



IPv4 の設定

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 の概要 \(1 ページ\)](#)
- [IPv4 の仮想化のサポート \(10 ページ\)](#)
- [IPv4の前提条件 \(10 ページ\)](#)
- [IPv4 の注意事項および制約事項 \(10 ページ\)](#)
- [デフォルト設定 \(11 ページ\)](#)
- [IPv4 の設定 \(11 ページ\)](#)
- [IPv4 設定の確認 \(29 ページ\)](#)
- [その他の参考資料 \(29 ページ\)](#)

IPv4 の概要

デバイス上で IP を設定し、ネットワーク インターフェイスに IP アドレスを割り当てることができます。IP アドレスを割り当てると、インターフェイスがイネーブルになり、そのインターフェイス上のホストと通信できるようになります。

IP アドレスは、デバイス上でプライマリまたはセカンダリとして設定できます。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。デバイスが生成したパケットは、常にプライマリ IPv4 アドレスを使用するため、インターフェイス上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 IP アドレスを共有する必要があります。各 IPv4 パケットは、送信元または宛先 IP アドレスからの情報に基づいています。詳細については、「[複数の IPv4 アドレス](#)」の項を参照してください。

サブネットを使用して、IP アドレスをマスクできます。マスクは、IP アドレスがどのサブネットに属するかを決定するために使用されます。IP アドレスは、ネットワーク アドレスとホスト アドレスで構成されています。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。サブネットマスクは 32 ビット値で、これにより IP パケットの受信者は、IP アドレスのネットワーク ID 部分とホスト ID 部分を区別できます。

IP 機能には、スーパーバイザ モジュールで終端する IPv4 パケットを取り扱い、また同様に、IPv4 ユニキャスト/マルチキャスト ルート ルックアップとソフトウェア アクセス コントロール リスト (ACL) の転送を含む IPv4 パケットの転送を行う役割があります。また、IP 機能は、ネットワーク インターフェイス IP アドレス設定、重複アドレスチェック、スタティック ルート、および IP クライアントのパケット送信/受信インターフェイスも管理します。



-
- (注) Nexusの動作ではnull0インターフェイス宛てのパケットがドロップされるため、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 3000スイッチはICMPまたはICMPv6パケットで応答しません。
-

複数の IPv4 アドレス

Cisco NX-OS は、インターフェイスごとに複数の IP アドレスをサポートします。さまざまな状況に備え、いくつでもセカンダリアドレスを指定できます。最も一般的な状況は次のとおりです。

- 特定のネットワーク インターフェイスのホスト IP アドレスの数が不足している場合。たとえば、サブネット化により、論理サブネットごとに 254 までのホストを使用できるが、物理サブネットの 1 つに 300 のホストアドレスが必要な場合は、ルータ上またはアクセスサーバ上でセカンダリ IP アドレスを使用して、1 つの物理サブネットに 2 つの論理サブネットを使用できます。
- 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 番目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ません。



-
- (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、同じネットワーク インターフェイス上の他のすべてのデバイスも、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。ネットワーク セグメント上で、一貫性のない方法でセカンダリ アドレスを使用すると、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 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 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。

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 13

表 3: Cisco Nexus 9300 EX 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 4: 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

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

表 5: 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

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

表 6: 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

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

表 7: 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)	<code>system routing max-mode host</code>

LPM ルーティング モード	Broadcom T2モード	CLI コマンド
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-alm
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。 <ul style="list-style-type: none"> • 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 8 : 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。

アドレス解決プロトコル

ネットワーク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り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、制限時間を変更します。

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。

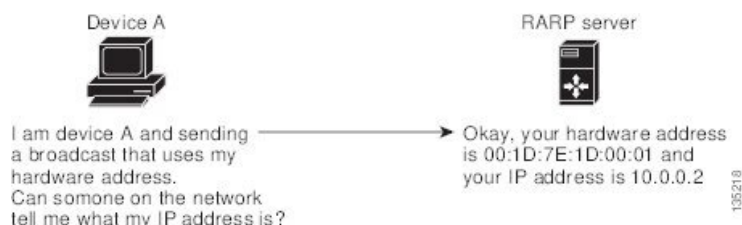
レイヤ2 スイッチは、デバイス上のどのポートがそのポートだけに送信されたメッセージを受信するかを決定します。ただし、レイヤ3 スイッチは、ARP キャッシュ（テーブル）を作成するデバイスです。

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。

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。

Path MTU Discovery

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。

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。

- 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。
- -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。

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
『Proxy ARP』	ディセーブル

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りますので注意してください。

IPv4 アドレス指定の設定

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	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	<p>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。</p> <ul style="list-style-type: none"> • 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

	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	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 モードの設定

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 モードの設定 \(Cisco Nexus 9500 プラットフォーム スイッチのみ\)](#)」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

	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

	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] 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 ($2x + y$ 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

	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)#	グローバル設定モードを開始します。
ステップ 2	[no] system routing mode hierarchical 64b-alm 例： switch(config)# system routing mode hierarchical 64b-alm	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：	この設定変更を保存します。

	コマンドまたはアクション	目的
	switch(config)# copy running-config startup-config	
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。



(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

	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 :	この設定変更を保存します。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	
ステップ 5	reload 例： <code>switch(config)# reload</code>	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、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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	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： <code>switch(config)# system routing template-lpm-heavy</code>	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： <code>switch(config)# show system routing mode</code> 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
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 ファミリー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

	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
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設定 (Cisco Nexus 9200 および 9300-EX プラットフォームスイッチ)

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。



(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 対応 済みスケーラビリティガイド (Cisco Nexus 9000 Series NX-OS Verified Scalability Guide)』を参照してください。

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. Multicast is not supported in this profile 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 エントリの設定

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

	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	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 の設定

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

	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	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 の設定

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

	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	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

	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	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。

無償 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

	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	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。

パス MTU ディスカバリの設定

パス MTU ディスカバリを設定できます。

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	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 ダイレクトブロードキャストの設定

IP ダイレクトブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャストアドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

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 ダイレクトブロードキャストを転送します。ダイレクト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。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャストアドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。

あるインターフェイスでダイレクト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ト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。

IP ダイレクト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

	コマンドまたはアクション	目的
ステップ 1	ip directed-broadcast [acl] 例： <pre>switch(config-if) # ip directed-broadcast</pre>	ダイレクト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。

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

	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設定

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

	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 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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 timeout timeout-in-seconds 例 : <pre>switch(config)# hardware ip glean throttle maximum timeout 300</pre>	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 : <pre>switch(config)# copy running-config startup-config</pre>	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 アドレスの設定

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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	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

	コマンドまたはアクション	目的
	例 : switch(config)# ip source loopback 0 icmp-errors	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 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。
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。

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。

