



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 の前提条件 \(6 ページ\)](#)
- [IPv4 の注意事項および制約事項 \(6 ページ\)](#)
- [デフォルト設定 \(7 ページ\)](#)
- [IPv4 の設定 \(7 ページ\)](#)
- [IPv4 設定の確認 \(14 ページ\)](#)

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 \(2 ページ\)](#) 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 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。

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。

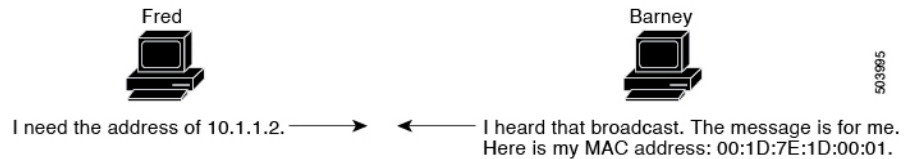
アドレス解決プロトコル

ネットワークング 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。

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。

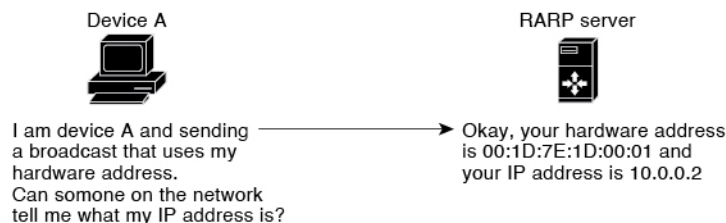
レイヤ2スイッチは、デバイス上のどのポートがそのポートだけに送信されたメッセージを受信するかを決定します。ただし、レイヤ3スイッチは、ARP キャッシュ (テーブル) を作成するデバイスです。

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ています。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 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。

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。
- **Cisco Nexus 3550-T - 10.1(2t)** リリース スイッチは、IPv4 パス全体のハードウェア ロード バランシングをサポートせず、IPv4 ECMP からの最初のパスだけをハードウェアにインストールします。追加のパスはソフトウェア ルーティング テーブルでのみ使用でき、最初のパスがダウンすると、次のパスがハードウェアに更新されます。さらに、ハードウェアにインストールするために ECMP パスが計算されたときに生成される syslog があります。

パラメータ	スケール番号
IP-Host-Route	3072 (最大) (クワッドあたり)
L3 ARP/隣接関係	386

パラメータ	スケール番号
IP-Routes	2304 (最大) (クワッドあたり) (注) すべての IPv4 ルート配布が Cisco Nexus® 3550-T ハードウェアに適合するわけではありません。ルートがハードウェアテーブルに収まらない場合は、ソフトウェア転送を行います。

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 : 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 :	インターフェイス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
	switch(config)# interface ethernet 1/3 switch(config-if)#	
ステップ 3	ip address ip-address/length [secondary] 例 : <pre>switch(config-if)# ip address 192.2.1.1 255.0.0.0</pre>	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。 <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 : <pre>switch(config-if)# show ip interface</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	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 : <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	interface ethernet number 例 : <pre>switch(config)# interface ethernet 1/3 switch(config-if)#</pre>	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 : <pre>switch(config-if)# ip address 192.168.1.1 255.0.0.0 secondary</pre>	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 : <pre>switch(config-if)# show ip interface</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	この設定変更を保存します。 (注) Cisco Nexus® 3550-T スイッチは、IPv4 パス全体のハードウェアロードバランシングをサポートしておらず、IPv4 ECMP からの最初のパスだけをハードウェアにインストールします。追加のパスはソフトウェアルーティングテーブルでのみ使用でき、最初のパスがダウンすると、次のパスがハードウェアに更新されます。

	コマンドまたはアクション	目的
		(注) Cisco Nexus® 3550-T スイッチは、インターフェイスで IP アドレスが設定されていない場合でも、ルート検索の結果に従って、MyMac を宛先として L3 パケットを転送します。SVI が作成されていない場合でも、MyMac パケットのルートテーブルルックアップが有効になっています。

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： <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	interface ethernet number 例： <pre>switch(config)# interface ethernet 1/3 switch(config-if)#</pre>	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： <pre>switch(config-if)# ip arp 192.168.1.1 0019.076c.1a78</pre>	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： <pre>switch(config-if)# copy running-config startup-config</pre>	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 1/3 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 1/3 switch(config-if)#	インターフェイス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 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 でのローカル プロキシ ARP を構成できます。

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 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 例： switch(config-if)# ip local-proxy-arp	SVI 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	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。
ステップ 2	interface ethernet number 例： switch(config)# interface ethernet 1/3 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。

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： 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	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
	例 : switch(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
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 default management]	ARP 統計情報を表示します。

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。