



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)、Address Resolution Protocol (ARP; アドレス解決プロトコル)、および Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) の設定方法を説明します。

この章では、次の内容について説明します。

- [「IPv4 について」 \(P.2-1\)](#)
- [「IPv4 のライセンス要件」 \(P.2-6\)](#)
- [「IPv4 の前提条件」 \(P.2-7\)](#)
- [「注意事項および制約事項」 \(P.2-7\)](#)
- [「デフォルト設定」 \(P.2-7\)](#)
- [「IPv4 の設定」 \(P.2-7\)](#)
- [「ダイレクトブロードキャストの設定」 \(P.2-14\)](#)
- [「IPv4 の設定例」 \(P.2-19\)](#)
- [「その他の関連資料」 \(P.2-19\)](#)

IPv4 について

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ク 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、送信元または宛先の IP アドレスからの情報に基づいています。[「複数の IPv4 アドレス」 \(P.2-2\)](#) 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 コントロール リスト (ACL) 転送が含まれます。IP 機能は、ネットワーク インターフェイスの 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、IP クライアントのパケット送信および受信インターフェイスも管理します。

ここでは、次の内容について説明します。

- 「複数の IPv4 アドレス」 (P.2-2)
- 「アドレス解決プロトコル」 (P.2-2)
- 「ARP キャッシング」 (P.2-3)
- 「ARP キャッシュのスタティック エントリおよびダイナミック エントリ」 (P.2-3)
- 「ARP を使用しないデバイス」 (P.2-4)
- 「Reverse ARP」 (P.2-4)
- 「プロキシ ARP」 (P.2-5)
- 「ローカル プロキシ ARP」 (P.2-5)
- 「ICMP」 (P.2-6)
- 「仮想化のサポート」 (P.2-6)

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、ルータの複数のアクティブなインターフェイス上に同時に表示できません。



(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。

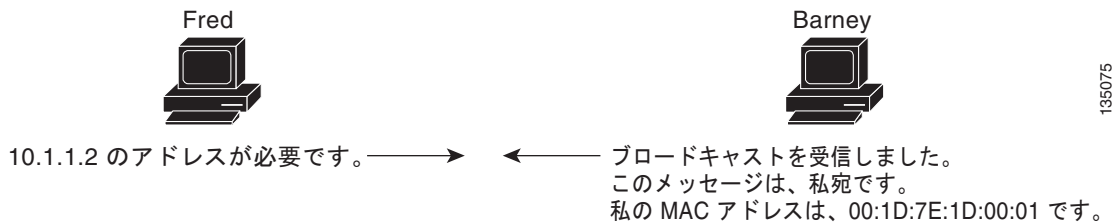
アドレス解決プロトコル

ネットワーク スイッチおよびレイヤ 3 スイッチは、Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して、IP (ネットワーク層) アドレスを Media Access Control (MAC; メディア アクセス コントロール) 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。図 2-1 は、ARP ブロードキャストと応答処理を示します。

図 2-1 ARP 処理



宛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、データを送信するスイッチがデフォルト 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 ゲートウェイがパケットを受信したあとに、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 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、無駄に使用されるネットワーク リソースが制限されます。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 キャッシュのスタティック エントリおよびダイナミック エントリ

スタティック ルートの使用時には、各スイッチの各インターフェイスの 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 アドレスを手動で設定する必要があります。スタティック ルーティングを使用すると、管理を強化できますが、より多くのルート テーブル保守作業が必要となります。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、ネットワーク内のスイッチが相互にルーティング テーブルの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。IP アドレスとそれに対応する MAC アドレスの両方を含む ARP キャッシュを備えるスイッチとは対照的に、ブリッジは、MAC アドレスのみを使用する独自のアドレス テーブルを構築します。

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。

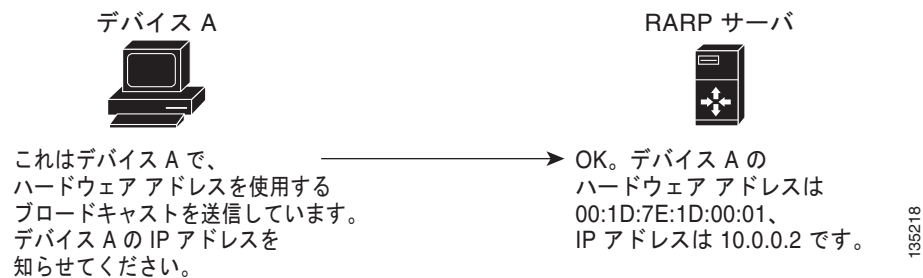
すべてのポートからメッセージを送信するハブとは異なり、レイヤ 2 スイッチは、メッセージの宛先であるデバイスに接続されているポートを特定し、そのポートにのみ送信します。ただし、レイヤ 3 スイッチは、ARP キャッシュ (テーブル) を作成するスイッチです。

Reverse ARP

RFC 903 で定義された Reverse ARP (RARP) は ARP と同様に機能しますが、RARP 要求パケットが 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。図 2-2 は、RARP の機能を図示したものです。

図 2-2 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 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 プロキシ 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なります。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。

Cisco Nexus 3000 シリーズ デバイスのハードウェアは、収集トラフィックからスーパーバイザを保護するための収集レート リミッタを備えています。最大エン트리数を超えると、ARP 要求が解決されていないパケットは、ハードウェアでドロップされるのではなく、引き続きソフトウェアで処理されます。

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。

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 混雑メッセージ
- 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 機能がイネーブルであるインターフェイス上ではディセーブルにされています。

仮想化のサポート

IPv4 は、Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) 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 によりデフォルト VRF が使用されます。詳細については、第 13 章「レイヤ 3 仮想化の設定」を参照してください。

IPv4 のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IPv4 にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

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。
- Cisco Nexus 3000 スイッチがレイヤ 2 またはレイヤ 3 のターミネーション スイッチとして使用される場合は、すべての VLAN に対して **mac-address-table-aging-time** を 1800 (デフォルトの ARP エージング タイムの 1500 秒より長い値) に設定することを推奨します。
- Cisco Nexus 3000 スイッチは、VLAN 単位の CAM エージング タイマーをサポートしていません。

デフォルト設定

表 2-1 に、IP パラメータのデフォルト設定を示します。

表 2-1 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
プロキシ ARP	ディセーブル

IPv4 の設定

ここでは、次の内容について説明します。

- 「IPv4 アドレス指定の設定」(P.2-8)
- 「複数の IP アドレスの設定」(P.2-9)
- 「スタティック ARP エントリの設定」(P.2-10)
- 「プロキシ ARP の設定」(P.2-11)
- 「ローカル プロキシ ARP の設定」(P.2-12)
- 「ダイレクト ブロードキャストの設定」(P.2-14)
- 「IP 収集スロットルの設定」(P.2-14)
- 「ハードウェア IP 収集スロットルの最大数の設定」(P.2-15)
- 「ハードウェア IP 収集スロットルのタイムアウトの設定」(P.2-16)
- 「ハードウェア IP 収集スロットルの syslog の設定」(P.2-17)



(注)

Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

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

	コマンド	目的
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 Example: switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport Example: 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] Example: switch(config-if)# ip address 192.2.1.1 255.0.0.0	インターフェイスにプライマリまたはセカンダリ IPv4 アドレスを指定します。 <ul style="list-style-type: none"> • ネットワーク マスクは、ドットで 4 つの部分に分けられている 10 進数のアドレスです。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、プレフィックスを構成するアドレスの上位の連続ビット (アドレスのネットワーク部分) の桁数を示す 10 進数の値です。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。

	コマンド	目的
ステップ 5	show ip interface Example: switch(config-if)# show ip interface	(任意) 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 6	copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

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だけ追加できます。

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

	コマンド	目的
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 <i>number</i> Example: switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport Example: 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。

	コマンド	目的
ステップ 4	<code>ip address ip-address/length</code> [secondary] Example: 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	<code>show ip interface</code> Example: switch(config-if)# show ip interface	(任意) 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 6	<code>copy running-config startup-config</code> Example: switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

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. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> Example: switch# configure terminal switch(config)#	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	<code>interface ethernet number</code> Example: switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>no switchport</code> Example: 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。

	コマンド	目的
ステップ 4	<pre>ip arp ipaddr mac_addr</pre> <p>Example: switch(config-if)# ip arp 192.2.1.1 0019.076c.1a78</p>	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	<pre>copy running-config startup-config</pre> <p>Example: switch(config-if)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

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 192.2.1.1 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 proxy-arp`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<pre>configure terminal</pre> <p>Example: switch# configure terminal switch(config)#</p>	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	<pre>interface ethernet number</pre> <p>Example: switch(config)# interface ethernet 2/3 switch(config-if)#</p>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<pre>no switchport</pre> <p>Example: switch(config-if)# no switchport</p>	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。

	コマンド	目的
ステップ4	<pre>ip proxy-arp</pre> <p>Example: switch(config-if)# ip proxy-arp</p>	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	<pre>copy running-config startup-config</pre> <p>Example: switch(config-if)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

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

	コマンド	目的
ステップ1	<pre>configure terminal</pre> <p>Example: switch# configure terminal switch(config)#</p>	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	<pre>interface ethernet <i>number</i></pre> <p>Example: switch(config)# interface ethernet 2/3 switch(config-if)#</p>	インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<pre>no switchport</pre> <p>Example: switch(config-if)# no switchport</p>	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。

	コマンド	目的
ステップ 4	<pre>ip local-proxy-arp</pre> <p>Example: switch(config-if)# ip local-proxy-arp</p>	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	<pre>copy running-config startup-config</pre> <p>Example: switch(config-if)# copy running-config startup-config</p>	(任意) この設定の変更を保存します。

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
```

Gratuitous ARP の設定

インターフェイス上で Gratuitous ARP を設定できます。

手順の概要

1. `configure terminal`
2. `interface ethernet number`
3. `no switchport`
4. `ip arp gratuitous {request | update}`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<pre>configure terminal</pre> <p>Example: switch# configure terminal switch(config)#</p>	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	<pre>interface ethernet number</pre> <p>Example: switch(config)# interface ethernet 2/3 switch(config-if)#</p>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<pre>no switchport</pre> <p>Example: switch(config-if)# no switchport</p>	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。

	コマンド	目的
ステップ4	<pre>ip arp gratuitous {request update}</pre> <p>Example: <pre>switch(config-if)# ip arp gratuitous request</pre></p>	インターフェイス上で Gratuitous ARP をイネーブルにします。イネーブルがデフォルトです。
ステップ5	<pre>copy running-config startup-config</pre> <p>Example: <pre>switch(config-if)# copy running-config startup-config</pre></p>	(任意) この設定の変更を保存します。

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

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
<code>ip directed-broadcast</code>	ダイレクトブロードキャストから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 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ための収集スロットルレートリミッタをサポートしています。



(注)

到達しない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設定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。

はじめる前に

正しい VDC を使用していることを確認します (または **switchto vdc** コマンドを使用します)。

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

	コマンド	目的
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 Example: switch(config)# hardware ip glean throttle	ARP スロットリングをイネーブルにします。
ステップ 3	no hardware ip glean throttle Example: switch(config)# no hardware ip glean throttle	ARP スロットリングをディセーブルにします。
ステップ 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

次に、IP 収集スロットルをイネーブル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 収集スロットルの最大数の設定

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。

はじめる前に

正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。

手順の概要

1. `configure terminal`
2. `hardware ip glean throttle maximum count`
3. `no hardware ip glean throttle maximum count`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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	<code>hardware ip glean throttle maximum count</code> Example: <code>switch(config)# hardware ip glean</code> <code>throttle maximum 2134</code>	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	<code>no hardware ip glean throttle maximum count</code> Example: <code>switch(config)# no hardware ip glean</code> <code>throttle maximum 2134</code>	デフォルトの制限値を適用します。 デフォルト値は 1000 です。範囲は 0 ~ 16,383 エントリです。
ステップ4	<code>copy running-config startup-config</code> Example: <code>switch(config)# copy running-config</code> <code>startup-config</code>	(任意) この設定の変更を保存します。

次に、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する例を示します。

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

はじめる前に

正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。

手順の概要

1. `configure terminal`
2. `hardware ip glean throttle maximum timeout timeout-in-sec`
3. `no hardware ip glean throttle maximum timeout timeout-in-sec`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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	<code>hardware ip glean throttle maximum timeout <i>timeout-in-sec</i></code> Example: <code>switch(config)# hardware ip glean throttle maximum timeout 300</code>	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	<code>no hardware ip glean throttle maximum timeout <i>timeout-in-sec</i></code> Example: <code>switch(config)# no hardware ip glean throttle maximum timeout 300</code>	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	<code>copy running-config startup-config</code> Example: <code>switch(config)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

次に、インストールされているドロップ隣接関係のタイムアウトを設定する例を示します。

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

ハードウェア IP 収集スロットルの syslog の設定

特定のフローでドロップされたパケットの数が設定されているパケット数を超えた場合は、syslog を生成できます。

はじめる前に

正しい VDC を使用していることを確認します (または `switchto vdc` コマンドを使用します)。

手順の概要

1. `configure terminal`

2. `hardware ip glean throttle syslog pck-count`
3. `no hardware ip glean throttle syslog pck-count`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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	<code>hardware ip glean throttle syslog pck-count</code> Example: <code>switch(config)# hardware ip glean throttle syslog 1030</code>	特定のフローでドロップされたパケットの数が設定されているパケット数を超えた場合は、 <code>syslog</code> を生成します。
ステップ3	<code>no hardware ip glean throttle syslog pck-count</code> Example: <code>switch(config)# no hardware ip glean throttle syslog 1030</code>	デフォルトの制限値を適用します。 デフォルトは 10000 パケットです。範囲は 0 ~ 65535 パケットです。 (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	<code>copy running-config startup-config</code> Example: <code>switch(config)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

次に、特定のフローでドロップされたパケットの数が設定されているパケット数を超えた場合に `syslog` を生成する例を示します。

```
switch# configure terminal
switch(config)# hardware ip glean throttle syslog 1030
switch(config-if)# copy running-config startup-config
```

IPv4 設定の確認

IPv4 の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<code>show hardware forwarding ip verify</code>	IP パケット検証の設定を表示します。
<code>show ip adjacency</code>	隣接関係テーブルを表示します。
<code>show ip arp</code>	ARP テーブルを表示します。
<code>show ip interface</code>	IP 関連のインターフェイス情報を表示します。
<code>show ip arp statistics [vrf vrf-name]</code>	ARP 統計情報を表示します。
<code>show ip adjacency summary</code>	スロットル隣接関係の数のサマリーを表示します。

コマンド	目的
<code>show ip arp summary</code>	スロットル隣接関係の数のサマリーを表示します。
<code>show ip adjacency throttle statistics</code>	スロットリングされた隣接関係のみを表示します。

IPv4 の設定例

次に、IPv4 アドレスを設定する例を示します。

```
configure terminal
interface ethernet 1/2
no switchport
ip address 192.2.1.1/16
```

その他の関連資料

IP の実装に関連する詳細情報については、次の項を参照してください。

- 「[関連資料](#)」 (P.2-19)
- 「[標準](#)」 (P.2-19)

関連資料

関連項目	マニュアル名
IP CLI コマンド	『Cisco Nexus 3000 Series Command Reference』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

