IPv4アドレス

この章では、Cisco NX-OS デバイス上でのインターネット プロトコル バージョン 4（IPv4）（アドレス指定を含む）、アドレス解決プロトコル（ARP）および Internet Control Message Protocol（ICMP）の設定方法を説明します。

この章は、次の項で構成されています。

- IPv4 アドレス （1 ページ）
- IPv4 の仮想化のサポート （11 ページ）
- IPv4の前提条件 （11 ページ）
- IPv4 の注意事項および制約事項 （11 ページ）
- デフォルト設定 （14 ページ）
- IPv4 の設定 （15 ページ）
- IPv4 設定の確認 （38 ページ）
- その他の参考資料 （39 ページ）

IPv4 アドレス

IP アドレスは、デバイスの各ネットワーク インターフェイスに割り当てられる一意の識別子であり、ネットワークを介して他のホストと通信できるようにします。ネットワーク インターフェイスに IP アドレスを設定することにより、これらのインターフェイスがネットワーク内でパケットを送受信できるようになります。

インターフェイスには、デバイスが生成するパケットの主な送信元と接続先である 1 つのプライマリ IP アドレスを設定できます。複数のサブネットまたはネットワーク要件をサポートするために、複数のセカンダリ IP アドレスをインターフェイスに割り当てることもできます。発信パケットは、常にこのプライマリ アドレスを送信元として使用するため、同じインターフェイス上のすべてのデバイスは、同じプライマリ IP アドレスを共有する必要があります。各 IPv4 パケットには、設定された IP アドレスから取得した送信元と接続先の情報が含まれています。詳細については、「複数 IPv4 アドレス」の項を参照してください。

サブネット マスクは、IP アドレスをネットワークとホストの部分に分割する 32 ビット値です。サブネット マスクを適用することで、IP アドレスが属するネットワークを指定し、ホス

トコンポーネントを分離します。サブネットマスクは、IP ネットワークがネットワーク ID とホスト ID を区別して、効果的なルーティングとアドレッシングを促進します。

デバイスの IP 機能は、ユニキャストおよびマルチキャスト ルート ルックアップ、ソフトウェアベースのアクセス コントロール リスト（ACL）転送、および重複アドレス ルックアップを含む、IPv4 パケットの処理と転送を管理します。また、ネットワーク インターフェイスの IP アドレス設定、スタティック ルート管理、および IP クライアントによるパケット送受信も監視します。

（注） Nexus スイッチは、null0 インターフェイスに送信されたパケットをドロップします。IPv4 または IPv6 パケットが null0 インターフェイスに送信された場合、Cisco Nexus 9000 スイッチは ICMP または ICMPv6 で応答しません。

複数の IPv4 アドレス

Cisco NX-OS、では、インターフェイスごとに複数のIPアドレスを設定できます。さまざまな要件を満たすために、任意の数のセカンダリ アドレスを設定できます。一般的なシナリオには、以下のものがあります：

- 単一のサブネットで許可されているよりも多くのホスト IP アドレスが必要な場合。たとえば、サブネット化スキームが論理的なサブネットあたり最大 254 のホストをサポートしているものの、単一の物理サブネット上に 300 のホストが必要な場合は、ルータまたはアクセス サーバーにセカンダリ IP アドレスを適用できます。これにより、2 つの論理的なサブネットを 1 つの物理サブネットにマッピングできます。
- 同じネットワークの 2 つのサブネットが別のネットワークによって物理的に分離されている場合は、セカンダリ アドレスを使用してそれらを統一することができます。この場合、1 つのネットワークが別のネットワークよりも効果的に拡張されます。1 つのサブネットは、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 セグメント上のいずれかのデバイスがセカンダリ IPv4 アドレスを使用している場合は、同じインターフェイス上の他のすべてのデバイスは、同じネットワークまたはサブネットからのセカンダリ アドレスを使用する必要があります。セグメント内のセカンダリ アドレスを一貫性のない仕方で適用すると、ただちにルーティング ループが発生する可能性があります。

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 9000 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。

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

表 *1 : 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。

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

表 *2 : 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**

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

表 *3 : 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**

Cisco Nexus 9300-FX プラットフォーム スイッチ用の LPM ルーティング モード

Cisco Nexus 9300-FX2 プラットフォーム スイッチ用の LPM ルーティング モード

Cisco Nexus 9300-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

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

表 *4 : 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 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 ルーティング モード	Broadcom T2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** （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		

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

表 *5 : 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（コンセプト）

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サポートします。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 テーブルからあふれたルートは、LPM テーブルのスペースを使用します。そのため、利用可能な LPM ルートの総数は減少します。この機能は、Cisco Nexus 9300 および 9500 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ているため、付加的なホスト 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。

アドレス解決プロトコル

ネットワーキング デバイスおよびレイヤ 3 スイッチは ARP を使用して、IP（ネットワーク層）アドレスを物理（Media Access Control（MAC）レイヤ）アドレスにマッピングし、IP パケットがネットワーク上に送信されるようにします。デバイスは、他のデバイスにパケットを送信する前に自身の ARP キャッシュを調べて、MAC アドレスまたは対応する宛先デバイスの IP アドレスがないかを確認します。エントリがまったくない場合、送信元のデバイスは、ネットワーク上の全デバイスにブロードキャスト メッセージを送信します。

各デバイスは、問い合わせられた IP アドレスを自身のアドレスと比較します。一致する IP アドレスを持つデバイスだけが、デバイスの MAC アドレスを含むパケットとともにデータを送信したデバイスに返信します。送信元デバイスは、あとで参照できるよう、宛先デバイスの MAC アドレスをその ARP テーブルに追加し、データリンク ヘッダーおよびトレーラを作成してパケットをカプセル化し、データの転送へと進みます。次の図は、ARP ブロードキャストと応答プロセスを示しています。

図 *1 : ARP* 処理

宛先デバイスが、別のデバイスを挟んだリモート ネットワーク上にあるときは、同じ処理が行われますが、データを送信するデバイスが、デフォルト ゲートウェイの MAC アドレスを求める ARP 要求を送信する点が異なります。アドレスが解決され、デフォルト ゲートウェイがパケットを受信した後に、デフォルト ゲートウェイは、接続されているネットワーク上で宛先の IP アドレスをブロードキャストします。宛先デバイスのネットワーク上のデバイスは、ARP を使用して宛先デバイスの MAC アドレスを取得し、パケットを配信します。ARP はデフォルトでイネーブルにされています。

デフォルトでシステム定義された CoPP ポリシー レートは、スーパーバイザ モジュールにバインドされた ARP ブロードキャスト パケットを制限します。デフォルトのシステム定義 CoPP ポリシーは、ARP ブロードキャスト ストームによるコントロール プレーン トラフィックへの影響を防止し、ブリッジド パケットに影響しません。

ARP キャッシング

ARP キャッシングにより、ブロードキャストが最小になり、ネットワーク リソースの浪費が抑制されます。IP アドレスの MAC アドレスへのマッピングは、ネットワーク間でパケットが送信されるたびに、ネットワーク上の各ホップ（デバイス）で行われるため、ネットワークのパフォーマンスに影響する場合があります。

- ARP キャッシングでは、ネットワーク アドレスとそれに関連付けられたデータリンク アドレスが一定の期間メモリ内に保存されるため、パケットが送信されるたびに同じアドレスにブロードキャストするための貴重なネットワーク リソースの使用が最小限に抑えられます。
- キャッシュ エントリは、定期的に失効するよう設定されているため、保守が必要です。これは、古い情報が無効となる場合があるためです。
- ネットワーク上のすべてのデバイスは、アドレスのブロードキャストに従ってアドレス テーブルを更新します。

ARP キャッシュのスタティックおよびダイナミック エントリ

スタティック ルーティング

スタティック ルーティングは、手動で各デバイスの各インターフェイスに対応する IP アドレス、サブネット マスク、ゲートウェイ、および対応する MAC アドレスを設定する必要があります。スタティック ルーティングでは、ルート テーブルを維持するために、より多くの処理が必要です。ルートを追加または変更するたびに、テーブルの更新が必要となるためです。

ダイナミック ルーティング

ダイナミック ルーティングは、ネットワーク上のデバイスが相互にルーティング テーブル情報を交換できるプロトコルを使用します。ダイナミック ルーティングは、キャッシュに制限時間を追加しない限り、ルート テーブルが自動更新されるため、スタティック ルーティングより効率的です。デフォルトの制限時間は 25 分ですが、キャッシュから追加および削除されるルートがネットワークに数多く存在する場合は、制限時間を変更できます。

ARP を使用しないデバイス

ネットワークが2つのセグメントに分割されると、ブリッジによりセグメントが結合され、各セグメントへのトラフィックが MAC アドレスに基づいてフィルタリングされます。ブリッジは MAC アドレスだけを使用する独自のアドレス テーブルを作成します。デバイスが IP アドレスおよび対応する MAC アドレスの両方を含む ARP キャッシュを持っています。

パッシブ ハブは、ネットワーク内の他のデバイスを物理的に接続する集中接続デバイスです。パッシブ ハブはそのすべてのポートでデバイスにメッセージを送信し、レイヤ1で動作しますが、アドレス テーブルを保持しません。

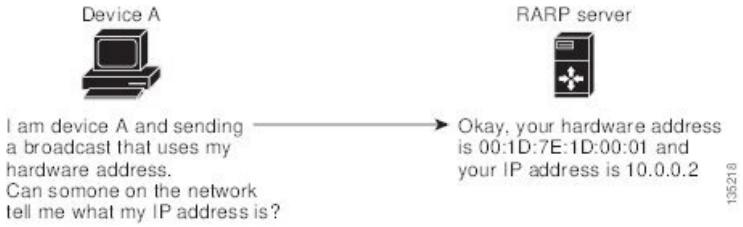
レイヤ2スイッチは、デバイス上のどのポートがそのポートだけに送信されたメッセージを受信するかを決定します。ただし、レイヤ3スイッチは、ARPキャッシュ（テーブル）を作成するデバイスです。

Reverse ARP

RFC 903 で定義された Reverse ARP（RARP）は、ARP と同じように動作しますが、RARP 要求パケットは MAC アドレスではなく IP アドレスを要求する点が異なります。RARP は多くの場合、ディスクレス ワークステーションで使用されます。これは、このタイプのデバイスには、起動時に使用する IP アドレスを格納する手段がないためです。認識できるアドレスは MAC アドレスだけで、これはハードウェアに焼き付けられているためです。

RARP を使用するには、ルータ インターフェイスとして、同じネットワーク セグメント上に RARP サーバが必要です。次の図に、RARP の仕組みを示します。

図 *2 : Reverse ARP*



RARP には、いくつかの制限があります。これらの制限により、ほとんどのビジネスでは、DHCP を使用してダイナミックに IP アドレスを割り当てています。DHCP は、RARP よりコスト効率が高く、必要な保守作業も少ないためです。最も重要な制限は次のとおりです。

- RARP はハードウェア アドレスを使用するため、多くの物理ネットワークを含む大規模なネットワークの場合は、各セグメント上に、冗長性のための追加サーバを備えた RARP サーバが必要です。各セグメントに 2 台のサーバを保持すると、コストがかかります。
- 各サーバは、ハードウェア アドレスと IP アドレスのスタティック マッピングのテーブルで設定する必要があります。IP アドレスの保守は困難です。
- RARP は、ホストの IP アドレスだけを提供し、サブネット マスクもデフォルト ゲートウェイも提供しません。

プロキシ ARP

プロキシ ARP を使用すると、物理的に 1 つのネットワーク上に存在するデバイスが、論理的に、同じデバイスまたはファイアウォールに接続された別の物理ネットワークの一部として表示されます。プロキシ ARP で、プライベート ネットワーク上のパブリック IP アドレスを持つデバイスをルータの背後に隠すと同時に、このデバイスを、ルータの前のパブリック ネットワーク上に表示できます。ルータはそのアイデンティティを隠すことにより、実際の宛先までパケットをルーティングする役割を担います。プロキシ ARP を使用すると、サブネット上の

デバイスは、ルーティングもデフォルト ゲートウェイも設定せずにリモート サブネットまで到達できます。

複数のデバイスが同じデータリンク層のネットワークでなく、同じ IP ネットワーク内にある場合、これらのデバイスは相互に、ローカル ネットワーク上にあるかのようにデータを送信しようとします。ただし、これらのデバイスを隔てるルータは、ブロードキャスト メッセージを送信しません。これは、ルータがハードウェア レイヤのブロードキャストを渡さず、アドレスが解決されないためです。

デバイスでプロキシ ARP をイネーブルにし、ARP 要求を受信すると、プロキシ ARP はこれを、ローカル LAN 上にないシステムに対する要求と見なします。デバイスは、ブロードキャストの宛先であるリモートの宛先であるかのように、自身の MAC アドレスをリモートの宛先の IP アドレスに関連付ける ARP 応答で応答します。ローカル デバイスは、自身が宛先に直接、接続されていると認識していますが、実際には、そのパケットは、ローカルデバイスによりローカル サブネットワークから宛先のサブネットワークへと転送されています。デフォルトでは、プロキシ ARP はディセーブルになっています。

ローカル プロキシ ARP

ローカル プロキシ ARP を使用して、通常はルーティングが不要なサブネット内の IP アドレスを求める ARP 要求に対して、デバイスが応答できるようにすることができます。ローカル プロキシ ARP を有効にすると、ARP は、サブネット内の IP アドレスを求めるすべての ARP 要求に応答し、サブネット内のホスト間ですべてのトラフィックを転送します。この機能は、ホストが接続されているデバイスの設定により意図的に、ホストの直接通信が禁止されているサブネットだけで使用してください。

Gratuitous ARP

Gratuitous ARP は、送信元 IP アドレスと宛先 IP アドレスが同じである要求を送信し、重複する IP アドレスを検出します。Cisco NX-OS は、 Gratuitous ARP または ARP キャッシュ更新の有効化または無効化をサポートします。

MAC 削除時の定期的な ARP 更新

ARP プロセスは MAC の削除を追跡し、設定されたカウントの設定された時間間隔で L3 VLAN インターフェイスに定期的な ARP 更新を送信します。MAC が学習されると、ARP プロセスは定期的な ARP 更新の送信を停止します。

詳細については、「SVI の MAC 削除での定期的な ARP リフレッシュの構成 （29 ページ）」を参照してください。

MAC 削除時の ARP 更新

インターフェイス フラップ、MAC アドレス テーブルのクリア、または、STP TCN 通知などのトリガーが発生すると、MAC アドレスは削除またはフラッシュされます。これらの MAC ア

ドレスが削除されると、ARPプロセスは、これらのMACアドレスに関連した全ての隣接関係に対して、ARP更新を開始します。これらのARPリフレッシュは、CoPP制限の影響を受けます。これにより、ARPプロセスがすべてのARPエントリを効果的に再学習できなくなります。

Cisco NX-OS リリース 10.5（3）Fから、ARP プロセスは2、4、8秒後に更新を再試行し、16秒後（応答がない場合）に削除する代わりに、2、4、8、および8秒後に更新を送信し、さらに8秒後に削除します（1回余分に更新する）。この変更によって、一部のARP応答パケットがCoPP 制限の対象となる場合でも、拡張済みの ARP エントリによる ARP 学習が向上します。

収集スロットル

着信 IP パケットがラインカードに転送されたときに、ネクスト ホップのアドレス解決プロトコル（ARP）の要求が解決されない場合、ラインカードはパケットをスーパーバイザに転送します（収集スロットル）。スーパーバイザはネクストホップのMACアドレスを解決し、ハードウェアをプログラミングします。

ARP 要求が送信されると、ソフトウェアは、同じネクストホップ IP アドレスへのパケットがスーパーバイザに転送されないようにするために、ハードウェア内に /32 ドロップ隣接関係を追加します。ARPが解決されると、そのハードウェアエントリは正しいMACアドレスで更新されます。タイムアウト期間が経過するまでに ARP エントリが解決されない場合、そのエントリはハードウェアから削除されます。

（注） Glean スロットリングは IPv4 および IPv6 でサポートされますが、IPv6 リンクローカル アドレスはサポートされません。

パス MTU ディスカバリ

パス最大伝送ユニット（MTU）ディスカバリは、TCP 接続のエンドポイント間のネットワーク内で使用可能な帯域幅の使用を最大化するための方法です。これは RFC 1191 で規定されています。この機能を有効または無効にしても、既存の接続に影響しません。

ICMP

Internet Control Message Protocol（ICMP）を使用して、IP 処理に関連するエラーおよびその他の情報を報告するメッセージパケットを提供できます。ICMPは、ICMP宛先到達不能メッセージ、ICMP エコー要求（2 つのホスト間でパケットを往復送信する）、およびエコー返信メッセージなどのエラー メッセージを生成します。ICMPは多くの診断機能も備えており、ホストへのエラーパケットの送信およびリダイレクトが可能です。デフォルトでは、ICMPがイネーブルにされています。

次に示すのは、ICMP メッセージ タイプの一部です。

- ネットワーク エラー メッセージ
- ネットワーク輻輳メッセージ

- トラブルシューティング情報
- タイムアウト告知

（注）
- ICMP リダイレクトは、ローカル プロキシ ARP 機能がイネーブルになっているインターフェイスではディセーブルになります。
- ICMP リダイレクト機能は、Cisco N93-C64E-SG2-Q スイッチ プラットフォームではサポートされません。ICMP リダイレクトが Cisco N93-C64E-SG2-Q スイッチで現在有効になっている場合は、無効にする必要があります。

IPv4 の仮想化のサポート

IPv4 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。

IPv4の前提条件

IPv4 には、次の前提条件があります。

- IPv4 はレイヤ 3 インターフェイス上だけで設定可能です。

IPv4 の注意事項および制約事項

IPv4 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。
- セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にだけ設定できます。
- ローカル プロキシ ARP は、複数のサブネットに属する複数の HSRP グループを持つインターフェイスではサポートされません。
- **ip proxy-arp** コマンドは、 **fabric forwarding mode anycast-gateway** で有効になっている SVI の VXLAN EVPN ファブリックではサポートされていません。
- -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。

- **system routing template-internet-peering** を設定した場合、マルチキャスト トラフィックはサポートされません。ただし、スイッチに機能 PIM および PIM を設定することは引き続き可能です。
- 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 IPv4 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、スタティック ルーティングは次のスイッチおよびライン カードでサポートされています。
  - Cisco Nexus 9804 スイッチ。
  - 9804 および 9808 プラットフォーム スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カード。
- 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 プラットフォーム 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(2)F 以降、スタティック ルーティングは Cisco Nexus 9232E-B1 スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(4)M 以降、MAC 削除サポートの定期的な ARP リフレッシュは、次の制限付きで Cisco Nexus 9000 シリーズ プラットフォーム スイッチで提供されます。
  - **ip arp refresh-adj-on-mac-delete retry** コマンドの設定中に、ARP が学習されて MAC が学習されていなくても、ARP プロセスはリフレッシュをトリガーしません。これは、MAC 削除/フラッシュ時に定期的な ARP リフレッシュを送信しようとします。
  - **ip arp refresh-adj-on-mac-delete retry** コマンドの設定後、MAC を削除すると、定期的な ARP リフレッシュ動作がトリガーされます。
  - この定期的な ARP リフレッシュのトリガーは、MAC 削除です。この機能は、バースト パケット受信時の MAC 学習ミスには対処しません。
  - 構成中に、規模/ネットワーク要件に基づいて適切な数と間隔を選択する必要があります。

- Cisco NX-OS リリース 10.4(1)F 以降、サブネット外の ARP 解決のサポートは、Cisco Nexus 9000 シリーズ プラットフォーム スイッチで次の L3 インターフェイスに提供されます。
  - イーサネット
  - サブインターフェイス
  - ポート チャネル
  - FEX
  - IP アンナンバード インターフェイス

（注）
- サブネット外 ARP 解決機能は、SVI L3 インターフェイス、および VPC、HSRP、または VXLAN 展開ではサポートされません。

- Cisco NX-OS リリース 10.4(2)F 以降では、次の機能を使用して、Cisco NX-OS デバイスのインターフェイスごとに ARP キャッシュ エントリを制限する **ip arp cache intf-limit** 設定がサポートされています。
  - グローバルモードとインターフェイスモードでサポートされます。ただし、インターフェイス モードの構成は、グローバル モードよりも優先されます。
  - 次の L3 インターフェイスでのみサポートされます。
    - SVI
    - SVI アンナンバード インターフェイス
  - 次の L3 インターフェイスではサポートされていません。
    - イーサネット
    - サブインターフェイス
    - ポート チャネル
    - アンナンバード インターフェイス
  - 構成がサポートされていないインターフェイスに適用される場合、この構成はグローバル モードに適用されます。
- Cisco NX-OS リリース 10.4(2)F 以降では、次の IPv4 レイヤ 3 機能が Cisco Nexus 9232E-B1 スイッチでサポートされています。
  - ARP
  - ECMP
  - IPv4 ユニキャスト ルート

- IPv4 ホスト ルート

- Cisco NX-OS リリース 10.4(2)F 以降では、クラス E IP アドレスを使用してすべての NX-OS 機能を構成できます。IPv4 アドレス空間が不足している場合は、クラス E の IP アドレスを使用して機能を構成できます。クラス E IP アドレスでは、次のスイッチおよびライン カードがサポートされています。
  - Cisco Nexus 92348GC-X
  - Cisco Nexus 9300-EX/FX/FX2/FX3/H2R/H1/GX/GX2
  - Cisco Nexus 9300C
  - Cisco Nexus 9700-EX/FX/GX ライン カード

- Cisco NX-OS リリース 10.4(2)F 以降では、次の IPv4 レイヤ 3 機能が N9336C-SE1 スイッチでサポートされています。
  - IPv4 ユニキャスト ルート
  - IPv4 ホスト ルート
  - IPv4 ネイバー探索
  - ARP
  - IP ダイレクト ブロードキャスト
  - 非 SVI IP アンナンバード インターフェイス

- Cisco NX-OSリリース 10.6(2)F 以降では、IPダイレクテッド ブロードキャスト設定で新しい **hw-assist** キーワードを使用して、IPダイレクテッド ブロードキャストのハードウェア転送を設定できます。
  - この機能は L3 トポロジでのみサポートされています。
  - この機能は VXLAN ではサポートされていません。
  - キーワード hw-assist は SVI でのみサポートされています
  - この機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2/HX ベースの TOR でサポートされています。EOR ではサポートされていません。

デフォルト設定

次の表に、IP パラメータのデフォルト設定値を示します。

パラメータ	デフォルト
ARP タイムアウト	1500 秒

パラメータ	デフォルト
『Proxy ARP』	無効化

IPv4 の設定

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

IPv4 アドレスを設定する

ネットワーク インターフェイスにプライマリ IP アドレスを割り当てることができます。

手順

ステップ 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。

ステップ 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。

ステップ 3 **ip address** *ip-address/length* [*secondary*]

例：

```
switch(config-if)# ip address
192.2.1.1 255.0.0.0
```

インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。

- 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。

ステップ 4 （任意） **show ip interface**

例：

```
switch(config-if)# show ip interface
```

IPv4 に設定されたインターフェイスを表示します。

ステップ 5 （任意） **copy running-config startup-config**

例：

```
switch(config-if)# copy running-config
startup-config
```

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

複数の IP アドレスの設定

セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にのみ追加できます。

手順

ステップ 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。

ステップ 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。

ステップ 3 **ip address** *ip-address/length* [*secondary*]

例：

```
switch(config-if)# ip address
192.168.1.1 255.0.0.0 secondary
```

設定したアドレスをセカンダリ IPv4 アドレスとして指定します。

ステップ 4 （任意） **show ip interface**

例：

```
switch(config-if)# show ip interface
```

IPv4 用に設定されたインターフェイスを表示します。

ステップ 5 （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。

最大ホスト ルーティング モードの構成

デフォルトでは、Cisco NX-OS 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 モードの構成（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 Series NX-OS Verified Scalability Guide』を参照してください。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 プラットフォーム 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。ここで $2x + y <= 128,000$

（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

ステップ 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。

ステップ 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、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。

ステップ 3 （任意） **show forwarding route summary**

例：

```
switch(config)# show forwarding route
summary
```

LPM モードを表示します。

ステップ 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。

ステップ 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。

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。

- 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

ステップ 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。

ステップ 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。

ステップ 3 （任意） **show forwarding route summary**

例：

```
switch(config)# show forwarding
route summary
```

LPM モードを表示します。

ステップ 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。

ステップ 5 **reload**

例：

```
switch(config)# reload
```

デバイス全体をリブートします。

LPMヘビールーティングモードの構成（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、より多くの 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 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 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 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 **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 モードの構成

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、ARP/ND スケールをデフォルト モード値の 2 倍に増やすために LPM デュアル ホスト 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 スイッチだけです。

Cisco NX-OS リリース 10.3(1)F 以降、**system routing template-dual-stack-host-scale** プロファイルは、Cisco Nexus 9300-FX3/GX/GX2B ToR スイッチおよび Nexus 9408 スイッチでマルチキャストと VXLAN をサポートします。

（注） **system routing template-dual-stack-host-scale** プロファイルが BGW で使用されていないことを確認します。

（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 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

ステップ 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。

ステップ 2 [**no**] **system routing template-dual-stack-host-scale**

例：

```
switch(config)# system routing template-dual-stack-host-scale
                       Warning: The command will take effect after next reload.
                       Note: This requires copy running-config to startup-config before switch
reload.
```

デバイスを LPM デュアルホスト ルーティング モードにして、より大きな ARP/ND スケールをサポートします。

ステップ 3 （任意） **show system routing mode**

例：

```
switch(config)# show system routing mode
```

LPM ルーティング モードを表示します。

ステップ 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。

ステップ 5 **reload**

例：

```
switch(config)# reload
```

デバイス全体をリブートします。

スタティック ARP エントリの構成

デバイス上でスタティック ARP エントリを設定して、IP アドレスをスタティック マルチキャスト MAC アドレスを含む MAC ハードウェア アドレスにマッピングできます。

手順

ステップ 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。

ステップ 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。

ステップ 3 **ip arp address** *ip-address mac-address*

例：

```
switch(config-if)# ip arp 192.168.1.1
0019.076c.1a78
```

IP アドレスを MAC アドレスにスタティック エントリとして関連付けます。

ステップ 4 （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。

プロキシ ARP の構成

デバイス上でプロキシ ARP を設定して、他のネットワークまたはサブネット上のホストのメディア アドレスを決定します。

手順

ステップ 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。

ステップ 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。

ステップ 3 **ip proxy arp**

例：

```
switch(config-if)# ip proxy arp
```

インターフェイス上でプロキシ ARP を有効にします。

ステップ 4 （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。

イーサネット インターフェイスでのローカル プロキシ ARP の構成

イーサネット インターフェイス上でローカル プロキシ ARP を設定することができます。

手順

ステップ 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。

ステップ 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。

ステップ 3 **[no] ip local-proxy-arp**

例：

```
switch(config-if)# ip local-proxy-arp
```

インターフェイス上でローカル プロキシ ARP をイネーブルにします。

ステップ 4 （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。

SVI でのローカル プロキシ ARP の設定

SVI でローカル プロキシ ARP を設定できます。CiscoNX-OS リリース 7.0(3)I7(1) 以降では、対応する VLAN で ARP ブロードキャストを抑制することができます。

始める前に

ARP ブロードキャストを抑制する場合は、hardware access-list tcam region arp-ether 256 double-wide コマンドを使用して、ARP/レイヤ 2 Ethertype の倍幅 ACL TCAM リージョン サイズを設定し、設定を保存して、スイッチをリロードします。（詳細については『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』の「ACL TCAM リージョン サイズの設定」のセクションを参照してください。）

手順

ステップ 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。

ステップ 2 **interface vlan vlan-id**

例：

```
switch(config)# interface vlan 5
                        switch(config-if)#
```

VLAN インターフェイスを作成し、SVI の設定モードを開始します。

ステップ 3 [**no**] **ip local-proxy-arp** [**no-hw-flooding**]

例：

```
switch(config-if)# ip local-proxy-arp no-hw-flooding
```

SVI でローカル プロキシ ARP をイネーブルにします。no-hw-flooding オプションは、対応する VLAN での ARP ブロードキャストを抑制します。

（注）
no-hw-flooding オプションを設定し、SVI で ARP ブロードキャストを許可するように設定を変更する場合は、まず no ip local-proxy-arp no-hw-flooding コマンドを使用してこの機能を無効にして、ip local-proxy-arp コマンドを開始する必要があります。

ステップ 4 （任意） **copy running-config startup-config**

例：

```
switch(config-if)# copy running-config startup-config
```

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SVI の MAC 削除での定期的な ARP リフレッシュの構成

Cisco NX-OS リリース 10.2(4)M 以降、SVI の MAC 削除時に定期的な ARP リフレッシュを行うよう構成できます。

デフォルトでは、このコマンドは無効になっています。このコマンドは、定期的な ARP リフレッシュの SVI で設定して、MAC 削除/フラッシュでサイレント ホストの ARP 応答パケットから MAC を学習する必要があります。

手順

ステップ 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。

ステップ 2 **interface vlan vlan-id**

例：

```
switch(config)# interface vlan 5
                        switch(config-if)#
```

VLAN インターフェイスを作成し、SVI の設定モードを開始します。

ステップ 3 [**no**] **ip arp refresh-adj-on-mac-delete retry** [**count** <*frequency count*>] [**interval** <*interval in sec*>]

例：

```
switch(config-if)# ip arp refresh-adj-on-mac-delete retry count 3 interval 15
                        switch(config-if)#
```

MAC 削除/フラッシュでサイレント ホストの ARP 応答パケットから MAC を学習するように ARP リフレッシュを構成します。

- <*frequency count*>：範囲は 1 ～ 3 です。デフォルトは 3 です。
- <*interval in sec*>：範囲は 1 ～ 60 秒です。デフォルトは 15 秒です。

（注）
間隔が ARP リフレッシュ時間の 3/4 より大きい場合、このコマンドは拒否され、次のメッセージが表示されます：

ARP タイムアウト構成により、ARP リフレッシュはこの間隔よりも早く送信されます。この構成は役に立ちません。

ステップ 4 （任意） **copy running-config startup-config**

例：

```
switch(config-if)# copy running-config startup-config
                        switch(config-if)#
```

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Gratuitous ARP の設定

インターフェイス上で Gratuitous ARP を設定できます。

手順

ステップ 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。

ステップ 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。

ステップ 3 **ip arp gratuitous** {**request** | **update**]

例：

```
switch(config-if)# ip arp gratuitous
request
```

インターフェイス上で無償 ARP をイネーブルにします。無償 ARP はデフォルトで有効になっています。

ステップ 4 （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。

サブネット外の ARP 解決の構成

Cisco NX-OS リリース 10.4(1)F 以降では、**ip arp outside-subnet** コマンドを使用してサブネット外 ARP 解決を有効または無効にできます。

このコマンドは、グローバル モードとインターフェイス モードの両方で使用できます。このコマンドが有効になっている場合、config-replace およびデュアル ステージ コミットには影響しません。

（注） このコマンドを有効にすると、Cisco NX-OS リリース 10.4(1)F からのダウングレードが制限され、ダウングレードを続行する前に、サブネット外 ARP 解決構成を削除するように求めるエラー メッセージがユーザーに表示されます。

手順

ステップ 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。

ステップ 2 **[no] ip arp outside-subnet**

例：

```
switch(config)# ip arp outside-subnet
```

接続されたホストのサブネット パケット トランザクションからの ARP を有効または無効にします。

ステップ 3 （任意） **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。

SVI インターフェイスごとの ARP キャッシュ制限の設定

Cisco NX-OS リリース 10.4(2)F 以降では、Cisco NX-OS デバイスの SVI インターフェイスごとに許可される ARP キャッシュ エントリの最大数を設定できます。この構成は、グローバル モードとインターフェイス モードの両方でサポートされます。

手順

ステップ 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。

ステップ 2 **interface vlan** *vlan-id*

例：

```
switch(config)# interface vlan 5
 switch(config-if)#
```

VLAN インターフェイスを作成し、SVI の設定モードを開始します。

ステップ 3 **[no] ip arp cache intf-limit** *value*

例：

```
switch(config-if)# ip arp cache intf-limit 50000
 switch(config-if)#
```

SVI インターフェイスの ARP キャッシュ エントリの制限を構成します。有効な ARP エントリの範囲は 1 ～ 128000 です。

intf-limit：インターフェイスごとの有効なダイナミック ARP エントリの数を指定します。

構成を削除するには、この **no** コマンドの no 形式を使用します。

ステップ 4 （任意） **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。

パス MTU ディスカバリの構成

パス MTU ディスカバリを設定できます。

手順

ステップ 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。

ステップ 2 **ip tcp path-mtu-discovery**

例：

```
switch(config)# ip tcp
path-mtu-discovery
```

パス MTU ディスカバリをイネーブルにします。

ステップ 3 （任意） **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。

IP ダイレクテッド ブロードキャストの設定

IP ダイレクテッド ブロードキャスト機能は、 IP ルーティング後の接続先サブネットのリンク層で、接続先サブネットの一部ではないノードからのパケットを転送します

宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクテッド ブロードキャストを転送します。ダイレクテッド ブロードキャスト パケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。

接続先 MAC アドレスはブロードキャストアドレスとして書き換えられ、パケットはリンク層のブロードキャストとして転送されます。

あるインターフェイスでダイレクテッドブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクテッドブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。アクセス リストを通じて渡すこれらパケットのみがサブネット上でブロードキャストされるように、IP アクセス リストを通じてこれらブロードキャストを任意でフィルタリングすることができます。

Cisco NX-OSリリース 10.6(2)F 以降、 IP ダイレクテッド ブロードキャストのハードウェアウェア転送を可能にする新しいキーワード hw-assist が導入されました。

IP ダイレクテッドブロードキャストをイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順

ip directed-broadcast[*acl* | **hw-assist**]

例：

```
switch(config-if) # ip directed-broadcast
```

ダイレクテッドブロードキャストの物理ブロードキャストへの変換をイネーブルにします。IP アクセスリスト上のこれらのブロードキャストを任意でフィルタリングできます。

CLI **ip directed-broadcast** を使用すると、IP ダイレクテッドブロードキャストのソフトウェア転送がイネーブルになります。

- acl：指定された IP アクセスリストでIP ダイレクテッドブロードキャストパケットをフィルタリングします。
- hw-assist： IP ダイレクテッド ブロードキャストのハードウェアウェア転送を有効にします。

インターフェイスで **ip directed-broadcast** *acl* コマンドまたは **ip directed-broadcast hw-assist** コマンドを使用できます。両方のコマンドを設定すると、最新の設定が優先されます。

IP 収集スロットルの設定

IP 収集スロットルを設定して、到達できないかまたは存在しないネクスト ホップの ARP 解決のためにスーパーバイザに送信される不要な収集パケットをフィルタリングすることを推奨します。IP収集スロットルは、ソフトウェアのパフォーマンスを向上させ、トラフィックをより効率的に管理します。

（注） Glean スロットリングは IPv4 および IPv6 でサポートされますが、IPv6 リンクローカル アドレスはサポートされません。

手順の概要

1. **configure terminal**
2. [**no**] **hardware ip glean throttle**
3. （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

ステップ 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。

ステップ 2	[**no**] **hardware ip glean throttle** 例： `switch(config) # hardware ip glean throttle`	IP 収集スロットルをイネーブルにします。
ステップ 3	（任意） **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。

ハードウェア IP 収集スロットルの最大値の構成

転送情報ベース（FIB）にインストールされている隣接関係の最大ドロップ数を制限できます。

手順

ステップ 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。

ステップ 2 [**no**] **hardware ip glean throttle maximum** *count*

例：

```
switch(config) # hardware ip glean
throttle maximum 2134
```

FIB にインストールされるドロップ隣接関係の数を設定します。

ステップ 3 （任意） **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。

ハードウェア IP 収集スロットルのタイムアウトの設定

インストールされたドロップ隣接関係が FIB 内に残る時間のタイムアウトを設定できます。

手順の概要

1. **configure terminal**
2. [**no**] **hardware ip glean throttle maximum timeout** *timeout-in-seconds*
3. （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

ステップ 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。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **hardware ip glean throttle maximum timeout** *timeout-in-seconds* 例： `switch(config)# hardware ip glean throttle maximum timeout 300`	インストールされたドロップ隣接関係が FIB 内に残る時間のタイムアウトを設定します。 範囲は 300 秒（5 分）～ 1800 秒（30 分）です。 （注） タイムアウト期間を超えた後、ドロップ隣接関係は FIB から削除されます。
ステップ 3	（任意） **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。

ICMP 送信元 IP フィールドのインターフェイス IP アドレスの構成

ICMP エラー メッセージを処理するように ICMP ソース IP フィールドのインターフェイス IP アドレスを設定できます。

手順

ステップ 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。

ステップ 2 [**no**] **ip source** {**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number*} **icmp-errors**

例：

```
switch(config)# ip source loopback 0
icmp-errors
```

ICMP 送信元 IP フィールドのインターフェイス IP アドレスを設定し、ICMP エラー メッセージをルーティングします。

ステップ 3 （任意） **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。

IPv4 リダイレクト Syslog の構成

IPv4 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

ステップ 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

ステップ 2 **ip redirect syslog** [<*value*>]

例：

```
switch(config)# ip redirect syslog 60
                        switch(config)#
```

過剰な IP リダイレクト メッセージの syslog を設定します。

- **ip redirect syslog**: IPv4 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。

ステップ 3 （任意） **no ip redirect syslog**

例：

```
switch(config)# no ip redirect syslog
```

過剰な IPv4 リダイレクト メッセージの syslog を無効にします。

IPv4 設定の確認

IPv4 の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip adjacency	隣接関係テーブルを表示します。

コマンド	目的
show ip adjacency summary	スロットル隣接関係の数のサマリーを表示します。
show ip arp	ARP テーブルを表示します。
show ip arp summary	スロットル隣接関係の数のサマリーを表示します。
show ip interface	IP に関連するインターフェイス情報を表示します。
show ip arp statistics [**vrf** *vrf-name*]	ARP 統計情報を表示します。
show ip arp internal info interface <*interface-name*>	設定されたカウントと間隔を表示します

その他の参考資料

IPv4 の関連資料

関連項目	マニュアル タイトル
TCAM リージョン	詳細については『Cisco Nexus 9000 シリーズ セキュリティ設定ガイド』の「ACL TCAM リージョン サイズの設定」のセクションを参照してください。

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。