IPv4 の設定

この章では、Cisco NX-OS スイッチ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

スイッチで IP を設定して、IP アドレスをネットワーク インターフェイスに割り当てられます。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、スイッチ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。スイッチ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 スイッチは、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 アドレスのセクション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。

Cisco NX-OS システムの IP 機能には、IPv4 パケットの処理と IPv4 パケットの転送を行う役割があります。これには、IPv4 ユニキャストおよびマルチキャスト ルート検索、リバース パス転送（RPF）チェック、およびソフトウェア アクセス制御リスト（ACL）転送が含まれます。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受信インターフェイスも管理します。

複数の IPv4 アドレス

Cisco NX-OS システムは、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ています。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で 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ません。

（注） ネットワーク セグメント上のいずれかのスイッチがセカンダリ 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スイッチも、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。

アドレス解決プロトコル

ネットワーク スイッチおよびレイヤ 3 スイッチは、アドレス解決プロトコル（ARP）を使用して、IP（ネットワーク層）アドレスをメディア アクセス コントロール（MAC）レイヤ アドレスにマップし、IP パケットのネットワーク間の送信を可能にします。スイッチは、別のスイッチにパケットを送信する前に、独自の ARP キャッシュを調べて、宛先スイッチの MAC アドレスおよび対応する IP アドレスがあるかどうかを確認します。エントリがない場合、発信元のスイッチは、ネットワーク上のすべてのスイッチにブロードキャスト メッセージを送信します。

各スイッチは、IP アドレスをそれぞれ自身の IP アドレスと比較します。一致する IP アドレスを持つスイッチだけが、スイッチの MAC アドレスを含むパケットとともにデータを送信した

スイッチに返信します。送信元スイッチは、以降の参照用に宛先スイッチの MAC アドレスを自身の ARP テーブルに追加し、データリンク ヘッダーの作成とパケットをカプセル化するトレーラの作成を行った後、データ転送を開始します。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

接続先スイッチが別のスイッチの背後のリモート ネットワークにある場合、データを送信するルーターがデフォルト ゲートウェイの MAC アドレスに対する ARP 要求を送信する場合を除いてプロセスは同じです。アドレスが解決され、デフォルト ゲートウェイがデータ 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。宛先スイッチのネットワーク上のスイッチは、ARP を使用して宛先スイッチの 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。

デフォルトのシステム定義 CoPP ポリシーは、ARP ブロード キャスト パケットのレート制限を行います。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、インターネットワークを送信される各パケットに対しネットワーク上のホップ（スイッチ）ごとに発生します。そのため、ネットワーク パフォーマンスに影響を与えます。

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、メモリに格納されるため、パケットが送信されるたびに同じアドレスを求めてブロードキャストする場合の、貴重なネットワーク リソースの使用が最小限となります。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スイッチは、アドレスがブロードキャストされるとそれぞれのテーブルを更新します。

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。スイッチとは対照的に MAC アドレスだけを使用するブリッジは、独自のアドレス テーブルを作成します。スイッチの場合には、IP アドレスおよび対応する MAC アドレスを含む ARP キャッシュがあります。

パッシブ ハブは、ネットワーク内の他のスイッチを物理的に接続する中央接続スイッチです。これは、そのすべてのポートからスイッチに対してメッセージを送信し、レイヤ 1 で動作しますが、アドレス テーブルは維持しません。

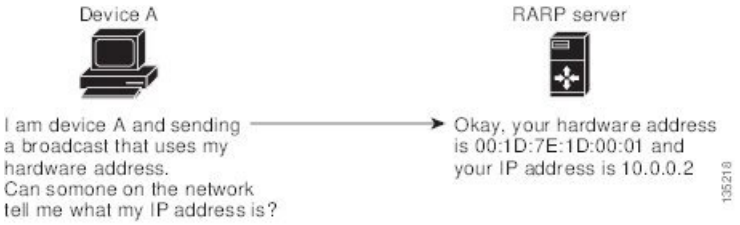
レイヤ 2 スイッチは、すべてのポートからメッセージを送信するハブとは異なり、メッセージの宛先であるデバイスに接続されるポートを決定し、そのポートにだけ送信します。ただし、レイヤ 3 スイッチは、ARP キャッシュ（テーブル）を作成するスイッチです。

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、ほとんどの企業では、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。

プロシキ ARP

プロキシ ARP によって、あるネットワーク上に物理的に存在するスイッチが、同じスイッチ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論理的な一部であることが可能になります。プロキシ ARP によって、ルータの背後のプライベート ネットワーク上のスイッチをパブリック IP アドレスを使用して隠すことができ、さらに、ルータの手前のパブリック

ネットワークにあるように見せることができます。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、サブネット上のスイッチは、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。

スイッチが同じデータリンク層ネットワークには存在しないが、同じ IP ネットワークに存在する場合、それらのスイッチはローカル ネットワーク上に存在するものとして、相互にデータ送信を試みます。ただし、これらのスイッチを隔てるルータは、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。

スイッチでプロキシ 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。スイッチは、ブロードキャストがアドレス指定されたリモートの宛先であるかのように、そのスイッチの MAC アドレスをリモートの宛先の IP アドレスと関連付ける ARP 応答で応答します。ローカル スイッチは、宛先に直接接続されていると確信しますが、実際には、パケットはローカル スイッチによってローカル サブネットワークから宛先サブネットワークへ転送されます。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 Proxy ARP を使用すると、通常ルーティングが必要ないサブネット内の IP アドレスを求める ARP 要求に対し、スイッチが応答するようにできます。ローカル プロキシ ARP をイネーブルにすると、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、接続先スイッチ上での設定により、意図的にホスト間の直接的なコミュニケーションが禁止されているサブネットについてだけ使用してください。

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 要求または ARP キャッシュの更新の有効または無効をサポートします。

収集スロットル

着信 IP パケットを転送するときに、ネクストホップのアドレス解決プロトコル（ARP）要求が解決されない場合、パケットはARP解決のために中央処理装置（CPU）にパントされます。CPU 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。

デバイスのハードウェアには、スーパーバイザを収集トラフィックから保護する収集レート リミッタがあります。エントリの最大数を超えている場合、ARP 要求が解決されなかったパケットは、ハードウェアでドロップされるのではなく、ソフトウェアで処理され続けます。

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。

ICMP

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 到達不能サポートによる送信元インターフェイスの設定

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。ICMP パケットがネットワーク スタック内で構築される場合、パケットは構成されたインターフェイス IP アドレスを使用します。イーサネット、ループバック、またはポート チャネル インターフェイスを選択して、IP アドレスを構成できます。

仮想化のサポート

IPv4 は、仮想ルーティングおよび転送（VRF）インスタンスをサポートしています。デフォルトでは、特に別の VRF を設定しない限り、Cisco NX-OS はユーザーをデフォルトの VRF に配置します。詳細については、「レイヤ 3 仮想化の設定」を参照してください。

ECMP を使用した IPv4 ルート

ルートのすべてのネクストホップが収集、ドロップ、またはパントの場合、すべてのネクストホップはマルチパス ハードウェア テーブルにそのままプログラムされます。

ルートの一部のネクストホップがグリーニング、ドロップ、またはパントであり、残りのネクストホップがそうでない場合、非グリーニング、ドロップ、またはパントのネクストホップのみがマルチパス ハードウェア テーブルにプログラムされます。

ECMP ルートの特定のネクストホップが解決されると（ARP ND が解決されると）、それに応じてマルチパス ハードウェア テーブルが更新されます。

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。

注意事項と制約事項

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。
- スイッチをレイヤ 2 またはレイヤ 3 の終端スイッチとして使用する場合、Cisco はすべての VLAN で **mac-address-table-aging-time** から 1800（デフォルトの ARP エージング時間の 1500 秒よりも長く）に設定することを推奨します。
- スイッチは VLAN 単位の VLAN cam エージング タイマーをサポートしません。
- Cisco Nexus 3600-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または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。
- 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 3600 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** 構成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。

デフォルト設定

次の表は、IP パラメータのデフォルト設定をリスト表示しています。

表 *1:* デフォルト *IP* パラメータ

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

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。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip address** *ip-address* / *length* [**secondary**]
5. （任意） **show ip interface**
6. （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	**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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip address** *ip-address* / *length* [**secondary**] 例：	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。

	コマンドまたはアクション	目的
	`switch(config-if)# ip address 192.2.1.1 255.0.0.0`	• 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 5	（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 6	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

例

次に、IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip address 192.2.1.1 255.0.0.0
switch(config-if)# copy running-config startup-config
```

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。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip address** *ip-address / length* [**secondary**]

5. （任意） **show ip interface**
6. （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	**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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip address** *ip-address / length* [**secondary**] 例： `switch(config-if)# ip address 192.2.1.1 255.0.0.0 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 5	（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 6	（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。

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9.3(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。このルーティング モードをサポートするのは、Cisco Nexus 3600-R プラットフォーム スイッチです。

（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 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 3600 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 3600-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 3600-R プラットフォーム スイッチが他のプレフィックス パターンを使用している場合は、文書化されたスケーラビリティの数値を達成できない可能性があります。

手順の概要

1. **configure terminal**
2. [**no**] **system routing template-internet-peering**
3. （任意） **show system routing mode**
4. **copy running-config startup-config**
5. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

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。

	コマンドまたはアクション	目的
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 モードの追加設定

大規模ルーティング環境でLPMインターネットピアリングルーティングモードでCisco Nexusスイッチを導入する場合、またはネクストホップ数が増加するルートの場合は、VDC リソース テンプレートで IPv4 のメモリ制限を増やす必要があります。

手順の概要

1. **configure terminal**
2. （任意） **show routing ipv4 memory estimate routes routes next-hops hops**
3. **vdc switch id id**
4. **limit-resource u4route-mem minimum min-limit maximum max-limit**
5. **exit**
6. **copy running-config startup-config**
7. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

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	（任意） **show routing ipv4 memory estimate routes routes next-hops hops**
	例：
	`switch(config)# show routing ipv4 memory estimate routes 262144 next-hops 32`
	`Shared memory estimates:`
	`Current max 512 MB; 78438 routes with 64 nhs`
	`in-use 2 MB; 2642 routes with 1 nhs (average)`
	`Configured max 512 MB; 78438 routes with 64 nhs`
	`Estimate memory with fixed overhead: 1007 MB; 262144 routes with 32 nhs`
	`Estimate with variable overhead included:`
	`- With MVPN enabled VRF: 1136 MB`
	`- With OSPF route (PE-CE protocol): 1375 MB`
	`- With EIGRP route (PE-CE protocol): 1651 M`
		共有メモリの見積もりを表示して、ルートのメモリ要件を判断します。

	コマンドまたはアクション	目的

ステップ 3	**vdc switch id id**
	例：
	`switch(config)# vdc switch id 1`
	`switch(config-vdc)#`
		VDC スイッチ ID を指定します。

ステップ 4	**limit-resource u4route-mem minimum min-limit maximum max-limit** 例： `switch(config-vdc)# limit-resource u4route-mem minimum 1024 maximum 1024`	IPv4 メモリの制限をメガバイト単位で指定します。

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

ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。
ステップ 7	**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

スイッチ上に、IP アドレスを MAC ハードウェア アドレス（スタティック マルチキャスト MAC アドレスを含む）にマップするスタティック ARP エントリを設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip arp ipaddr mac_addr**
5. **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	**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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**ip arp ipaddr mac_addr** 例： `switch(config-if)# ip arp 192.2.1.1 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 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

例

次に、スタティック ARP エントリを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip arp 1 92.2.1.1 0019.076c.1a78
switch(config-if)# copy running-config startup-config
```

プロキシ ARP の設定

スイッチで、別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 アドレス定義する Proxy ARP を設定できます。

手順の概要

1. **configure terminal**

2. **interface ethernet number**
3. **no switchport**
4. **ip proxy-arp**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**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 をイネーブルにします。
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。

例

次に、プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip proxy-arp
switch(config-if)# copy running-config startup-config
```

ローカル プロキシ ARP の設定

スイッチ上でローカル プロキシ ARP を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip local-proxy-arp**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します
ステップ 4	**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 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

例

次に、ローカル プロキシ ARP を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip local-proxy-arp
switch(config-if)# copy running-config startup-config
```

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。

手順の概要

1. **configure terminal**
2. **interface ethernet number**
3. **no switchport**
4. **ip arp gratuitous** { **request** | **update** }
5. **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	**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 switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 4	**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。デフォルトはイネーブルです。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

例

次に、IP 収集スロットルを有効にする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle
switch(config-if)# copy running-config startup-config
```

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。

手順の概要

1. **configure terminal**
2. **[no] ip arp outside-subnet**
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] 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：	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`	

SVI インターフェイスごとの ARP キャッシュの構成

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。

手順の概要

1. **configure terminal**
2. **interface vlan** *vlan-id*
3. **[no] ip arp cache intf-limit** *value*
4. （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	**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。

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スイッチは、ユニキャスト IP パケットをそのサブネット上のホストに転送するのと同じ方法で、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スイッチに到着すると、宛先サブネット上のブロードキャストとして「展開」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にブロードキャストとして展開されます。

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。

コマンド	目的
ip directed-broadcast	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有効にします。

IP 収集スロットルの設定

Cisco NX-OS ソフトウェアは、収集トラフィックからスーパーバイザを保護する収集スロットル レート リミッタをサポートします。

（注） 到達不能な、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た不要な収集パケットをフィルタリングするために、「hardware ip glean throttle」コマンドを使用して、IP 収集スロットル機能を構成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. **hardware ip glean throttle**

3. **no hardware ip glean throttle**
4. （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	**hardware ip glean throttle** 例： `switch(config)# hardware ip glean throttle`	ARP スロットリングを有効にします。
ステップ 3	**no hardware ip glean throttle** 例： `switch(config)# no hardware ip glean throttle`	ARP スロットリングを無効にします。
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。

例

次に、IP 収集スロットルを有効にする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle
switch(config-if)# copy running-config startup-config
```

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. **hardware ip glean throttle maximum timeout** *timeout-in-seconds*
3. [**no**] **hardware ip glean throttle maximum timeout** *timeout-in-seconds*
4. （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	**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。
ステップ 3	[**no**] **hardware ip glean throttle maximum timeout** *timeout-in-seconds* 例： `switch(config)# no hardware ip glean throttle maximum timeout 300`	デフォルトの制限値を適用します。 タイムアウト値は秒単位です。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 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。

例

次に、Gratuitous ARP 要求をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle maximum timeout 300
switch(config-if)# copy running-config startup-config
```

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。

手順の概要

1. **configure terminal**

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

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**] **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。

例

この例では、ICMP 送信元 IP フィールドでインターフェイス IP アドレスを構成する方法を示します。

```
switch# configure terminal
switch(config)# ip source ethernet 1/1 icmp-errors
```

この例では、ICMP 送信元 IP フィールドでインターフェイス IP アドレスを構成する方法を示します。

```
switch# configure terminal
switch(config)# no ip source ethernet 1/1 icmp-errors
```

IP パケットのソフトウェア転送のロギングの設定

NX-OS ソフトウェアによって転送される IP パケットのロギング条件を設定できます。条件は次のとおりです。

- パケットの最小数（サイズ）
- オプションの期間（ロギング間隔）

ロギング条件により、1秒あたりのパケット数（pps）のしきい値が作成されます。トラフィックが条件を満たしているか超えると、NX-OS はコンソール メッセージをログに記録します。次に例を示します。

```
2019 jul 31 15:28:31 switch-1 %$ VDC-1 %$ %USER-3-SYSTEM_MSG: Packets per second exceeded
 the configured threshold 40, current PPS: 1262  - netstack
```

ip pps threshold unicast-forward コマンドを使用して、転送されるパケットの条件を設定できます。この機能を無効にするには、**no ip pps threshold unicast-forward**を使用します。

手順の概要

1. **config terminal**
2. **ip pps threshold unicast-forward** *pps-threshold* [*syslog-interval*]
3. （オプション）**show ip pps threshold**

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	**config terminal**
	例：
	`switch-1# config terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch-1(config)#`
		端末の構成を開始します

ステップ 2	**ip pps threshold unicast-forward** *pps-threshold* [*syslog-interval*]
	例：
	`switch-1(config)# ip pps threshold unicast-forward 50 5`
	`switch-1(config)#`
		この機能を有効にして条件を設定します。
		• *pps-threshold* は 1 ～ 30000 パケットです。
		• *syslog-interval* は 1 ～ 60 秒です。デフォルト値は 1 秒です。

ステップ 3	（オプション）**show ip pps threshold**
	例：
	`switch-1(config) show ip traffic pps`
	`PPS type : unicast-forward, PPS limit : 50, Log Interval: 5`
	`switch-1(config)#`
		現在の PPS しきい値設定を表示します。

例

次の例は、特定のフローで転送されるパケット数が、設定されたパケット数および 2 秒ごとに 4000 パケットというロギング間隔を超えた場合に、コンソール メッセージを設定する方法を示しています。

```
switch-1# configure terminal
switch-1(config)# ip pps threshold unicast-forward 4000 2
switch-1(config)# copy running-config startup-config
```

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
how hardware forwarding ip verify	IP パケット検証の設定を表示します。
show ip adjacency	隣接関係テーブルを表示します。
show ip arp	ARP テーブルを表示します。
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 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 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。

IPv4 の設定例

次に、IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config)# no switchport
switch(config-if)#ip address 192.2.1.1/1
```

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。