CHAPTER 2

IPv4 の設定

この章では、Cisco NX-OS デバイス上で、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）、およびインターネット制御メッセージ プロトコル（ICMP）を設定する方法について説明します。

この章では、次の内容について説明します。

IPv4 について

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、送信元または宛先の 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」（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。

IP 機能は、スーパーバイザ モジュールで終端する IPv4 パケットを処理するだけでなく、IPv4 パケットを転送する役割を果たします。これには、IPv4 ユニキャスト/マルチキャスト ルートの検索、リバース パス転送（RPF）のチェック、およびソフトウェア アクセス コントロール リスト/ポリシー ベース ルーティング（ACL/PBR）の転送が含まれます。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/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

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、サブネット化によって論理サブネットごとに最大 254 のホストが許可されるが、1 つの物理サブネット上に 300 のホスト アドレスが必要な場合は、ルータまたはアクセス サーバ上のセカンダリ IP アドレスを使用して、1 つの物理サブネットを使用する 2 つの論理サブネットを構成できます。
- 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、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。

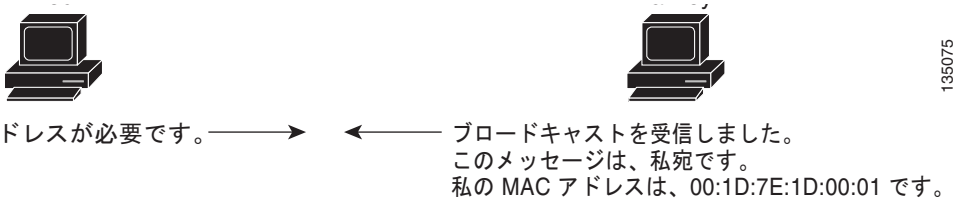
（注） ネットワーク セグメント上のいずれかのデバイスがセカンダリ IPv4 アドレスを使用している場合は、同じネットワーク インターフェイス上の他のすべてのデバイスも、同じネットワークまたはサブネットからのセカンダリ アドレスを使用する必要があります。ネットワーク セグメント上で、一貫性のない方法でセカンダリ アドレスを使用すると、ただちにルーティング ループが発生する可能性があります。

アドレス解決プロトコル

ネットワーキング デバイスおよびレイヤ 3 スイッチは ARP を使用して、IP（ネットワーク層）アドレスを物理（Media Access Control（MAC）層）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。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



宛先デバイスが別のデバイスを挟んだリモート ネットワーク上に存在する場合もプロセスは同じですが、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 アドレスに対する 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。

システムで定義されたデフォルトの CoPP ポリシーは、スーパーバイザ モジュール宛ての ARP ブロードキャスト パケットにレート制限を適用します。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、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、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。情報が古くなる可能性があるため、定期的に期限切れになるように設定されたキャッシュ エントリを保持する必要があります。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 エントリおよびダイナミック エントリ

スタティック ルーティングでは、各デバイスのインターフェイスごとに 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 ルーティングでは、ルート テーブルの保守に必要な作業が増えます。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 アドレスのみを使用する独自のアドレス テーブルを構築します。デバイスには、IP アドレスと、対応する MAC アドレスの両方を含む 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。

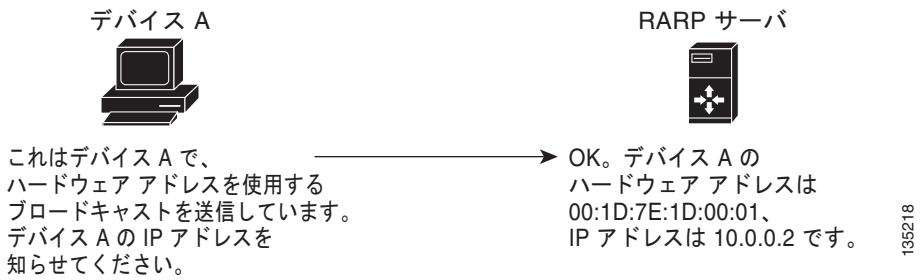
レイヤ 2 スイッチは、メッセージの宛先であるデバイスにどのポートが接続されているかを特定し、そのポートにのみ送信します。ただし、レイヤ 3 スイッチは、ARP キャッシュ（テーブル）を作成するデバイスです。

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 を使用すると、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しながら、引き続きそのデバイスをルータの前にあるパブリック ネットワーク上に存在す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層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、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、重複した IP アドレスを検出するために、同一の送信元 IP アドレスと宛先 IP アドレスを含む要求を送信します。Cisco NX-OS Release 4.0(3) 以降のリリースでは、Gratuitous ARP 要求または ARP キャッシュ更新のイネーブル化/ディセーブル化がサポートされます。

収集スロットル

ラインカードで着信 IP パケットを転送する場合、ネクスト ホップに対するアドレス解決プロトコル（ARP）要求が解決されていないと、そのラインカードはスーパーバイザにパケットを転送します（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。

Cisco Nexus 7000 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。最大エントリ数を超えると、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。

パス MTU ディスカバリ

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

ICMP

インターネット制御メッセージ プロトコル（ICMP）を使用すると、エラーや IP 処理に関連する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、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。VRF は仮想化デバイス コンテキスト（VDC）内にあります。デフォルトでは、特に別の VDC および VRF を設定しない限り、Cisco NX-OS によりデフォルト VDC およびデフォルト VRF が使用されます。詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』および第 14 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	IP 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 のライセンス スキームの詳細については、『*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。

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。
- F2 シリーズ モジュールは、IPv4 トンネル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。

- 「IP パケット検証の設定」（P.2-15）
- 「ダイレクト ブロードキャストの設定」（P.2-16）
- 「IP 収集スロットルの設定」（P.2-17）
- 「ハードウェア IP 収集スロットルの最大数の設定」（P.2-18）
- 「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.2-19）
- 「ハードウェア IP 収集スロットルの syslog の設定」（P.2-20）

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

IPv4 アドレス指定の設定

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。

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. **interface ethernet** *number*
3. **ip address** *ip-address/length*
4. （任意）**show ip interface**
5. （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**
	
	例：
	`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*
	
	例：
	`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。

	コマンド	目的
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	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。 • 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、プレフィクス長として示される場合もあります。プレフィクス長は、プレフィ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。
ステップ 4	**show ip interface** 例： 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 5	**copy running-config startup-config** 例： 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)# ip address 192.168.1.1 255.0.0.0
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。

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. **interface ethernet** *number*
3. **ip address** *ip-address/length*
4. （任意）**show ip interface**
5. （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** 例： 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* 例： 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	**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	show ip interface 例： 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 5	**copy running-config startup-config** 例： 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

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。

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. **interface ethernet** *number*
3. **ip arp** *ipaddr mac_addr*
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** 例： 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* 例： 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	**ip arp** *ipaddr mac_addr* 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	**copy running-config startup-config** 例： 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、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)# ip arp 192.168.1.1 0019.076c.1a78
switch(config-if)# copy running-config startup-config
```

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. **interface ethernet** *number*
3. **ip proxy-arp**
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** 例： 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* 例： 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	**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 4	**copy running-config startup-config** 例： 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、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)# ip proxy-arp
switch(config-if)# copy running-config startup-config
```

ローカル プロキシ ARP の設定

デバイス上でローカル プロキシ ARP 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. **interface ethernet** *number*
3. **ip local-proxy-arp**
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** 例： 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* 例： 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	**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	**copy running-config startup-config** 例： 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、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)# 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。

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. **interface ethernet** *number*
3. **ip arp gratuitous** {**request** | **update**}
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** 例： 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* 例： 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	**ip arp gratuitous** {**request** | **update**} 例： switch(config-if)# ip arp gratuitous request	インターフェイス上で Gratuitous 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 4	**copy running-config startup-config** 例： 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、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 ip arp gratuitous request
switch(config-if)# copy running-config startup-config
```

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。

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. **ip tcp path-mtu-discovery**
3. （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** 例： 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	**ip tcp path-mtu-discovery** 例： switch(config)# ip tcp path-mtu-discovery	パス MTU 探索をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）この設定の変更を保存します。

IP パケット検証の設定

Cisco NX-OS は、IP パケット検証をチェックする侵入検知システム（IDS）をサポートしています。これらの IDS チェックは、イネーブルまたはディセーブルにすることができます。

IDS チェックをイネーブルにするには、グローバル 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
hardware ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}	IP アドレスに対して次の IDS チェックを実行します。 • **destination zero** : 宛先 IP アドレスが 0.0.0.0 である場合は IP パケットをドロップします。 • **identical** : 送信元 IP アドレスが宛先 IP アドレスと同じである場合は IP パケットをドロップします。 • **reserved** : IP アドレスが 127.x.x.x の範囲内にある場合は、それをドロップします。 • **source** : 送信元 IP アドレスが 255.255.255.255（ブロードキャスト）であるか、または 224.x.x.x の範囲内（マルチキャスト）である場合は、IP パケットをドロップします。
hardware ip verify checksum	パケット チェックサムが無効である場合は IP パケットをドロップします。
hardware ip verify fragment	パケット フラグメントにゼロ以外のオフセットがあり、DF ビットがアクティブである場合は、IP パケットをドロップします。

コマンド	目的
hardware ip verify length {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **minimum**}	IP アドレスに対して次の IDS チェックを実行します。 • **consistent** : イーサネット フレーム サイズが IP パケット長にイーサネット ヘッダーを加えた値以上である場合は、IP パケットをドロップします。 • **maximum max-frag** : 最大フラグメント オフセットが 65536 より大きい場合は IP パケットをドロップします。 • **maximum max-tcp** : TCP 長が IP ペイロード長より大きい場合は IP パケットをドロップします。 • **maximum udp** : IP ペイロード長が UDP パケット長より小さい場合は IP パケットをドロップします。 • **minimum** : イーサネット フレーム長が IP パケット長に 4 オクテット（CRC 長）を加えた値より小さい場合は、IP パケットをドロップします。
hardware ip verify tcp tiny-frag	IP フラグメント オフセットが 1 の場合、または IP フラグメント オフセットが 0 で IP ペイロード長が 16 未満の場合は、TCP パケットをドロップします。
hardware ip verify version	ethertype が 4（IPv4）にセットされていない場合は IP パケットをドロップします。

IP パケット検証の設定を表示するには、**show hardware forwarding ip verify** コマンドを使用します。

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、そのアドレスにより、そのインターフェイスの接続先の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着信 IP 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。必要に応じて、アクセス リストを通過する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 リストでこれらのブロードキャストをフィルタリングできます。

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。

コマンド	目的
ip directed-broadcast [*acl*]	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。必要に応じて、IP アクセス リストでこれらのブロードキャストをフィルタリングできます。

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。

IP 収集スロットルをイネーブルにすることができます。

（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**
	
	例：
	`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** 例： `switch(config)# hardware ip glean throttle`	ARP スロットリングをイネーブルにします。

	コマンド	目的
ステップ 3	no **hardware ip glean throttle** 例： switch(config)# no hardware ip glean throttle	ARP スロットリングをディセーブルにします。
ステップ 4	**copy running-config startup-config** 例： 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るドロップ隣接関係の最大数を制限できます。

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	**configure terminal** 例： 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 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。

	コマンド	目的
ステップ 3	**no hardware ip glean throttle maximum** ***count*** 例： `switch(config)# no hardware ip glean throttle maximum 2134`	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 ～ 32767 エントリです。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（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	**configure terminal**
	
	例：
	`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 maximum timeout** ***timeout-in-sec*** 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。

	コマンド	目的
ステップ 3	**no hardware ip glean throttle maximum timeout** ***timeout-in-sec*** 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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（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	**configure terminal**
	
	例：
	`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 syslog** ***pck-count*** 例： `switch(config)# hardware ip glean throttle syslog 1030`	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 を生成します。

	コマンド	目的
ステップ 3	**no hardware ip glean throttle syslog** *pck-count* **例：** `switch(config)# no hardware ip glean throttle syslog 1030`	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	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（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 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show 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 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 adjacency throttle statistics	スロットリングされた隣接関係のみを表示します。
show ip interface	IP 関連の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。

IPv4 の設定例

N7K-F132-15 モジュールは、レイヤ 2 スイッチングのみを実行します。そのため、1 つの Nexus 7000 シリーズ シャーシ内にこのモジュールと M シリーズ モジュールの両方が存在するときにレイヤ 3 の手順を実行すると、システムはプロキシ ルーティングを使用します。また、プロキシ ルーティングも設定できます。

ここでは、次の内容について説明します。

- 「例：モジュール上のすべてのポートをプロキシ ルーティングのために予約する」（P.2-22）
- 「例：プロキシ ルーティングのためのポートの予約」（P.2-24）
- 「例：プロキシ ルーティングからのポートの除外」（P.2-25）

例：モジュール上のすべてのポートをプロキシ ルーティングのために予約する

次に、モジュール上のすべてのポートをプロキシ ルーティングのために予約する例を示します。

ステップ 1　どのモジュールがデバイス内に存在するかを判定します。

```
switch# show module
Mod  Ports  Module-Type                        Model              Status
---  -----  ---------------------------------- ------------------ ------------
1    32     10 Gbps Ethernet Module            N7K-M132XP-12      ok
2    48     10/100/1000 Mbps Ethernet Module N7K-M148GT-11      ok
3    48     1000 Mbps Optical Ethernet Modul N7K-M148GS-11      ok
5    0      Supervisor module-1X               N7K-SUP1           active *
6    0      Supervisor module-1X               N7K-SUP1           ha-standby
8    32     1/10 Gbps Ethernet Module          N7K-F132XP-15      ok
```

F1 モジュールはスロット 8 内にあり、M1 モジュールはスロット 1 ～ 3 内にあります。

ステップ 2　どのポートが VDC で使用可能かを判定します。

```
switch# show vdc membership | end "Ethernet3/48"

vdc_id: 0 vdc_name: Unallocated interfaces:

vdc_id: 1 vdc_name: switch interfaces:
       Ethernet1/9           Ethernet1/10          Ethernet1/11
       Ethernet1/12          Ethernet1/13          Ethernet1/14
       Ethernet1/15          Ethernet1/16          Ethernet1/17
       Ethernet1/18          Ethernet1/19          Ethernet1/20
       Ethernet1/21          Ethernet1/22          Ethernet1/23
       Ethernet1/24          Ethernet1/25          Ethernet1/26
       Ethernet1/27          Ethernet1/28          Ethernet1/29
       Ethernet1/30          Ethernet1/31          Ethernet1/32

       Ethernet2/1           Ethernet2/2           Ethernet2/3
       Ethernet2/4           Ethernet2/5           Ethernet2/6
       Ethernet2/7           Ethernet2/8           Ethernet2/9
       Ethernet2/10          Ethernet2/11          Ethernet2/12
       Ethernet2/25          Ethernet2/26          Ethernet2/27
       Ethernet2/28          Ethernet2/29          Ethernet2/30
       Ethernet2/31          Ethernet2/32          Ethernet2/33
       Ethernet2/34          Ethernet2/35          Ethernet2/36
       Ethernet2/37          Ethernet2/38          Ethernet2/39
       Ethernet2/40          Ethernet2/41          Ethernet2/42
       Ethernet2/43          Ethernet2/44          Ethernet2/45
       Ethernet2/46          Ethernet2/47          Ethernet2/48

       Ethernet3/1           Ethernet3/2           Ethernet3/3
       Ethernet3/4           Ethernet3/5           Ethernet3/6
       Ethernet3/7           Ethernet3/8           Ethernet3/9
       Ethernet3/10          Ethernet3/11          Ethernet3/12
       Ethernet3/13          Ethernet3/14          Ethernet3/15
       Ethernet3/16          Ethernet3/17          Ethernet3/18
       Ethernet3/19          Ethernet3/20          Ethernet3/21
       Ethernet3/22          Ethernet3/23          Ethernet3/24
       Ethernet3/25          Ethernet3/26          Ethernet3/27
       Ethernet3/28          Ethernet3/29          Ethernet3/30
       Ethernet3/31          Ethernet3/32          Ethernet3/33
       Ethernet3/34          Ethernet3/35          Ethernet3/36
       Ethernet3/37          Ethernet3/38          Ethernet3/39
       Ethernet3/40          Ethernet3/41          Ethernet3/42
```

```
       Ethernet3/43          Ethernet3/44          Ethernet3/45
       Ethernet3/46          Ethernet3/47          Ethernet3/48
```

ステップ 3　どのポートがプロキシ ルーティングに使用可能かを判定します。

```
switch# show hardware proxy layer-3 detail

Global Information:
       F1 Modules:     Count: 1         Slot: 8
       M1 Modules:     Count: 3         Slot: 1-3

       Replication Rebalance Mode:             Manual
       Number of proxy layer-3 forwarders:     13
       Number of proxy layer-3 replicators:    8

Forwarder Interfaces                    Status     Reason
-------------------------------------------------------------------------------
Eth1/9, Eth1/11, Eth1/13, Eth1/15       up         SUCCESS
Eth1/10, Eth1/12, Eth1/14, Eth1/16      up         SUCCESS
Eth1/17, Eth1/19, Eth1/21, Eth1/23      up         SUCCESS
Eth1/18, Eth1/20, Eth1/22, Eth1/24      up         SUCCESS
Eth1/25, Eth1/27, Eth1/29, Eth1/31      up         SUCCESS
Eth1/26, Eth1/28, Eth1/30, Eth1/32      up         SUCCESS
Eth2/1-12                               up         SUCCESS
Eth2/25-36                              up         SUCCESS
Eth2/37-48                              up         SUCCESS
Eth3/1-12                               up         SUCCESS
Eth3/13-24                              up         SUCCESS
Eth3/25-36                              up         SUCCESS
Eth3/37-48                              up         SUCCESS

Replicator Interfaces                   #Interface-Vlan   Interface-Vlan
-------------------------------------------------------------------------------
Eth1/1, Eth1/3, Eth1/5, Eth1/7, Eth1/9,  0
Eth1/11, Eth1/13, Eth1/15
Eth1/2, Eth1/4, Eth1/6, Eth1/8, Eth1/10, 0
Eth1/12, Eth1/14, Eth1/16
Eth1/17, Eth1/19, Eth1/21, Eth1/23,      0
Eth1/25, Eth1/27, Eth1/29, Eth1/31
Eth1/18, Eth1/20, Eth1/22, Eth1/24,      0
Eth1/26, Eth1/28, Eth1/30, Eth1/32
Eth2/1-24                                0
Eth2/25-48                               0
Eth3/1-24                                0
Eth3/25-48                               0
switch#
```

（注）　ポートは、対応するポート グループ内に一覧表示されます。

ステップ 4　ユニキャストおよびマルチキャスト プロキシ ルーティングのためにモジュールを予約します。

```
switch# configure terminal
switch(config)# hardware proxy layer-3 forwarding use module 2
switch(config)# hardware proxy layer-3 replication use module 2
```

ステップ 5　この設定を確認します。

```
switch(config)# show hardware proxy layer-3 detail

Global Information:
       F1 Modules:     Count: 1         Slot: 8
       M1 Modules:     Count: 3         Slot: 1-3
```

```
       Replication Rebalance Mode:             Manual
       Number of proxy layer-3 forwarders:     3
       Number of proxy layer-3 replicators:    2

Forwarder Interfaces                       Status     Reason
-------------------------------------------------------------------------------
Eth2/1-12                                  up         SUCCESS
Eth2/25-36                                 up         SUCCESS
Eth2/37-48                                 up         SUCCESS

Replicator Interfaces                      #Interface-Vlan   Interface-Vlan
-------------------------------------------------------------------------------
Eth2/1-24                                  0
Eth2/25-48                                 0
switch(config)#
```

例：プロキシ ルーティングのためのポートの予約

次に、モジュール上の一部のポートをプロキシ ルーティングのために予約する例を示します。

ステップ 1　モジュール上のポートのサブセットを予約します。

```
switch(config)# hardware proxy layer-3 forwarding use interface ethernet 2/1-6 <----
-subset of port group
switch(config)# hardware proxy layer-3 replication use interface ethernet 2/1-6 <----
-subset of port group
```

この例では、ポート グループのポートのサブセットを予約します。

ステップ 2　この設定を確認します。

```
switch(config)# show hardware proxy layer-3 detail

Global Information:
       F1 Modules:     Count: 1         Slot: 8
       M1 Modules:     Count: 3         Slot: 1-3

       Replication Rebalance Mode:             Manual
       Number of proxy layer-3 forwarders:     1
       Number of proxy layer-3 replicators:    1

Forwarder Interfaces                       Status     Reason
-------------------------------------------------------------------------------
Eth2/1-12                                  up         SUCCESS

Replicator Interfaces                      #Interface-Vlan   Interface-Vlan
-------------------------------------------------------------------------------
Eth2/1-24                                  0 <----------- full port group
switch(config)#
```

（注）　ポート グループ内のすべてのポートがプロキシ ルーティングのために予約されています。

例：プロキシ ルーティングからのポートの除外

次に、モジュール上の一部のポートをプロキシ ルーティングから除外する例を示します。

ステップ 1　モジュール上のポートのサブセットを除外します。

```
switch(config)# hardware proxy layer-3 forwarding exclude interface ethernet 2/1-12
<---subset of port group
switch(config)# hardware proxy layer-3 replication exclude interface ethernet 2/1-12
```

ステップ 2　この設定を確認します。

```
switch(config)# show hardware proxy layer-3 detail

Global Information:
       F1 Modules:     Count: 1         Slot: 8
       M1 Modules:     Count: 3         Slot: 1-3

       Replication Rebalance Mode:             Manual
       Number of proxy layer-3 forwarders:     12
       Number of proxy layer-3 replicators:    7

Forwarder Interfaces                       Status     Reason
-------------------------------------------------------------------------------
Eth1/9, Eth1/11, Eth1/13, Eth1/15          up         SUCCESS
Eth1/10, Eth1/12, Eth1/14, Eth1/16         up         SUCCESS
Eth1/17, Eth1/19, Eth1/21, Eth1/23         up         SUCCESS
Eth1/18, Eth1/20, Eth1/22, Eth1/24         up         SUCCESS
Eth1/25, Eth1/27, Eth1/29, Eth1/31         up         SUCCESS
Eth1/26, Eth1/28, Eth1/30, Eth1/32         up         SUCCESS
Eth2/25-36                                 up         SUCCESS
Eth2/37-48                                 up         SUCCESS
Eth3/1-12                                  up         SUCCESS
Eth3/13-24                                 up         SUCCESS
Eth3/25-36                                 up         SUCCESS
Eth3/37-48                                 up         SUCCESS

Replicator Interfaces                      #Interface-Vlan   Interface-Vlan
-------------------------------------------------------------------------------
Eth1/1, Eth1/3, Eth1/5, Eth1/7, Eth1/9,    0
Eth1/11, Eth1/13, Eth1/15
Eth1/2, Eth1/4, Eth1/6, Eth1/8, Eth1/10,   0
Eth1/12, Eth1/14, Eth1/16
Eth1/17, Eth1/19, Eth1/21, Eth1/23,        0
Eth1/25, Eth1/27, Eth1/29, Eth1/31
Eth1/18, Eth1/20, Eth1/22, Eth1/24,        0
Eth1/26, Eth1/28, Eth1/30, Eth1/32
Eth2/25-48                                 0 <---- e 2/1-24 excluded
Eth3/1-24                                  0
Eth3/25-48                                 0
switch(config)#
```

（注）　ポート グループ内のすべてのポートがプロキシ ルーティングから除外されています。

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.2-26）
- 「標準」（P.2-26）

関連資料

関連項目	マニュアル名
IP CLI コマンド	*『Cisco Nexus 7000 Series NX-OS Unicast Routing 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。	—

IP 機能の履歴

表 2-2 は、この機能のリリースの履歴です。

表 2-2　IP 機能の履歴

機能名	リリース	機能情報
IP	6.0(1)	F2 シリーズ モジュールに対して更新されました。
IP ダイレクト ブロードキャストのための ACL フィルタ	5.2(1)	IP アクセス リストで IP ダイレクト ブロードキャストをフィルタリングするためのサポートが追加されました。
収集スロットル	5.1(1)	IPv4 収集スロットルのサポートが追加されました。
IP	5.0(2)	Release 4.2 以降、変更はありません。
IP	4.2(1)	Release 4.1 以降、変更はありません。
ARP	4.1(4)	ARP ブロードキャスト ストーム防止機能のサポートが追加されました。
IP	4.1(3)	**platform ip verify** コマンドが **hardware ip verify** コマンドに変更されました。
ARP	4.0(3)	Gratuitous ARP のサポートが追加されました。次のコマンドが追加されました。 • **ip arp gratuitous** {**request** | **update**}
IP	4.0(1)	この機能が導入されました。