンクローカル アドレスのネクストホップを持つデフォルト ルートを追加します。

例

次に、show ipv6 interface コマンドを使用して、管理インターフェイスで IPv6 アドレスが構成されていることを表示および確認する例を示します。[情報（Information）] には、SLAAC で生成されたアドレスを含む、インターフェイスに構成されているすべての IPV6 アドレスが表示されます。また、ステートレス アドレスの自動構成がインターフェイスで有効になっているかどうかも示します。

```
Device# show ipv6 interface mgmt 0

IPv6 Interface Status for VRF "management"(2)
mgmt0, Interface status: protocol-up/link-up/admin-up, iod: 2
IPv6 address:
1955::2f6:63ff:fe8b:c9f8/64 [VALID]
IPv6 subnet: 1955::/64
IPv6 link-local address: fe80::2f6:63ff:fe8b:c9f8 (default) [VALID]
…..
Stateless autoconfig configured on the interface
```

This example shows how to use the show ipv6 route vrf management command to display the IPv6 routing table for VRF management:

```
Device# show ipv6 route vrf management

IPv6 Routing Table for VRF "management"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
0::/0, ubest/mbest: 1/0
*via fe80::2f6:63ff:fe8b:c9ff, mgmt0, [2/0], 00:02:00, icmpv6
1955::/64, ubest/mbest: 1/0, attached
*via 1955::2f6:63ff:fe8b:c9f8, mgmt0, [0/0], 15:59:22, direct,
1955::2f6:63ff:fe8b:c9f8/128, ubest/mbest: 1/0, attached
*via 1955::2f6:63ff:fe8b:c9f8, mgmt0, [0/0], 15:59:22, local
```

This example shows how to use the show ipv6 nd int mgmt command to display the ICMPv6 ND interfaces for VRF management:

```
Device# show ipv6 nd int mgmt 0

ICMPv6 ND Interfaces for VRF "management"
mgmt0, Interface status: protocol-up/link-up/admin-up
IPv6 address:
1955::2f6:63ff:fe8b:c9f8/64 [VALID]
IPv6 link-local address: fe80::2f6:63ff:fe8b:c9f8 [VALID]
…….
Subnets configured via SLAAC and their states:
Prefix 1955::/64[PREFERRED] Preferred lifetime left: 6d23h Valid lifetime lef
t: 4w1d
```

LPMヘビールーティングモードの設定（CiscoNexus9200および9300-EX プラットフォーム スイッチおよび 9732C-EX ライン カードのみ）

Cisco NX-OS リリース 7.0(3)I4(4) 以降では、極めて多くの LPM ルート エントリをサポートするために LPM のヘビー ルーティング モードを設定できます。このルーティング モードをサポートするのは、Cisco Nexus 9200 および 9300-EX シリーズのスイッチと、9732C-EX ライン カードを搭載した Cisco Nexus 9508 スイッチだけです。

（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ヘビー ルーティング モードのスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] system routing template-lpm-heavy**
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

Step 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。

Step 2	**[no] system routing template-lpm-heavy** 例： `switch(config)# system routing template-lpm-heavy`	デバイスをLPMヘビー ルーティング モードにして、より大きなLPM スケールをサポートします。

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

Step 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。
Step 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 モードの設定（Cisco Nexus 9500-R プラットフォーム スイッチ、Cisco Nexus 9300-EX プラッ

トフォーム スイッチ、および Cisco Nexus 9000 シリーズ スイッチと 9700-EX ライン カードのみ）

Cisco NX-OS リリース7.0(3)I6(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。Cisco Nexus 9300-EX プラットフォーム スイッチおよび 9700-EXライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチのみこのルーティング モードをサポートしています。

Cisco NX-OS リリース 9.3(1) 以降、Cisco Nexus 9500-R プラットフォーム スイッチはこのルーティング モードをサポートします。

（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 9000 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 9500-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 9500-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

Step 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。

	コマンドまたはアクション	目的
Step 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。

Step 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。

Step 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。
Step 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
Step 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

Step 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。

Step 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。

Step 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。 （注） Cisco Nexus リリース 10.2(2)F 以降、このコマンドは 32 ビット バージョンのソフトウェアにのみ適用されます。

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

Step 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。
Step 7	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

LPM デュアルホスト ルーティング モードの設定（Cisco Nexus 9200 および 9300-EX プラットフォーム スイッチ）

より多くの LPM ルート エントリをサポートするために、LPM ヘビー ルーティング モードを設定できます。このルーティング モードをサポートするのは、Cisco Nexus 9200 および 9300-EX プラットフォーム スイッチと、9732C-EX ライン カードを搭載した Cisco Nexus 9508 スイッチだけです。

（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 ヘビー ルーティング モードのスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] system routing template-lpm-heavy**
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

Step 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。

Step 2	**[no] system routing template-lpm-heavy** 例： `switch(config)# system routing template-lpm-heavy`	デバイスを LPM ヘビー ルーティング モードにして、より大きな LPM スケールをサポートします。

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

	コマンドまたはアクション	目的
Step 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。
Step 5	**reload** 例： `switch(config)# reload`	デバイス全体をリブートします。

IPv6 リダイレクト Syslog の構成

IPv6 リダイレクト Syslog を有効/無効にするか、ログ間隔を変更するには、次の CLI を使用します。

（注） デフォルトでは、syslog のリダイレクトが有効になっています。

手順の概要

1. **configure terminal**
2. **ipv6 redirect syslog** [<*value*>]
3. （任意） **no ipv6 redirect syslog**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 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

Step 2	**ipv6 redirect syslog** [<*value*>]
	例：
	`switch(config)# ip redirect syslog 60`
	`switch(config)#`
		過剰な IPv6 リダイレクト メッセージの syslog を構成します。
		• **ipv6 redirect syslog**: IPv6 リダイレクト メッセージの syslog を有効にします。
		• *value*: ログ間隔を設定します。範囲は最小 30 秒から最大 1800 秒です。デフォルト インターバルは 60 秒です。

	コマンドまたはアクション	目的
Step 3	（任意） **no ipv6 redirect syslog** 例： `switch(config)# no ipv6 redirect syslog`	過剰な IPv6 リダイレクト メッセージの syslog を無効にします。

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 system routing mode	LPM ルーティング モードを表示します。
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。
show ipv6 nd addr-registry	コンピューティング ノードの IPv6 アドレス レジストリ エントリを表示します。

IPv6 の設定例

次の例は IPv6 の設定方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# ipv6 address 2001:db8::/64 eui64
switch(config-if)# 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。