ネットワーク スタック IPv4 および IPv6 の実装

ネットワーク スタック IPv4 および IPv6 機能は、インターネット プロトコル バージョン 4（IPv4）およびインターネット プロトコル バージョン 6（IPv6）の設定とモニタリングに使用します。

制約事項

IPv6 に対応している Cisco IOS XR ソフトウェア リリースでは、1 つのインターフェイス上に複数の 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。

フォールバック VRF の実装

仮想ルーティングおよびフォワーディング（VRF）は、同じルータ上にルーティングテーブルの複数のインスタンスが同時に存在できるようにする IP テクノロジーです。ルーティング インスタンスは独立しているため、同じ IP アドレスを競合することなく使用できます。

データ パケットの宛先プレフィックスが、設定されている VRF のどのルートとも一致しない場合、グローバル ルーティング テーブルからデフォルト ルートが識別されます。ただし、デフォルト ルートを使用するには明示的なネクスト ホップが必要なため、効率的でない可能性があります。フォールバック VRF ルートを設定することをお勧めします。宛先が VRF テーブルで一致しない場合は、フォールバック VRF テーブルが使用されます。フォールバック VRF には、グローバル ルーティング テーブルまたは非グローバル VRF テーブルを使用できます。

制約事項

フォールバック VRF ルートを設定する場合は、次の制約事項が適用されます。

- フォールバック VRF ルートは、各プライマリ VRF のアドレス ファミリごとに 1 つのみ設定できます。
- LPTS 受信トラップはサポート対象外であるため、ping、トレースルート、または低速パス アプリケーションはフォールバック VRF でサポートされません。
- Cisco NCS 560 シリーズ ルータでは、1000 の VRF と 1 つのグローバル テーブルのみがサポートされます。
- VRF へのスタティック デフォルト ルートを設定すると、このスタティック デフォルト ルートがフォールバック VRF よりも優先されます。VRF のデフォルト ルートを設定すると、ルート ルックアップにグローバル ルーティング テーブルが使用されます。デフォルト ルートは、設定済みのネクスト ホップに必ず転送されます。
- プライマリ VRF でパケットのルート ルックアップが失敗した場合、フォールバック VRF でルートルックアップを実行するためにパケットがリサイクルされます。したがって、パケットのルーティング パフォーマンスが最大で 50% 低下します。
- パケットの ACL ベース転送（ABF）VRF リダイレクトと VRF フォールバックの両方を設定すると、パケットは2回リサイクルされます。したがって、パケットのルーティング パフォーマンスが最大で 33% 低下します。
- フォールバック VRF でパケットのルートが見つかった場合、グリーニング IPv4 およびグリーニング IPv6 隣接関係パケットのみが正常にパントされます。
- ループ設定では、パケットのルートがプライマリとフォールバックのどちらの VRF でも見つからない場合、パケットはリサイクルパスでループします。最終的にパケットはリサイクル出力キューにドロップされます。リサイクル キューの優先順位が最も高いため、ループしているトラフィックのレートが高いと、他の正常なリサイクルパケットがドロップされる可能性があります。

ネットワーク スタック IPv4 および IPv6 の例外

Cisco IOS XR ソフトウェアでのネットワーク スタック機能には、次の例外があります。

- Cisco IOS XR ソフトウェアでは、**clear ipv6 neighbors** および **show ipv6 neighbors** コマンドに **location** *node-id* キーワードが含まれています。場所を指定した場合、指定した場所の隣接エントリのみが表示されます。
- **ipv6 nd scavenge-timeout** コマンドは、stale 状態の隣接エントリの有効期間を設定します。隣接エントリの廃棄タイマーの有効期間が切れると、そのエントリはクリアされます。
- Cisco IOS XR ソフトウェアでは、**show ipv4 interface** および **show ipv6 interface** コマンドに **location** *node-id* キーワードが含まれています。場所を指定した場合、指定した場所のインターフェイス エントリのみが表示されます。
- Cisco IOS XR ソフトウェアでは、設定時に、競合する IP アドレス エントリが許可されます。アクティブな 2 つのインターフェイスの間に IP アドレス競合が存在する場合、Cisco

IOS XR ソフトウェアは、設定されている競合ポリシーに従って、インターフェイスを停止します（デフォルト ポリシーでは、より高いインターフェイス インスタンスを停止します）。

IPv4 および IPv6 機能

Cisco IOS XR ソフトウェアが IPv4 と IPv6 の両方のアドレスを使用して設定されている場合、インターフェイスは IPv4 と IPv6 の両方のネットワーク上のデータを送受信できます。

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。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。IPv6 プレフィックス集約、簡略化されたネットワーク リナンバリング、および IPv6 サイト マルチホーミング機能によって、より効率的なルーティングを実現する IPv6 アドレッシング階層が提供されます。IPv6 は、Open Shortest Path First（OSPF）やマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）など、広く導入されているルーティング プロトコルをサポートしています。

IPv6 ネイバー探索（nd）プロセスでは、インターネット制御メッセージ プロトコル（ICMP）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（ローカル リンク）上のネイバーのリンク層アドレスを判断し、ネイバーに到達可能かどうかを確認し、隣接ルータを追跡します。

Cisco IOS XR ソフトウェアの IPv6

以前は IPng（次世代）と呼ばれていた IPv6 は、インターネット プロトコル（IP）の最新バージョンです。IP は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。IP バージョン 4（IPv4）の 32 ビット アドレッシング方式ではインターネットの成長の需要を十分に満たせないことが明らかになったときに、IPv6 が提案されました。長い議論の後で、IP を IPng のベースにするが、はるかに大きなアドレス空間と、簡略化されたメイン ヘッダーや拡張ヘッダーなどの改善を追加することが決定されました。IPv6 は、Internet Engineering Task Force（IETF）から発行されている RFC 2460、『*Internet Protocol, Version 6 (IPv6) Specification*』で最初に規定されました。IPv6 でサポートされるアーキテクチャとサービスについては他の RFC で規定されています。

ネットワーク スタック IPv4 および IPv6 の実装方法

ここでは、次の手順について説明します。

IPv4 アドレス指定の設定

IP を設定するための基本的かつ必須のタスクは、IPv4 アドレスをネットワーク インターフェイスに割り当てることです。こうすることで、インターフェイスがイネーブルになり、IPv4 を使用するこれらのインターフェイスでホストとの通信が可能になります。IP アドレスは IP データグラムの送信先を特定します。インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ アドレスを設定できます。ソフトウェアにより生成されるパケットは、必ずプライマリ IPv4 アドレスを使用します。そのため、セグメントのすべてのネットワーキング デバイスは、同じプライマリ ネットワーク番号を共有する必要があります。

このタスクに関連付けられているのは、IP アドレスのサブネット化およびマスキングに関する決定です。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネットマスクと呼ばれます。

（注） シスコでは、ネットワーク フィールドに対して左寄せの連続ビットを使用するネットワーク マスクのみをサポートしています。

設定例

IPv4 アドレス 192.168.1.27 とネットワーク マスク「/8」が、**インターフェイス HundredGigE 0/9/0/1** に割り当てられます。

（注） 4 分割ドット付き 10 進表記のアドレスでネットワーク マスクを指定します。たとえば、255.0.0.0 は、1 に等しい各ビットが、ネットワーク アドレスに属した対応するアドレス ビットを意味することを示します。ネットワーク マスクは、スラッシュ（/）および数字、つまり、プレフィックス長として示される場合もあります。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。スラッシュは 10 進数値の前に置かれ、IP アドレスとスラッシュの間にスペースは入りません。

```
Router#configure HundredGigE0/9/0/1
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 192.168.1.27/8
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
 ipv4 address 192.168.1.27 255.0.0.0
!
```

確認

HundredGigEインターフェイスがアクティブであり、IPv4がイネーブルであることを確認します。

```
Router# show ipv4 interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.168.1.27/8
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

関連コマンド

- ipv4 address
- show ipv4 interface

IPv6 アドレッシングの設定

ルータでのIPv6トラフィックのグローバル転送を可能にするため、IPv6アドレスは個々のルータインターフェイスに設定されます。デフォルトでは、IPv6アドレスは設定されていません。

（注） **ipv6 address** コマンドの *ipv6-prefix* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。

ipv6 address コマンドの **/prefix-length** 引数には、プレフィックスを構成しているアドレスの連続する上位ビットの数（アドレスのネットワーク部）を示す 10 進数の値を指定します。10 進値の前にはスラッシュが必要です。

ipv6 address link-local コマンドの *ipv6-address* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。

IPv6 マルチキャスト グループ

インターフェイスで IPv6 トラフィックを転送できるようにするには、そのインターフェイスで IPv6 アドレスを設定する必要があります。インターフェイスにグローバル 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 FF02:0:0:0:0:1: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
- 全ルータ リンクローカル マルチキャスト グループ FF02::2

（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。

設定例

IPv6 アドレス 2001:0DB8:0:1::1/64 が、**インターフェイス HundredGigE 0/9/0/1** に割り当てられます。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address 2001:0DB8:0:1::1/64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
 ipv4 address 192.168.1.27 255.0.0.0
 ipv4 address 1.0.0.1 255.255.255.0 secondary
 ipv4 address 2.0.0.1 255.255.255.0 secondary
 ipv6 address 2001:db8:0:1::1/64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
  Global unicast address(es):
    2001:db8:0:1::1, subnet is 2001:db8:0:1::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ffa6:1c75 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
  Table Id is 0xe0800000
```

```
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- ipv6 address
- interface
- show ipv6 interface

設定例

IPv6 アドレス 2001:0DB8:0:1::/64 が、**インターフェイス HundredGigE 0/9/0/1** に割り当てられます。**eui-64** キーワードを指定して、IPv6 アドレスの下位 64 ビットにインターフェイス識別子（ID）を含むサイトローカルおよびグローバル IPv6 アドレスを設定します。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。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
 ipv4 address 192.168.1.27 255.0.0.0
 ipv4 address 1.0.0.1 255.255.255.0 secondary
 ipv4 address 2.0.0.1 255.255.255.0 secondary
 ipv6 address 2001:db8:0:1::/64 eui-64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
  Global unicast address(es):
    2001:db8:0:1:c672:95ff:fea6:1c75, subnet is 2001:db8:0:1::/64
  Joined group address(es): ff02::1:ffa6:1c75 ff02::2 ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
  Table Id is 0xe0800000
```

```
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- ipv6 address
- interface
- show ipv6 interface

設定例

IPv6 アドレス FE80::260:3EFF:FE11:6770 が、**インターフェイス HundredGigE 0/9/0/1** に割り当てられます。link-local キーワードを指定して、リンクローカルアドレスをインターフェイスに設定します。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。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address FE80::260:3EFF:FE11:6770 link-local
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1
 ipv6 address fe80::260:3eff:fe11:6770 link-local
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 がリンクローカルアドレスで有効になっていることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::260:3eff:fe11:6770
  Global unicast address(es):
    2001:db8:0:1:260:3eff:fe11:6770, subnet is 2001:db8:0:1::/64
  Joined group address(es): ff02::1:ff11:6770 ff02::2 ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
```

```
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- ipv6 address
- interface
- show ipv6 interface

設定例

明示的な IPv6 アドレスが設定されていない**インターフェイス HundredGigE 0/9/0/1** での IPv6 の処理を有効にします。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 enable
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
ipv6 enable
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
  No global unicast address is configured
  Joined group address(es): ff02::1:ffa6:1c75 ff02::2 ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- ipv6 enable
- interface
- show ipv6 interface

ネットワーク インターフェイスへの複数の IP アドレスの割り当て

Cisco IOS XR ソフトウェアは、インターフェイスごとに複数の IP アドレス（セカンダリ アドレス）をサポートしています。セカンダリ アドレスは無制限に指定できます。セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合があります。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホスト アドレスが必要になるとします。ルータまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- 多くの旧式ネットワークは、レベル 2 ブリッジを使用して構築され、サブネット化されませんでした。セカンダリ アドレスは、慎重に使用することで、サブネット化されたルータベース ネットワークへの移行に役立ちます。旧式のブリッジ セグメントのルータで、そのセグメントに複数のサブネットがあることを簡単に認識されるようにできます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。別のネットワークによって物理的に分離された複数のサブネットから、セカンダリ アドレスを使用して、1 つのネットワークを作成できます。このような場合、最初のネットワークは、2 番めのネットワークの上に拡張されます。つまり、上の階層となります。サブネットは、同時に複数のアクティブなインターフェイス上に表示できないことに注意してください。

（注） ネットワーク セグメント上の任意のルータがセカンダリ IPv4 アドレスを使用した場合、同一のセグメント上にある他のルータもすべて、同一のネットワークまたはサブネットからセカンダリ アドレスを使用する必要があります。

注意 ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。

設定例

セカンダリ IPv4 アドレス 192.168.1.27 が Hundredgige インターフェイス 0/0/0/1 に割り当てられます。

注：IPv6 の場合は、**secondary** キーワードを指定せずに、インターフェイスに複数の IPv6 アドレスを設定できます。

```
Router# configure
Router(config)# interface HundredGigE 0/9/0/1
Router(config-if)# ipv4 address 192.168.1.27 255.255.255.0 secondary
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1
 ipv4 address 192.168.1.27 255.255.255.0 secondary
!
```

確認

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is unassigned
  Secondary address 192.168.1.27/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

関連コマンド

- ipv4 address
- show ipv4 interface

IPv4 および IPv6 プロトコル スタックの設定

このタスクでは、IPv4 と IPv6 の両方のプロトコル スタックをサポートするようにシスコのネットワーク デバイスのインターフェイスを設定します。

シスコのネットワーク デバイスのインターフェイスが IPv4 アドレスと IPv6 アドレスの両方で設定されている場合、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転送します。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。

設定例

インターフェイス HundredGigE 0/9/0/1 に IPv4 アドレス 192.168.99.1 と IPv6 アドレス 2001:0DB8:c18:1::3/64 を設定します。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 192.168.99.1 255.255.255.0
Router(config-if)#ipv6 address 2001:0DB8:c18:1::3/64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router# show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
 ipv4 address 192.168.99.1 255.255.255.0
 ipv6 address 2001:db8:c18:1::3/64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv4 と IPv6 が有効になっていることを確認します。

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.168.99.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000

Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
  Global unicast address(es):
   2001:db8:c18:1::3, subnet is 2001:db8:c18:1::/64
  Joined group address(es): ff02::1:ff00:3 ff02::1:ffa6:1c75 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- ipv4 address
- ipv6 address
- show ipv4 interface
- show ipv6 interface

アンナンバード インターフェイス上での IPv4 処理のイネーブル化

ここでは、明示的な IP アドレスをインターフェイスに割り当てることなく、IPv4 ポイントツーポイント インターフェイスをイネーブルにするプロセスについて説明します。アンナンバード インターフェイスがパケットを生成する場合（たとえば、ルーティング アップデートのため）は必ず、IP パケットの送信元アドレスとして指定したインターフェイスのアドレスが使用されます。また、アンナンバードインターフェイスを介してアップデートを送信するルーティング プロセスを判別する場合、指定されたインターフェイスのアドレスが使用されます。その制限を次に示します。

- High-Level Data Link Control（HDLC）、PPP、およびフレーム リレーのカプセル化を使用するインターフェイスには、アンナンバードを設定できます。フレーム リレー カプセル化を使用するシリアルインターフェイスにもアンナンバードを設定できますが、そのインターフェイスはポイントツーポイント サブインターフェイスでなければなりません。
- インターフェイスには IP アドレスがないため、ping EXEC コマンドを使用してインターフェイスがアップ状態かどうかを確認することはできません。簡易ネットワーク管理プロトコル（SNMP）は、インターフェイス ステータスのリモートでのモニタリングに使用できます。
- IP セキュリティ オプションは、アンナンバード インターフェイス上でサポートできません。

Intermediate System-to-Intermediate System（IS-IS）をシリアル回線全体で設定する場合、シリアル インターフェイスをアンナンバードとして設定し、それにより、各インターフェイス上で IP アドレスは必須ではないことを規定している RFC 1195 に準拠することができます。

設定例

明示的な IP アドレスを割り当てることなく、IPv4 ポイントツーポイント インターフェイスをイネーブルにします。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 unnumbered loopback 0
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
 ipv4 point-to-point
```

```
 ipv4 unnumbered Loopback0
!
```

確認

```
Router#show interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is up, line protocol is up
  Interface state transitions: 5
  Hardware is Hundredgige, address is 00e2.2a33.445b (bia 00e2.2a33.445b)
  Layer 1 Transport Mode is LAN
  Internet address is 10.0.0.2/32
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability 255/255, txload 194/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  Last link flapped 01:38:49
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters 02:34:16
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 7647051000 bits/sec, 12254894 packets/sec
     1061401410 packets input, 82789675614 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 5 broadcast packets, 19429 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     76895885948 packets output, 6192569128048 bytes, 0 total output drops
     Output 7 broadcast packets, 18916 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions

Router #show run int lo 0
interface Loopback0
 ipv4 address 10.0.0.2 255.255.255.255
```

関連コマンド

- ipv4 unnumbered
- show interfaces

IPv4 ICMP レート制限

IPv4 ICMP レート制限機能では、IPv4 ICMP 宛先到達不能メッセージが生成されるレートを制限します。Cisco IOS XR ソフトウェアは、通常の宛先到達不能メッセージ用と DF 宛先到達不能メッセージ用の2つのタイマーを保守します。これらは同じ時間制限およびデフォルトを共有します。DF キーワードが設定されていない場合、icmp ipv4 rate-limit unreachable コマンドによって DF 宛先到達不能メッセージの時間値が設定されます。DF キーワードが設定されている場合、その時間値は、通常の宛先到達不能メッセージの時間値とは無関係のままになります。

設定例

IPv4 ICMP 宛先到達不能メッセージが 1,000 ミリ秒ごとに生成されるレートを制限します。

DF キーワードは、コード 4 フラグメンテーションが必要で、Don't Fragment（DF）が設定されているときに ICMP 宛先到達不能メッセージの IP ヘッダーに指定されているように ICMP 宛先到達不能メッセージを送信するレートを任意で制限します。

```
Router#configure
Router(config)#icmp ipv4 rate-limit unreachable 1000
Router(config)#icmp ipv4 rate-limit unreachable DF 1000
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in icmp
Building configuration...
icmp ipv4 rate-limit unreachable DF 1000
icmp ipv4 rate-limit unreachable 1000
```

確認

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.85.1.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1 224.0.0.2
      224.0.0.5 224.0.0.6
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

送信または受信する ICMP 到達不能メッセージの数は、**show ipv4 traffic** コマンドを使用して指定できます。

```
Router# show ipv4 traffic
ICMP statistics:
  Sent: 0 admin unreachable, 5 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        5 total
  Rcvd: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        0 total, 0 checksum errors, 0 unknown
```

関連コマンド

- icmp ipv4 rate-limit unreachable
- show ipv4 traffic

IPv6 ICMP レート制限

IPv6 ICMP レート制限機能によって、IPv6 ICMP エラー メッセージがネットワークへ送信されるレートを制限するためのトークン バケット アルゴリズムが実装されます。IPv6 ICMP レート制限の初期の実装では、エラーメッセージ間に固定の間隔が定義されていましたが、traceroute などの一部のアプリケーションでは、間断なく送信される要求のグループへの返信が必要になる場合があります。エラー メッセージ間の固定間隔は、traceroute などのアプリケーションで動作するのに十分な柔軟性がなく、アプリケーションが失敗する原因となることがあります。トークンバケット方式を実装すると、複数のトークンを仮想バケットに格納できます。トークンごとに1つのエラーメッセージを送信できます。バケットに格納できるトークンの最大数を指定でき、エラー メッセージが送信されるたびに 1 つのトークンがバケットから削除されます。一連のエラー メッセージが生成された場合は、バケットが空になるまでエラー メッセージを送信できます。トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラーメッセージは送信されません。トークン バケット アルゴリズムは、レート制限の平均時間間隔を増やさず、固定時間間隔方式よりも柔軟性が高くなります。

設定例

50 ミリ秒の間隔と、20 トークンのバケット サイズを IPv6 ICMP エラー メッセージに設定します。

- milliseconds 引数では、トークンがバケットに追加される間隔を指定します。
- オプションの bucketsize 引数では、バケットに格納されるトークンの最大数を定義します。

```
Router#configure
Router(config)#ipv6 icmp error-interval 50 20
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config
Building configuration...
!! IOS XR Configuration version = 6.0.0.26I
!! Last configuration change at Mon Dec 14 22:07:35 2015 by root
!
hostname test-83
logging console debugging
username root
 group root-lr
 group cisco-support
 secret 5 $1$d2NC$RbAdqdU7kw/kEJoMP/IJG1
!
cdp
ipv6 icmp error-interval 50 20
icmp ipv4 rate-limit unreachable DF 1000
```

```
icmp ipv4 rate-limit unreachable 1000
ipv4 conflict-policy static
```

関連コマンド

- ipv6 icmp error-interval

柔軟な送信元 IP の選択

障害に応答する Internet Control Message Protocol（ICMP）応答パケットで柔軟な送信元 IP アドレスを選択できます。

設定例

送信元アドレスの選択に関する RFC コンプライアンスをイネーブルにします。

```
Router#configure
Router(config)#icmp ipv4 source rfc
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in source rfc
Building configuration...
icmp ipv4 source rfc
```

関連コマンド

IPARM 競合解決の設定

このタスクでは、IP Address Repository Manager（IPARM）アドレス競合解決のパラメータを設定します。

- 静的ポリシー解決
- 最長プレフィックス アドレス競合解決
- 最大 IP アドレス競合解決
- 接続ルートに対する Route-Tag のサポート

静的ポリシー解決

静的ポリシー解決の設定により、新しいアドレス設定が現在実行中のインターフェイスに影響するのを防ぎます。

設定例

競合ポリシーを静的に設定します。つまり、新しいインターフェイスアドレスが現在実行中のインターフェイスに影響するのを防ぎます。

```
Router#configure
Router(config)#ipv4 conflict-policy static
*/For IPv6, use the ipv6 conflict-policy static command/*
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in ipv4 config
Building configuration...
!! IOS XR Configuration version = 6.0.0.26I
!! Last configuration change at Mon Dec 14 21:57:27 2015 by root
!
hostname sample-83
logging console debugging
username root
 group root-lr
 group test
 secret 5 $1$d2NC$RbAdqdU7kw/eKJpMo/GJI1
!
cdp
ipv4 conflict-policy static
interface Loopback0
 ipv4 address 1.1.1.1 255.255.255.255
!
…..
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr             Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24   HundredGigE0/9/0/1  192.85.1.1/24 default


Forced down interface         Up interface                   VRF
```

関連コマンド

- ipv4 conflict-policy
- ipv6 conflict-policy

最長プレフィックス アドレス競合解決

この競合解決ポリシーは、プレフィックスが最長の IP アドレスに最も高い優先度を付与することを試みます。つまり、現在実行しているインターフェイスの最長プレフィックスアドレスと競合しない競合セット内のすべてのアドレスが、同様に実行を許可されます。

設定例

最長プレフィックス アドレス競合解決を設定します。

```
Router# configure
Router(config)# ipv4 conflict-policy longest-prefix
*/For IPv6, use the ipv6 conflict-policy command*/
Router(config)# commit
```

実行コンフィギュレーション

```
Router# show running-config | in longest-prefix
Building configuration...
ipv4 conflict-policy longest-prefix
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr             Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24   HundredGigE0/9/0/1  192.85.1.1/24 default


Forced down interface         Up interface                   VRF
```

最大 IP アドレス競合解決

この競合解決ポリシーは、値が最も高い IP アドレスに最も高い優先度を付与することを試みます。つまり、値が最も高い IP アドレスが優先されます。

設定

最大 IP アドレス競合解決を設定します。

```
Router# configure
Router(config)#ipv4 conflict-policy highest-ip
*/For IPv6, use the ipv6 conflict-policy highest-ip command/*
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in highest-ip
Building configuration...
ipv4 conflict-policy highest-ip
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr             Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24   HundredGigE0/9/0/1  192.85.1.1/24 default


Forced down interface         Up interface                   VRF
```

接続ルートに対する Route-Tag のサポート

接続ルートに対する Route-Tag のサポート機能は、インターフェイスのすべての IPv4 および IPv6 アドレスにタグを付加します。このタグは、IPv4 および IPv6 の管理エージェント（MA）から、IPv4 および IPv6 の Address Repository Manager（ARM）およびルーティング プロトコルに伝搬されるため、ユーザは、Routing Policy Language（RPL）スクリプトを使用してルートタグを調べることで、接続ルートの再配布を制御します。これにより、ルートポリシーのルートタグを確認して、一部のインターフェイスの再配布を回避できます。ルートタグがポリシー

に一致し、再配布を回避できるスタティック ルートと接続ルート（インターフェイス）では、このルート タグ機能はすでに利用可能になっています。

設定例

インターフェイス HundredGigE 0/9/0/1 に対して、ルート タグ 20 が付いた IPv4 アドレス 10.0.54.2/30 を指定します。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 10.0.54.2/30 route-tag 1899
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1
 ipv4 address 10.0.54.2/30 route-tag 1899
!
```

確認

ルートのパラメータを確認します。

```
Router#show route 10.0.54.2
Routing entry for 10.0.54.2/32
  Known via "local", distance 0, metric 0 (connected)
  Tag 1899
Routing Descriptor Blocks
    directly connected, via HundredGigE0/9/0/1
      Route metric is 0
  No advertising protos.
```

関連コマンド

- route-tag

拡大された IPv6 アドレス空間

グローバルに一意な IP アドレスの需要は今後増加すると予想され、その需要を満たす必要があることが、IPv6 の主な目的です。モバイル インターネット対応デバイス（携帯情報端末（PDA）、電話、車両など）、Home Area Network（HAN）、ワイヤレス データ サービスなどのアプリケーションによって、グローバルに一意な IP アドレスの需要が増大しています。IPv6 は、ネットワーク アドレス ビット数を（IPv4 での）32 ビットの 4 倍の 128 ビットにしているため、地球上のすべてのネットワーク デバイスにグローバルに一意な IP アドレスを十分に提供できます。IPv6 アドレスをグローバルに一意にすることで、ネットワーク デバイスのグローバルな到達可能性とエンドツーエンドのセキュリティが実現されます。これは、アドレスの需要を喚起するアプリケーションとサービスに不可欠な機能です。また、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ネットワーク アドレス変換（NAT）の使用が低減されます。したがって、IPv6 を使用すると、ネットワーク エッジにある境界ルー

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。

IPv6 アドレス形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のようにコロン（:）で区切られた一連の 16 ビットの 16 進フィールドで表されます。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 アドレスを扱いやすくするために、2 つのコロン（::）を使用して、IPv6 アドレスの先頭、中間、最後の部分の連続したゼロの 16 進フィールドを圧縮できます。（これらのコロンは、連続したゼロの 16 進フィールドを表します）。表 1 : 圧縮された IPv6 アドレス形式 （21 ページ）に、圧縮された IPv6 アドレス形式を示します。

連続する 16 ビット値がゼロで表されている場合は、 *ipv6-address* 引数の一部として 2 つのコロンを使用できます。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。

（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。

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 *1 :* 圧縮された *IPv6* アドレス形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:0DB8:800:200C:417A	1080::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 1 : 圧縮された IPv6 アドレス形式 （21 ページ）に示されているループバック アドレスを使用して、IPv6 パケットを自身に送信できます。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（127.0.0.1）と同じように機能します。

（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ができません。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は、そのパケットを作成したノード内に留まっている必要があります。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。

表 1：圧縮された IPv6 アドレス形式 （21 ページ）に示されている未指定アドレスは、IPv6 アドレスがないことを示します。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（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ができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

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* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。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 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、単一ノード上の単一インターフェイスの識別子です。ユニキャストアドレスに送信されるパケットは、そのアドレスで識別されるインターフェイスに配信されます。Cisco IOS XR ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされています。

- 集約可能グローバル アドレス
- サイトローカル アドレス（IETF では廃止を提案しています）
- リンクローカル アドレス
- IPv4 互換 IPv6 アドレス

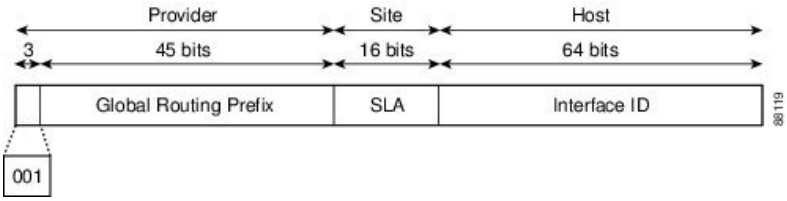
集約可能グローバル アドレス

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で使用されます。

集約可能グローバル IPv6 アドレスは、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID により定義されます。バイナリ 000 から開始するアドレスを除き、すべてのグローバル ユニキャスト アドレスには 64 ビットのインターフェイス ID があります。現在の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 アドレス形式に関するドキュメント）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 アドレッシ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。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、リンク層アドレスに基づいています。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。

インターフェイス ID は、次のいずれかに該当する変更済みの EUI-64 形式で構築されています。

- すべての IEEE 802 インターフェイス タイプ（イーサネット インターフェイス、FDDI インターフェイスなど）の場合、最初の 3 オクテット（24 ビット）は、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）の組織固有識別子（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 進数値です。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。値 0 はローカルに管理されている識別子を示し、値 1 はグローバルに一意の IPv6 インターフェイス識別子を示します。

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

（注） ポイントツーポイントプロトコル（PPP）を使用するインターフェイスの場合は、接続の両端のインターフェイスが同じ MAC アドレスを持つ可能性があるため、接続の両端で使用されるインターフェイス識別子は、両方の識別子が一意になるまでネゴシエーション（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識別子の構築に使用されます。

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。

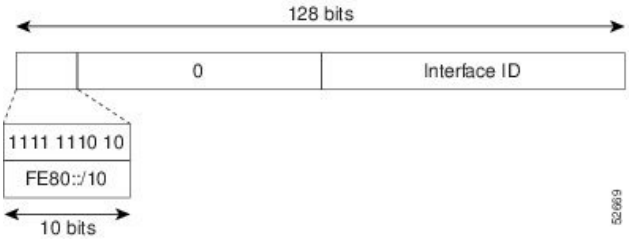
1. ルータに MAC アドレスが（ルータの MAC アドレス プールから）照会されます。
2. 使用できる MAC アドレスがない場合は、ルート プロセッサ（RP）またはラインカード（LC）のシリアル番号を使用して、リンクローカル アドレスを形成します。

リンクローカル アドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレ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。ノードの通信にサイトローカル アドレスまたは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 ルータでは、送信元または宛先がリンクローカル アドレスであるパケットを他のリンクに転送できません。

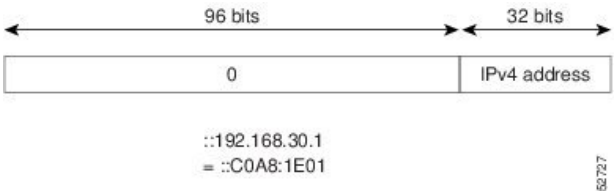
図 *2 :* リンクローカル アドレス形式



IPv4 互換 IPv6 アドレス

IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットがゼロであり、アドレスの下位 32 ビットが IPv4 アドレスである IPv6 ユニキャスト アドレスです。IPv4 互換 IPv6 アドレスの形式は、0:0:0:0:0:0:A.B.C.D または ::A.B.C.D です。IPv4 互換 IPv6 アドレスの 128 ビット全体がノードの IPv6 アドレスとして使用され、下位 32 ビットに埋め込まれた IPv4 アドレスがノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 と IPv6 の両方のプロトコル スタックをサポートするノードに割り当てられ、自動トンネルで使用されます。次の図は、IPv4 互換 IPv6 アドレスの構造と、許容されるアドレス フォーマットのいくつかを示しています。

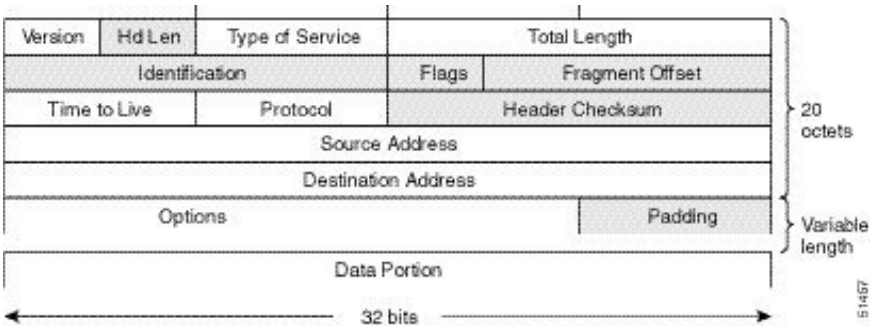
図 *3 : IPv4* 互換 *IPv6* アドレス形式



簡易 IPv6 パケット ヘッダー

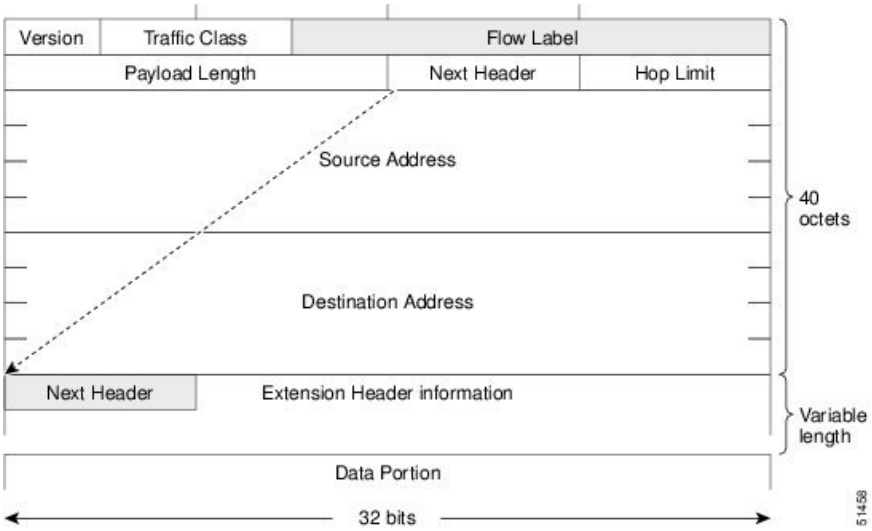
基本 IPv4 パケット ヘッダーには、合計サイズが 20 オクテット（160 ビット）の 12 のフィールドがあります。この 12 個のフィールドの後にはオプション フィールドが続く場合があり、さらにその後に、通常はトランスポートレイヤパケットであるデータ部分が続きます。可変長のオプション フィールドは、IPv4 パケット ヘッダーの合計サイズに加算されます。IPv4 パケット ヘッダーのグレーの部分のフィールドは、IPv6 パケット ヘッダーに含まれません。

図 *4 : IPv4* パケット ヘッダー形式



基本 IPv6 パケット ヘッダーには、合計サイズが 40 オクテット（320 ビット）の 8 つのフィールドがありますIPv6 では、フラグメンテーションはルータによって処理されず、チェックサムはネットワーク層で使用されないため、IPv6 ヘッダーからフィールドが除去されました。代わりに、IPv6 の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、チェックサムはデータ リンク層とトランスポート層で使用されます（IPv4 では、ユーザ データグラム プロトコル（UDP）トランスポート層でオプションのチェックサムが使用されます。IPv6 では、UDP チェックサムを使用して内部パケットの完全性を確認する必要があります）。また、基本 IPv6 パケット ヘッダーとオプション フィールドは 64 ビットに揃えられています。これにより、IPv6 パケットの処理が容易になります。

図 *5 : IPv6* パケット ヘッダー形式



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。

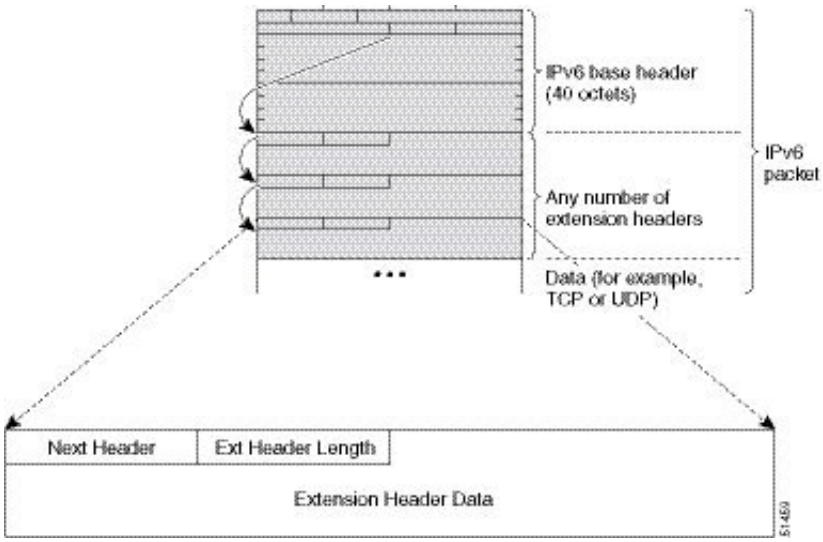
表 *2 :* 基本 *IPv6* パケット ヘッダー フィールド

フィールド	説明
バージョン	IPv4 パケット ヘッダーのバージョン フィールドと同様ですが、IPv4 を意味する数字 4 の代わりに IPv6 を意味する数字 6 が示されます。

フィールド	説明
トラフィック クラス	IPv4 パケット ヘッダーのタイプ オブ サービス フィールドと同様です。トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。
フロー ラベル	IPv6 パケット ヘッダーの新しいフィールドです。フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。ペイロード長フィールドは、パケットのデータ部分の合計長を示します。
次ヘッダー	IPv4 パケット ヘッダーのプロトコル フィールドと同様です。次ヘッダー フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。基本 IPv6 ヘッダーの後ろに続く情報のタイプは、TCP や UDP パケットなどのトランスポートレイヤ パケット、または拡張ヘッダーです。
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。

基本 IPv6 パケット ヘッダーの 8 つのフィールドの後に、オプションの拡張ヘッダーおよびパケットのデータ部分が続きます。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。拡張ヘッダーがまとまってヘッダーのチェーンを形成します。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 *6 : IPv6* 拡張ヘッダー形式



次の表に、拡張ヘッダー タイプとその次ヘッダー フィールド値をリストします。

表 *3 : IPv6* 拡張ヘッダー タイプ

ヘッダー タイプ	次ヘッダーの値	説明
ホップバイホップ オプション ヘッダー	0	このヘッダーは、パケットのパス上のすべてのホップで処理されます。存在する場合、ホップバイホップ オプション ヘッダーは、常に基本 IPv6 パケット ヘッダーの直後に続きます。
宛先オプション ヘッダー	60	宛先オプション ヘッダーは、任意のホップバイホップ オプションヘッダーの後に続くことがあります。その場合、宛先オプション ヘッダーは、最終的な宛先と、ルーティング ヘッダーで指定された各通過アドレスでも処理されます。また、宛先オプション ヘッダーは、任意のカプセル化セキュリティペイロード（ESP）ヘッダーの後に続くこともあります。その場合、宛先オプションヘッダーは、最終的な宛先でだけ処理されます。
ルーティング ヘッダー	43	ルーティング ヘッダーは送信元のルーティングに使用されます。
フラグメント ヘッダー	44	フラグメント ヘッダーは、送信元が、送信元と宛先の間のパスの最大伝送ユニット（MTU）よりも大きいパケットをフラグメント化する必要がある場合に使用されます。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。

ヘッダー タイプ	次ヘッダーの値	説明
認証ヘッダー および ESP ヘッダー	51 50	認証ヘッダーと ESP ヘッダーは、パケットの認証、整合性、および機密性を提供するために IP セキュリティ プロトコル（IPSec）内で使用されます。これらのヘッダーは、IPv4 と IPv6 の両方で同一です。
上位層ヘッダー	6（TCP） 17（UDP）	上位層（トランスポート）ヘッダーは、データを転送するためにパケットの内部で使用される典型的なヘッダーです。2 つの主要なトランスポート プロトコルは TCP と UDP です。
モビリティ ヘッダー	IANA で実行	バインディングの作成と管理に関連するすべてのメッセージで、モバイル ノード、通信ノード、およびホーム エージェントによって使用される拡張ヘッダーです。

IPv6 のパス MTU ディスカバリ

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。

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 リンクには、1500 オクテットの MTU 値の使用をお勧めします。

（注） パス MTU ディスカバリは、TCP を使用するアプリケーションでのみサポートされます。

IPv6 ネイバー探索

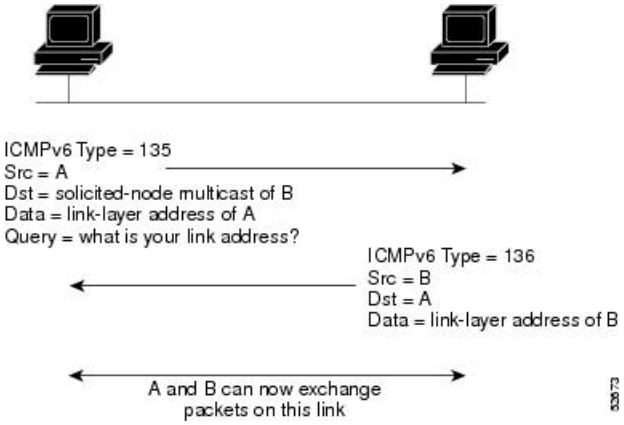
IPv6 のネイバー探索プロセスは、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーの到達可能性を確認して、隣接ルータの状況を把握します。

IPv6 ネイバー送信要求メッセージ

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ノードが別のノードのリンク

層アドレスを判断する必要がある場合、ネイバー請求メッセージ内の送信元アドレスは、ネイバー請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 *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。そのような変更があった場合、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。

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。上位層プロトコル（TCP

など）からの肯定確認応答は、接続で転送が順調に進行している（宛先に到達しつつある）こと、またはネイバー送信要求メッセージに対する応答でネイバー アドバタイズメント メッセージが受信されたことを示します。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。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。送信要求ネイバー アドバタイズメント メッセージがネイバーから返されることは、転送パスがまだ機能していることを示す肯定確認応答です。（送信要求フラグに値 1 が設定されているネイバー 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応答でのみ送信されます）。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。

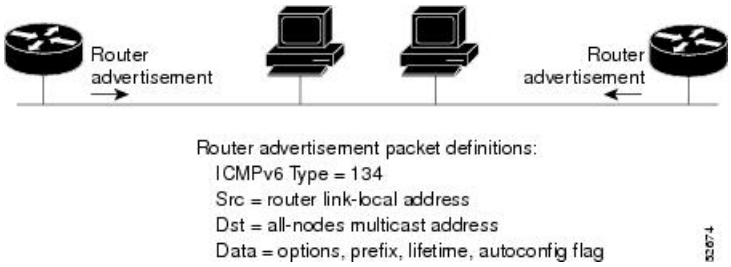
ネイバー送信要求メッセージは、ユニキャスト IPv6 アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。アドレスがインターフェイスに割り当てられる前に、重複アドレス検出がまず新しいリンクローカル IPv6 アドレスで実行されます（重複アドレス検出の実行時、新しいアドレスは暫定的な状態にあります）。具体的には、ノードは未指定の送信元アドレスと一時的なリンクローカルアドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカル 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 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。Cisco IOS XR ソフトウェアでの重複アドレス検出のシスコ実装では、64 ビット インターフェイス識別子から生成されるエニーキャスト アドレスまたはグローバル アドレスの一意性はチェックされません。

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 ルータの設定済みの各インターフェイスへ定期的に送信されます。ルータ アドバタイズメント メッセージは全ノード マルチキャスト アドレスに送信されます。

図 *8 : IPv6* ネイバー探索 - 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 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

ルータ アドバタイズメントは、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 Type 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ルータ アドバタイズメント 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。ルータ送信要求メッセージが通常システム起動時にホストによって送信される（ホストにユニキャストアドレスが設定されていない）場合、ルータ送信要求メッセージの送信元アドレスは、通常は未指定の 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。ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。ルータ送信要求に応答してルータ アドバタイズメントが送信される場合、ルータ アドバタイズメント 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。

次のルータ アドバタイズメント メッセージ パラメータを設定できます。

- ルータ アドバタイズメント 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

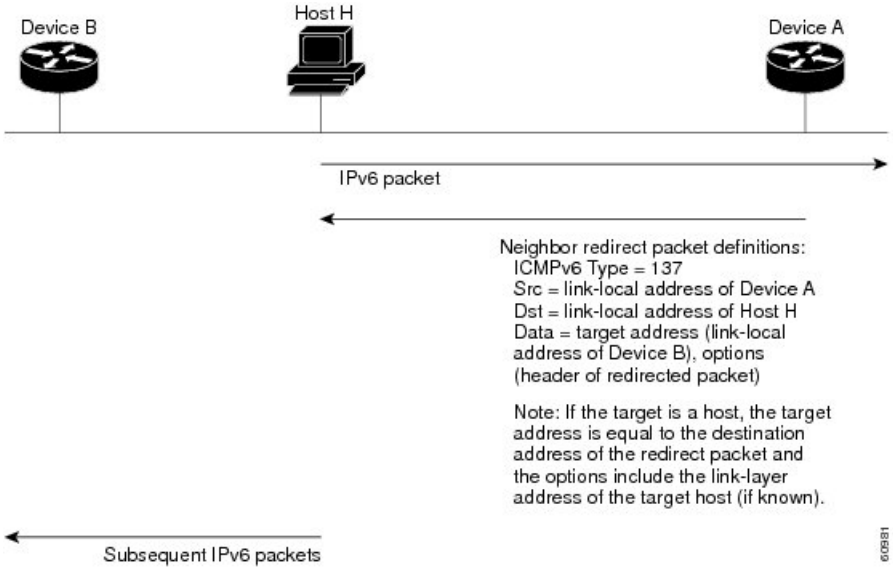
設定されたパラメータはインターフェイスに固有です。ルータ アドバタイズメント メッセージ（デフォルト値を含む）の送信は、イーサネットと FDDI インターフェイス上では自動的にイネーブルになります。その他のインターフェイス タイプの場合、ルータ アドバタイズメント メッセージの送信は、インターフェイス コンフィギュレーション モードで **no ipv6 nd suppress-ra** コマンドを使用して手動で設定する必要があります。ルータ アドバタイズメント メッセージの送信を個々のインターフェイスでディセーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。

（注） ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント 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。

IPv6 ネイバー リダイレクト 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 137 は、IPv6 ネイバー リダイレクト メッセージを示します。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

図 *9 : 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。スタティック ルーティングの場合、ネクストホップ ルータのアドレスは、ルータのリンクローカルアドレスを使用して指定する必要があります。ダイナミック ルーティングの場合は、すべての IPv6 プロトコルが隣接ルータのリンクローカル アドレスを交換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 メッセージを送信する必要があります。

- 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。

ルータがすべての IPv6 ICMP エラー メッセージ（ネイバー リダイレクト メッセージを含む）を生成するレートを制限するには、**ipv6 icmp error-interval** グローバル コンフィギュレーション コマンドを使用します。これにより、リンク層の輻輳が低減されます。

（注） ルータはネイバー リダイレクト メッセージを受信してもそのルーティング テーブルを更新せず、ホストはネイバー リダイレクト メッセージを発信しません。

Address Repository Manager

IPv4 および IPv6 の Address Repository Manager（IPARM）は、システムで設定されたグローバル IP アドレスの一意性を強制適用し、IP アドレスを消費するアプリケーション プログラム インターフェイス（API）を使用して、グローバル IP アドレス情報（アンナンバード インターフェイス情報を含む）をルート プロセッサ（RP）およびラインカード（LC）上のプロセスに伝達します。

アドレス競合解決

競合解決には、競合データベースおよび競合セット定義という 2 つの部分があります。

競合データベース

IPARM では、グローバル競合データベースを保持します。互いに競合する IP アドレスは、競合セットと呼ばれるリストに保持されます。これらの競合セットは、グローバル競合データベースを構成します。

IP アドレスのセットは、そのセット内の少なくとも 1 つのプレフィックスが、同じセットに属する他のすべての IP アドレスと競合する場合に、競合セットの一部であると見なされます。たとえば、次の 4 つのアドレスは、単一の競合セットの一部です。

アドレス 1：10.1.1.1/16

アドレス 2：10.2.1.1/16

アドレス 3：10.3.1.1/16

アドレス 4：10.4.1.1/8

競合する IP アドレスが競合セットに追加されると、アルゴリズムによってそのセット全体が調べられ、そのセット内の最も優先度の高いアドレスが判別されます。

この競合ポリシーアルゴリズムは決定論的アルゴリズムであり、つまり、ユーザは、インターフェイス上のいずれのアドレスがイネーブルまたはディセーブルであるかがわかります。イネーブルなインターフェイス上のアドレスは、その競合セットの最も優先度の高いアドレスとして宣言されます。

競合ポリシー アルゴリズムは、セット内の最も優先度の高い IP アドレスを判別します。