# DHCP スヌーピングの設定

この章の内容は、次のとおりです。

# DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのように機能します。具体的には、次の処理を実行します。

- 信頼できない発信元からの DHCP メッセージを検証するとともに、DHCP サーバからの無効な応答メッセージを除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

ダイナミック ARP インスペクション（DAI）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

DHCP スヌーピングは、VLAN ごとにグローバルにイネーブルになっています。デフォルトでは、すべての VLAN で DHCP スヌーピングは非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

# DHCP の概要

Dynamic Host Configuration Protocol（DHCP）はインターネット ホストに設定パラメータを提供します。DHCP は次の処理を行います。

- ホスト固有の設定パラメータを DHCP サーバからホストに伝達する。
- ホストにネットワーク アドレスを割り当てる。

DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバ ホストが、ダイナミックに設定されるホストに対して、ネットワーク アドレスを割り当て、設定パラメータを提供します。

デフォルトで、DHCP は次の IP アドレス割り当てメカニズムをサポートします。

- 自動割り当て：DHCP は無期限の IP アドレスをクライアントに割り当てます。
- 動的割り当て：DHCP は一定期間（またはクライアントがアドレスを明示的に放棄するまで）IP アドレスをクライアントに割り当てます。
- 手動割り当て：ネットワーク管理者が IP アドレスをクライアントに割り当てます。DHCP はクライアントに割り当てられたアドレスを伝達するために使われます。

DHCP メッセージの形式は、ブートストラップ プロトコル（BOOTP）メッセージの形式に基づいています。この形式では、BOOTP リレー エージェント機能および BOOTP クライアントと DHCP サーバ間の相互運用性がサポートされます。BOOTP リレー エージェントを使用すると、各物理ネットワーク セグメントに DHCP サーバを導入する必要がありません。

DHCP は IANA によって BOOTP に割り当てられた 2 つのポートを使用します。宛先 UDP ポート 67 はサーバにデータを送信し、UDP ポート 68 はクライアントにデータを送信します。

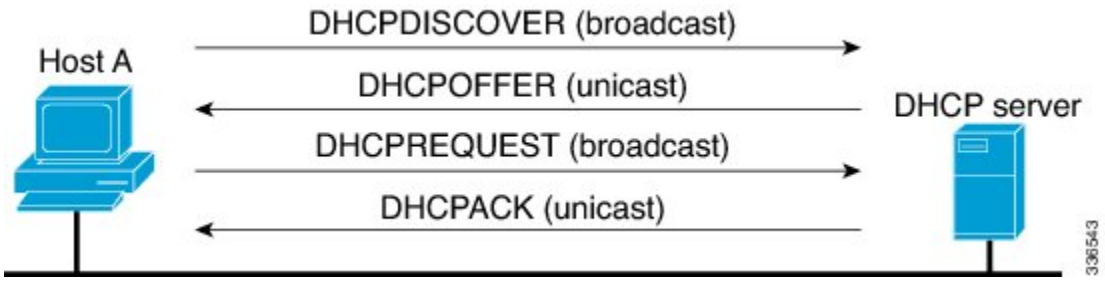
DHCP の動作は次の 4 つの基本フェーズに分類されます。

- IP 検出
- IP リース オファー
- IP 要求
- IP リース確認応答

（注） DHCP の動作フェーズは、多くの場合 DORA（検出、オファー、要求、および確認応答）と略されます。

次の図では、DHCP クライアントが DHCP サーバに IP アドレスを要求する際の基本的な手順を示します。クライアントであるホスト A が DHCPDISCOVER ブロードキャスト メッセージを送信して、Cisco IOS DHCP サーバの場所を特定します。DHCP サーバは、DHCPOFFER ユニキャスト メッセージで、設定パラメータ（IP アドレス、MAC アドレス、ドメイン名、IP アドレスのリースなど）をクライアントに提示します。

**図 *1*： *DHCP* サーバに対する *IP* アドレスの *DHCP* 要求**




クライアントは、DHCPREQUEST ブロードキャスト メッセージで、提示された IP アドレスの正式な要求を DHCP サーバに戻します。DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。

# BOOTP パケット形式

BOOTP 要求と応答は、次の図と表に示すように UDP データグラムでカプセル化されます。

**図 *2*：*BOOTP* パケット形式**

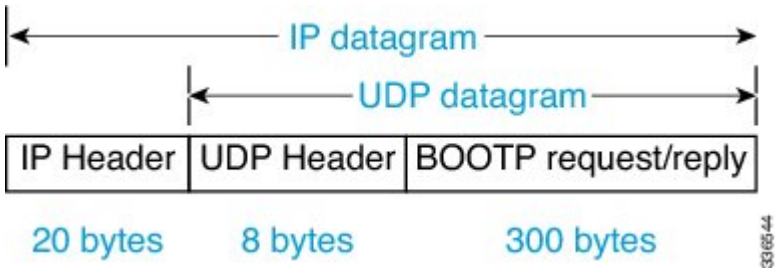



**図 *3*：*300* バイトの *BOOTP* 要求と応答の形式**

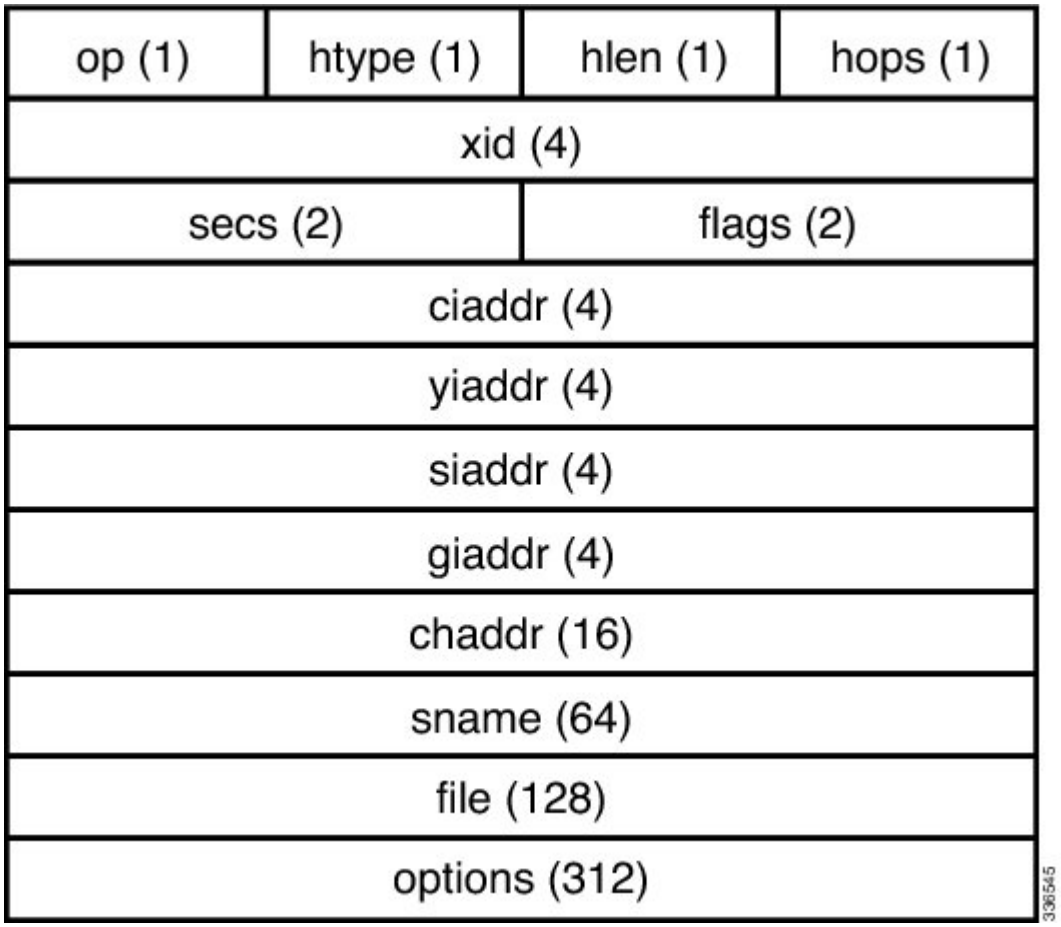


表 *1* : *BOOTP* 要求と応答の形式

| フィールド | バイト | 名前 | 説明 |
|---|---|---|---|
| op | 1 | OpCode | パケットが要求か応答かを識別します。1=BOOTREQUEST および 2=BOOTREPLY。 |
| htype | 1 | Hardware Type | ネットワーク ハードウェア タイプを指定します。 |
| hlen | 1 | Hardware Length | ハードウェア アドレスの長さを指定します。 |
| hops | 1 | Hops | クライアントは値をゼロに設定し、要求がルータを経由して転送されるとその値が増分されます。 |
| xid | 4 | Transaction ID | クライアントによって選択される乱数。特定の DHCP トランザクション用に交換されるすべての DHCP メッセージはこの ID（xid）を使用します。 |
| secs | 2 | Seconds | DHCP プロセスが開始されてからの秒数を指定します。 |
| flags | 2 | Flags | メッセージがブロードキャストかユニキャストかを示します。 |
| ciaddr | 4 | Client IP Address | クライアントが IP アドレスの状態をバインディング済み、更新、または再バインディングと認識したときに使用されます。 |

| フィールド | バイト | 名前 | 説明 |
|---|---|---|---|
| yiaddr | 4 | Your IP Address | クライアントの IP アドレスが 0.0.0.0 の場合、DHCP サーバは提供されたクライアントの IP アドレスをこのフィールドに指定します。 |
| siaddr | 4 | Server IP Address | クライアントが DHCP サーバの IP アドレスを認識している場合、このフィールドには DHCP サーバ アドレスが入力されます。認識していない場合は、DHCP サーバからの DHCPOFFER および DHCPACK で使用されます。 |
| giaddr | 4 | Router IP Address | DHCP/BootP リレー エージェントによって入力されるゲートウェイ IP アドレス。 |
| chaddr | 16 | Client MAC Address | DHCP クライアントの MAC アドレス。 |
| sname | 64 | Server Name | 任意のサーバ ホスト名。 |
| File | 128 | Boot Filename | ブート ファイル名。 |
| Options | 変数 | Option Parameters | DHCP サーバによって提供される任意のパラメータ。RFC 2132 には使用可能なすべてのオプションが記載されています。 |

# 信頼できる送信元と信頼できない送信元

DHCP スヌーピングでは、ポートを「信頼できる」または「信頼できない」送信元として識別します。DHCP スヌーピングをイネーブルにすると、デフォルトでは、vEthernet（vEth）ポートはすべて「信頼できない」となり、イーサネット ポート（アップリンク）、ポート チャネル、特殊な vEth ポート（仮想サービス ドメイン（VSD）などの他の機能が使用する）はすべて「信頼できる」となります。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるデバイスです。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、クライアント ポートは信頼できない送信元として扱われます。

Cisco Nexus 1000V スイッチでは、接続しているインターフェイスの信頼状態を設定して、送信元が信頼できることを示します。アップリンク ポート（アップリンク機能を持つことがポート プロファイルで定義されている）は、信頼できるポートです。したがって、信頼できないポートであると設定することはできません。

DHCP スヌーピングは以下を実行して、信頼できないクライアントと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。

- 信頼できるポートに接続されたサーバからの DHCP メッセージのみを受け入れる。サーバからクライアントへのデータである UDP ポート 68 の DHCP メッセージが、信頼できないポートで受信された場合にすべてドロップする。
- リース IP アドレスを持つクライアントに関する情報が保存される DHCP スヌーピング バインディング データベースを構築および管理する。
- DHCP スヌーピング バインディング データベースを使用して、クライアントからの以降の要求を検証する。

デフォルトでは、すべての VLAN で DHCP スヌーピングは非アクティブです。DHCP スヌーピングは 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。DHCP スヌーピングは、VLAN ごとにグローバルにイネーブルになっています。

# DHCP スヌーピング バインディング データベース

DHCP スヌーピングは、代行受信した DHCP メッセージから抽出された情報を使用して、各仮想イーサネット モジュール（VEM）上でデータベースを動的に構築および維持します。DHCP スヌーピングがイネーブルになっている VLAN にホストが関連付けられている場合、このデータベースには、リース IP アドレスを持つ信頼できない各クライアントのエントリが含まれています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

（注） DHCP スヌーピング バインディング データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

デバイスが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、DHCP スヌーピングを使用すると、デバイスが DHCPACK メッセージをサーバから受信したときにデータベースにエントリを追加できます。DHCP スヌーピングでは、IP アドレスのリース期限が過ぎた際に、またはデバイスが DHCP クライアントから DHCPRELEASE または DHCP DECLINE を受信した際に、またはデバイスが DHCP サーバから DHCPNACK を受信した際にデータベースからエントリを削除することもできます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

動的に追加されたエントリをバインディング データベースから削除するには、clear ip dhcp snooping binding コマンドを使用します。

# DHCP スヌーピングの Option 82 データ挿入

DHCP では、多数の加入者に対する IP アドレスの割り当てを一元管理できます。Option 82 をイネーブルにすると、デバイスはクライアントが接続されている vEthernet 番号とクライアントが属する仮想スーパーバイザ モジュール（VSM）を使って、ネットワークに接続されている加入者デバイス（およびその MAC アドレス）を識別します。加入者 LAN 上のマルチ ホストをアクセス デバイスの同一ポートに接続でき、これらは一意に識別されます。

Cisco Nexus 1000V で Option 82 をイネーブルにすると、次のイベントが順番に表示されます。

1. ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
2. Cisco Nexus 1000V 仮想イーサネット モジュール（VEM）は、この DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）、受信されたパケットの発信元のポート ID、および vEth 番号（回線 ID サブオプション）が含まれます。
3. デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
4. DHCP サーバはこのパケットを受信します。サーバは、Option 82 に対応している場合、リモート ID、回線 ID、またはその両方を使用して IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることのできる IP アドレスの数の制限などのポリシーを実装したりできます。DHCP サーバは、Option 82 フィールドを DHCP 応答内にエコーします。
5. DHCP サーバは、その応答を Cisco Nexus 1000V に送信します。Cisco Nexus 1000V は、リモート ID フィールドと回線 ID フィールドを検証し、最初に挿入した Option 82 データであることを確認します。Cisco Nexus 1000V VEM は、Option 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続されているインターフェイスにそのパケットを転送します。

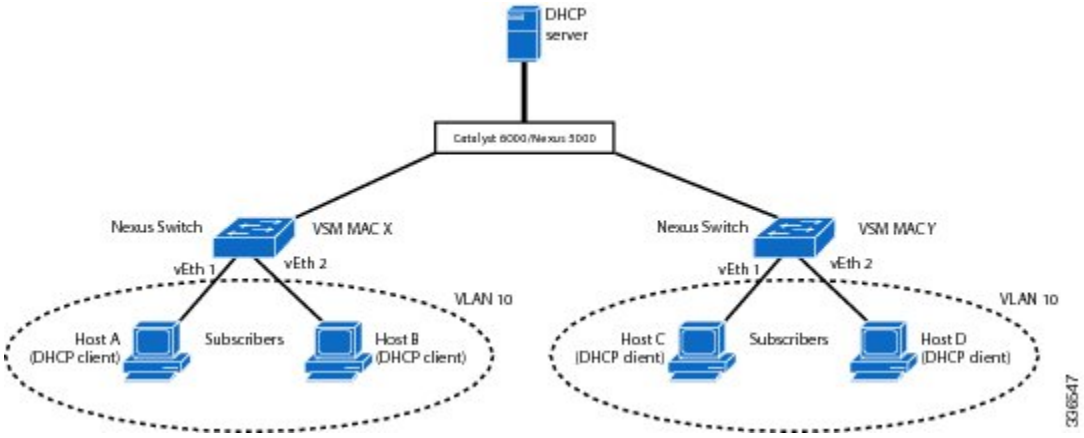
### Option 82 の挿入

次の図では、Option 82 の挿入の一般的な使用例を説明します。ホスト A とホスト B は、VLAN 10 上にある VSM MAC アドレス X を持つ Cisco Nexus 1000V に属しています。同様に、ホスト C とホスト D は VLAN 10 上にある VSM MAC アドレスが Y の Cisco Nexus 1000V に属しています。すべてのクライアントは、アップストリーム スイッチに接続されている共通の DHCP サーバから IP アドレスを受け取ります。

Option 82 の挿入により、ホスト C とホスト A に特定の IP アドレスを割り当てることができます。これらのホストはどちらも VLAN 10 の一部で、vEth 番号が同じ（vEthernet1）です。DHCP パケット内の VSM MAC アドレスを使用して、ホスト D とホスト B（vEthernet 2）に IP アドレスを割り当てることもできます。

1 つ目の Cisco Nexus 1000V でホストされているクライアント A および B からの DHCP パケットでは、リモート ID フィールドに VSM MAC X が含まれ、クライアント C および D からの要求ではリモート ID フィールドに VSM MAC Y が含まれます。クライアントが同じ VLAN（VLAN 10）に属していても、リモート ID に基づいて、DHCP サーバにプールを設定して各 Cisco Nexus 1000V 上のクライアントに個別の IP セットを割り当てることができます。

**図 *4*：*Option 82* の挿入トポロジ**




### サブオプションのパケット形式

次の図は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示しています。Cisco Nexus 1000V は、DHCP スヌーピングをグローバルにイネーブルにしたときや、Option 82 データの挿入と削除をイネーブルにしたときにこれらのパケット形式を使用します。回線 ID サブオプションの回線 ID 文字列は、クライアントが接続された vEth ポートの名前です。リモー

ト ID サブオプションの MAC アドレスは、Cisco Nexus 1000V の Asynchronous Inter-process Communication（AIPC）インターフェイスです。

図 *5*：リモート *ID* サブオプション フレーム フォーマット

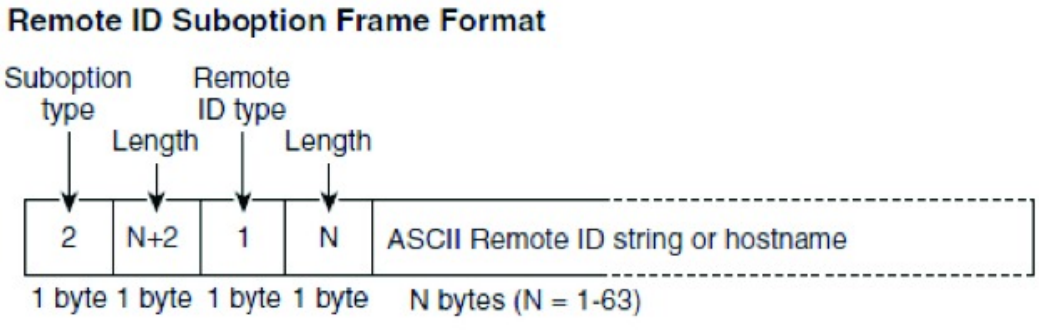
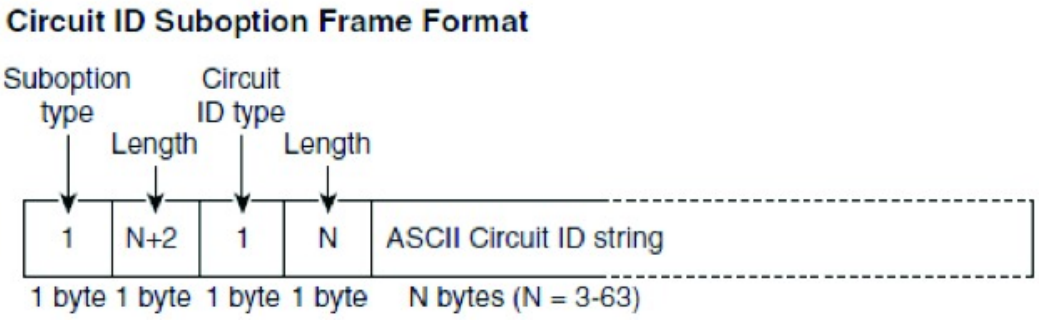



図 *6*：回線 *ID* サブオプション フレーム フォーマット




# DHCP スヌーピングのライセンス要件

次の表に、この機能のライセンス要件を示します。

| 機能 | ライセンス要件 |
|---|---|
| DHCP スヌーピング | Cisco Nexus 1000V では階層ベースのライセンス アプローチが採用されています。Cisco Nexus 1000V は、Essential と Advanced の 2 つのエディションで出荷されます。スイッチエディションが Advanced エディションとして設定されている場合、ライセンスを必要とする高度な機能として DHCP スヌーピング、ダイナミック ARP インスペクション（DAI）、および IP ソースガード（IPSG）を使用できます。<br>（注） feature dhcp コマンドを使用して Cisco Nexus 1000V で DHCP スヌーピングをイネーブルにします。スイッチ エディションが Essential の場合、feature コマンドは失敗します。 |

# DHCP スヌーピングの前提条件

- DHCP スヌーピングを設定するには、DHCP に関する知識が必要です。
- この機能のライセンス要件については、「ライセンス要件」の項を参照してください。

# DHCP スヌーピングの注意事項および制約事項

- DHCP スヌーピング データベースは各 VEM 上に作成され、1 つのデータベースに最大 2048 個のバインディングを格納できます。すべての VEM の DHCP バインディング エントリを合計した最大数は 12,000 です。
- DHCP スヌーピングをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートは、デフォルトで信頼できるポートとなっています。これらのポートを「信頼できない」と設定しても、その設定は無視されます。
- VSM の接続に VEM が使用される場合、つまり VSM の VSM Asynchronous Inter-process Communication（AIPC）、管理、およびインバンドのポートが特定の VEM 上にある場合は、これらの仮想イーサネット インターフェイスを信頼できるインターフェイスとして設定する必要があります。
- Cisco Nexus 1000V からのデバイス アップストリームの接続インターフェイスは、このデバイスで DHCP スヌーピングがイネーブルになっている場合、「信頼できる」として設定する必要があります。

- プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、対応するすべてのセカンダリ VLAN でスヌーピングがイネーブルになります。セカンダリ VLAN でのみ DHCP スヌーピングをイネーブルにする設定は無効です。
- 128 を超えるアクセス コントロール リスト（ACL）（MAC と IP ACL の組み合わせ）を設定する場合は、VSM RAM が 3 GB（3072 MB）に設定されていることを確認します。
- VXLAN ポートでは DHCP スヌーピングをイネーブルにできません。

# DHCP 設定のデフォルト値

| パラメータ | デフォルト |
|---|---|
| DHCP 機能 | ディセーブル |
| DHCP スヌーピング グローバル | ディセーブル |
| DHCP スヌーピング VLAN | ディセーブル |
| DHCP スヌーピングの MAC アドレス検証 | イネーブル |
| DHCP スヌーピング信頼状態 | Trusted：イーサネット インターフェイス、vEthernet インターフェイス、およびポート チャネル（VSD 機能に参加しているもの）。<br>Untrusted：VSD 機能に参加していない vEthernet インターフェイス。 |
| DHCP スヌーピング レート制限 | なし |

# DHCP スヌーピングの設定

## DHCP スヌーピングの最小設定

1. DHCP 機能をイネーブルにします。
2. DHCP スヌーピングをグローバルにイネーブルにします。
3. 少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。

   デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。
4. DHCP サーバとデバイスが、信頼できるインターフェイスを使用して接続されていることを確認します。

# DHCP 機能のイネーブル化またはディセーブル化

デフォルトでは、DHCP はディセーブルです。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **feature dhcp** | 機能をグローバルにイネーブルにします。no コマンド オプションの後に copy running-start コマンドを付けると、DHCP 関連の設定がすべて削除されます。copy running-start コマンドを使わずに no コマンドを使用すると、DHCP 関連の設定はスタートアップ コンフィギュレーションに保存されたまま残ります。DHCP スヌーピングはライセンスを必要とする高度な機能として使用できます。Cisco Nexus 1000V のライセンス要件の詳細については、『Cisco Nexus 1000V License Configuration Guide』を参照してください。 |
| ステップ 3 | switch(config)# **show feature** | （任意）<br>使用可能な各機能の状態（イネーブルまたはディセーブル）を表示します。 |
| ステップ 4 | switch(config)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         enabled
http-server           1         enabled
lacp                  1         enabled
netflow               1         disabled
port-profile-roles    1         enabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
switch(config)# copy running-config startup-config
```

# DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

DHCP スヌーピングに関する次の情報を知っておく必要があります。

- デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。
- DHCP スヌーピングがグローバルにディセーブルになると、DHCP スヌーピングはすべて停止し、DHCP メッセージは中継されなくなります。
- DHCP スヌーピングを設定した後でグローバルにディセーブルにした場合も、残りの設定は維持されます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | 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** | switch(config)# **feature dhcp** | DHCP をグローバルにイネーブルにします。DHCP スヌーピングはライセンスを必要とする高度な機能として使用できます。 |
| **ステップ 3** | switch(config)# [**no**] **ip dhcp snooping** | IP DHCP スヌーピングをイネーブルにします。**no** オプションを使用すると、DHCP スヌーピングがディセーブルになりますが、既存の DHCP スヌーピング設定は保存されます。 |
| **ステップ 4** | switch(config)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| **ステップ 5** | switch(config)# **show ip dhcp snooping** | （任意）<br>DHCP スヌーピングの IP 設定を表示します。 |
| **ステップ 6** | switch(config)# **copy running-config startup-config** | （任意）<br>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。 |

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)# show running-config dhcp
feature dhcp ip dhcp snooping
switch (config#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:none
DHCP snooping is operational on the following VLANs:none
Insertion of Option 82 is disabled
Verification of MAC address is enabled
```

```
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
------------         -------        ---------
Vethernet1           No              Unlimited
Vethernet2           No              Unlimited
Vethernet3           No              Unlimited
Vethernet4           No              Unlimited
Vethernet5           No              Unlimited

switch(config)# copy running-config startup-config
```

# VLANに対するDHCPスヌーピングのイネーブル化またはディセーブル化

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

（注） プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、対応するすべてのセカンダリ VLAN でスヌーピングがイネーブルになります。セカンダリ VLAN でのみ DHCP スヌーピングをイネーブルにする設定は無効です。

## はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

## 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **feature dhcp** | DHCP をグローバルにイネーブルにします。DHCP スヌーピングはライセンスを必要とする高度な機能として使用できます。 |
| ステップ 3 | switch(config)# [**no**] **ip dhcp snooping vlan vlan-list** | vlan-list で指定する VLAN の DHCP スヌーピングをイネーブルにします。**no** オプションを使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。 |
| ステップ 4 | switch(config)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| ステップ 5 | switch(config)# **show ip dhcp snooping** | （任意）<br>DHCP スヌーピングの IP 設定を表示します。 |
| ステップ 6 | switch(config)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | ションにコピーして、変更を継続的に保存します。 |

（注） DHCP スヌーピングがイネーブルになっている VLAN が動作可能であることを確認してください。DHCP スヌーピングが VLAN 上で動作しない場合は、VLAN が Cisco Nexus 1000V で設定済みで、アクティブ状態であるかどうかを確認します。

次に、DHCP スヌーピングを VLAN でイネーブルまたはディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# show running-config dhcp
feature dhcp
ip dhcp snooping
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted        Pkt Limit
------------          -------        ---------
Vethernet1            No              Unlimited
Vethernet2            No              Unlimited
Vethernet3            No              Unlimited
Vethernet4            No              Unlimited
Vethernet5            No              Unlimited


switch(config)# copy running-config startup-config
```

# DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルまたはディセーブルにします。信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。MAC アドレス検証はデフォルトでイネーブルになります。

## はじめる前に

EXEC モードで CLI にログインする必要があります。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# [**no**] **ip dhcp snooping verify mac-address** | DHCP スヌーピングの MAC アドレス検証をイネーブルにします。**no** オプションを使用すると MAC アドレス検証がディセーブルになります。 |
| ステップ 3 | switch(config)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| ステップ 4 | switch(config)# **show ip dhcp snooping** | （任意）<br>DHCP スヌーピングの IP 設定を表示します。 |
| ステップ 5 | switch(config)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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て、変更を継続的に保存します。 |

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# no ip dhcp snooping verify mac-address
switch(config)# show running-config dhcp
feature dhcp
ip dhcp snooping
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is disabled
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
------------         -------        ---------
Vethernet1           No              Unlimited
Vethernet2           No              Unlimited
Vethernet3           No              Unlimited
Vethernet4           No              Unlimited
Vethernet5           No              Unlimited
switch(config)# copy running-config startup-config
```

# インターフェイスの信頼状態の設定

ここでは、特定の仮想イーサネット（vEth）インターフェイスが DHCP メッセージの送信元として信頼できるものかどうかを設定する手順を説明します。次のいずれかの方法を使用して、DHCP 信頼状態を設定できます。

- レイヤ 2 vEthernet インターフェイス
- レイヤ 2 vEthernet インターフェイスのポート プロファイル

デフォルトでは、vEthernet インターフェイスは「信頼できない」となっています。ただし、仮想サービス ドメイン（VSD）などの他の機能で使用される特別な vETH ポートは例外であり、信頼されています。

DHCP スヌーピングをシームレスに実行するために、ダイナミック ARP インスペクション（DAI）、IP ソース ガード、および VSD サービス VM のポートはデフォルトで信頼できるポートになっています。これらのポートを「信頼できない」と設定しても、その設定は無視されます。

## はじめる前に

- EXEC モードで CLI にログインしていること。
- vEthernet インターフェイスがレイヤ 2 インターフェイスとして設定されていること。

## 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | 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** | switch(config)# **interface vethernet***interface-number* | 指定した vEthernet インターフェイスのインターフェイス コンフィギュレーション モードを開始します。インターフェイス設定を使用して、インターフェイスを信頼できるインターフェイスとして設定する場合に、このコマンドを使用します。 |
| **ステップ 3** | switch(config)# **port-profile***profilename* | 指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。ポート プロファイル設定を使用して、インターフェイスを信頼できるインターフェイスとして設定します。 |
| **ステップ 4** | switch(config-if)# [**no**] **ip dhcp snooping trust** | DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | switch(config-if)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| ステップ 6 | switch(config-if)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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て、変更を永続的に保存します。 |

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip dhcp snooping trust

switch(config)# port-profile vm-data
switch(config-port-profile)# ip dhcp snooping trust
switch(config-port-profile)# show running-config dhcp
feature dhcp
interface Vethernet1
  ip dhcp snooping trust
interface Vethernet3
  ip dhcp snooping trust
interface Vethernet10
  ip dhcp snooping trust
interface Vethernet11
  ip dhcp snooping trust
interface Vethernet12
  ip dhcp snooping trust
interface Vethernet13
  ip dhcp snooping trust
ip dhcp snooping
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config-port-profile)# copy running-config startup-config
```

# DHCP パケットのレート制限の設定

各ポートで受信する DHCP パケット/秒のレートの制限を設定するには、次の手順を実行します。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

次の情報を知っている必要があります。

- ポートは、この手順で設定した DHCP パケット/秒のレートの制限を超えると、errdisabled 状態になります。
- インターフェイスまたはポート プロファイルにレート制限を設定できます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **interface vethernet***interface-number* | 指定した vEthernet インターフェイスのインターフェイス 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 | switch(config)# **port-profile***profilename* | 指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。 |
| ステップ 4 | switch(config-if)# [**no**] **ip dhcp snooping limit rate***rate* | DHCP パケット/秒（1 ～ 2048）のレートに制限を設定します。noオプションを使用すると、レート制限が削除されます。 |
| ステップ 5 | switch(config-if)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| ステップ 6 | switch(config-if)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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て、変更を永続的に保存します。 |

次に、DHCP パケットのレート制限を設定する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip dhcp snooping limit rate 15
switch(config-if)# show running-config dhcp
switch(config-if)# copy running-config startup-config

switch(config)# port-profile vm-data
switch(config-port-profile)# ip dhcp snooping limit rate 15
switch(config-port-profile)# show running-config dhcp
feature dhcp
interface Vethernet3
  ip dhcp snooping trust
  ip dhcp snooping limit rate 15
ip dhcp snooping
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config-port-profile)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
```

```
------------          -------         ---------
Vethernet1            No               Unlimited
Vethernet2            No               Unlimited
Vethernet3            Yes               15
Vethernet4            No               Unlimited
Vethernet5            No               Unlimited
switch(config-port-profile)# copy running-config startup-config
```

# DHCP レート制限違反がディセーブルなポートの検出

DHCP レート制限の超過がディセーブルになっているポートの検出をグローバルに設定するには、次の手順を実行します。

インターフェイスを error-disabled 状態から手動で回復するには、shutdown コマンドを入力してから、no shutdown コマンドを入力する必要があります。

（注） 設定されたレートに違反すると、ポートは自動的に errdisable 状態になります。

## はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

## 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | 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** | switch(config)# **feature dhcp** | DHCP をグローバルにイネーブルにします。DHCP スヌーピングはライセンスを必要とする高度な機能として使用できます。 |
| **ステップ 3** | switch(config)# [**no**] **errdisable detect cause dhcp-rate-limit** | DHCP error-disabled 検出をイネーブルにします。**no** オプションを使用すると、DHCP error-disabled 検出がディセーブルになります。 |
| **ステップ 4** | switch(config)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| **ステップ 5** | switch(config)# **show errdisable detect** | （任意）<br>ポートが error-disabled 状態になっている理由を表示します。 |
| **ステップ 6** | switch(config)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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て、変更を永続的に保存します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|

次に、DHCP レート制限違反がディセーブルになっているポートを検出する例を示します。

```
switch# configure terminal
switch(config)# errdisable detect cause dhcp-rate-limit
switch(config)# show running-config dhcp
switch(config)# show errdisable detect
ErrDisable Reason            Timer Status
-----------------            ------------
link-flap                    enabled
dhcp-rate-limit              enabled
arp-inspection               enabled
ip-addr-conflict             enabled
switch(config)# copy running-config startup-config
```

# DHCP レート制限違反がディセーブルなポートの回復

DHCP レート制限の違反がディセーブルになっているポートの自動リカバリをグローバルに設定するには、次の手順を実行します。

レートによって errdisable ステートになるポート。

インターフェイスを error-disabled 状態から手動で回復するには、shutdown コマンドを入力してから、no shutdown コマンドを入力する必要があります。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | 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** | switch(config)# [**no**] **errdisable recovery cause dhcp-rate-limit** | DHCP error-disabled 検出をイネーブルにします。**no** オプションを使用すると、DHCP error-disabled 検出がディセーブルになります。 |
| **ステップ 3** | switch(config)# **errdisable recovery interval***time interval* | DHCP error-disabled 回復間隔を設定します。*timer interval* は 30 ～ 65535 の秒数です。 |
| **ステップ 4** | switch(config)# **show errdisable recovery** | （任意）<br>vEth が error-disabled 状態から回復する回復間隔を表示します。 |
| **ステップ 5** | switch(config)# **copy running-config startup-config** | （任意）<br>リブートおよびリスタート時に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 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | ションにコピーして、変更を継続的に保存します。 |

次に、DHCP レート制限違反がディセーブルになっているポートを回復する例を示します。

```
switch# configure terminal
switch(config)# errdisable detect cause dhcp-rate-limit
switch(config)# errdisable recovery interval 30
switch(config)# show running-config dhcp
switch(config)# show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            ------------
link-flap                    disabled
dhcp-rate-limit              enabled
arp-inspection               disabled
security-violation           disabled
psecure-violation            disabled
failed-port-state            enabled
ip-addr-conflict             disabled

        Timer interval: 30
switch(config)# copy running-config startup-config
```

# DHCP スヌーピング バインディング データベースのクリア

## すべてのバインディング エントリの消去

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **clear ip dhcp snooping binding** | DHCP スヌーピング バインディング データベースに動的に追加されたエントリを消去します。 |
| ステップ 2 | switch# **show ip dhcp snooping binding** | （任意）<br>DHCP スヌーピング バインディング データベースを表示します。 |

```
switch# clear ip dhcp snooping binding
switch# show ip dhcp snooping binding
```

## インターフェイスのバインディング エントリの消去

### はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- インターフェイスに関する次の情報が収集されていること。
  - VLAN ID
  - IP アドレス
  - MAC アドレス

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} \| **vlan** *vlan-id1* \| **interface** *interface-id1*] | DHCP スヌーピング バインディング データベースから、動的に追加されたインターフェイスのエントリを消去します。 |
| ステップ 2 | switch# **show ip dhcp snooping binding** | DHCP スヌーピング バインディング データベースを表示します。 |

```
switch# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface
vethernet 1
switch# show ip dhcp snooping binding
```

# DHCP のスイッチおよび回線情報のリレー

DHCP パケットの VSM MAC アドレスおよび vEth ポート情報をグローバルにリレーできます。このプロセスは、Option 82 およびリレー エージェント情報オプションとも呼ばれます。

### はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

（注） HA ペア設定で、DHCP パケットの Option 82 フィールドに挿入されている MAC は、現在のアクティブ VSM の AIPC インターフェイスのものです。したがって DHCP サーバの一致基準は、スイッチオーバーを考慮してプライマリとセカンダリ両方の VSM の AIPC MAC に一致する必要があります。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# [**no**] **ip dhcp snooping information option** | DHCP パケットの VSM MAC アドレスおよび vEthernet ポート情報をリレーするよう DHCP を設定します。<br>この設定を削除するには、**no** オプションを使用します。 |
| ステップ 3 | switch(config)# **show running-config dhcp** | （任意）<br>DHCP スヌーピング設定を表示します。 |
| ステップ 4 | switch(config)# **show ip dhcp snooping** | （任意）<br>DHCP スヌーピングの IP 設定を表示します。 |
| ステップ 5 | switch(config)# **copy running-config startup-config** | （任意）<br>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。 |

次に、DHCP のスイッチおよび回線情報をリレーする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)# show running-config dhcp
feature dhcp
interface Vethernet3
  ip dhcp snooping trust
  ip dhcp snooping limit rate 15
ip dhcp snooping
ip dhcp snooping information option
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is enabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted        Pkt Limit
------------          -------        ---------
Vethernet1            No              Unlimited
Vethernet2            No              Unlimited
Vethernet3            Yes              15
Vethernet4            No              Unlimited
Vethernet5            No              Unlimited
switch(config)# copy running-config startup-config
```

# スタティック IP エントリの追加または削除

デフォルトでは、デバイスにはスタティック IP ソース エントリは設定されていません。Cisco Nexus1000 上のスタティック IP エントリを追加または削除するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal** | 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 | switch(config)# **feature dhcp** | IPSG機能をイネーブルにします。IPSGはライセンスを必要とする高度な機能として使用できます。 |
| ステップ 3 | switch(config)# [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface vethernet** *interface-number* | 現在のインターフェイスのスタティック IP ソース エントリを作成します。スタティック IP ソース エントリを削除する場合は、no オプションを使用します。 |
| ステップ 4 | switch(config)# **show ip dhcp snooping binding** [**interface vethernet** *interface-number*] | （任意）<br>スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレス バインディングを表示します。スタティック エントリは、Type カラムに「static」と表示されます。 |
| ステップ 5 | switch(config-if)# **copy running-config startup-config** | （任意）<br>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。 |

次に、スタティック IP エントリを追加または削除する例を示します。

```
switch# configure terminal
switch(config)#  ip source binding 10.5.22.178 001f.28bd.0014 vlan 100 interface vethernet
 3
switch(config)# show ip dhcp snooping binding interface vethernet 3
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  --------------
00:1f:28:bd:00:14  10.5.22.178      infinite   static       100   Vethernet3
switch(config)# copy running-config startup-config
```

# DHCP スヌーピング設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

| コマンド | 目的 |
|---|---|
| **show running-config dhcp** | DHCP スヌーピング設定を表示します。 |
| **show ip dhcp snooping** | DHCP スヌーピングに関する一般的な情報を表示します。 |
| **show ip dhcp snooping binding** | DHCP スヌーピング バインディング テーブルの内容を表示します。 |
| **show feature** | DHCP などの使用可能な機能と、それらがイネーブルかどうかを表示します。 |

# DHCP スヌーピングのモニタリング

DHCP スヌーピングの統計情報をモニタするには、show ip dhcp snooping statistics コマンドを使用します。

```
swtich(config)# show ip dhcp snooping statistics

Packets processed 0
Packets forwarded 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to service dhcp not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
```

# DHCP スヌーピングの設定例

次に、VLAN 100 上で DHCP スヌーピングをイネーブルにする例を示します。vEthernet インターフェイス 5 が「信頼できる（trusted）」となっているのは、DHCP サーバがこのインターフェイスに接続されているからです。次に、クライアントが接続されているインターフェイスでレート制限を 15 pps に設定する例を示します。クライアントは port-profile client-pp を使用し、レート制限違反が発生するとクライアント ポートは error-disabled 状態になり、60 秒後に回復します。DHCP サーバによって、クライアントの 1 つにはスタティック DHCP IP が割り当てられ、1 つの IP アドレスに無制限のリース期間が割り当てられています。

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 100
switch(config)# interface veth 5
switch(config-if)# ip dhcp snooping trust
switch(config)# port-profile type vethernet client-pp
switch(config-port-prof)# ip dhcp snooping limit rate 15
switch(config)# errdisable detect cause dhcp-rate-limit
```

```
switch(config)# errdisable recovery interval 60
switch(config)# ip source binding 192.168.0.55  00:50:56:81:42:74 vlan 100 interface vethernet
 12

switch (config-if)# show feature
Feature Name          Instance      State
--------------------        -------      --------
cts                         1         disabled
dhcp-snooping               1         enabled
http-server                 1         enabled
lacp                        1         enabled
netflow                     1         enabled
network-segmentation        1         enabled
port-profile-roles          1         disabled
private-vlan                1         enabled
segmentation                1         enabled
sshServer                   1         enabled
tacacs                      1         disabled
telnetServer                1         disabled
vtracker                    1         disabled

switch(config-if)# show run dhcp

feature dhcp

interface Vethernet1
  ip dhcp snooping limit rate 15

interface Vethernet5
  ip dhcp snooping trust

interface Vethernet10
  ip dhcp snooping limit rate 15

interface Vethernet11
  ip dhcp snooping limit rate 15

interface Vethernet12
  ip dhcp snooping limit rate 15

interface Vethernet13
  ip dhcp snooping limit rate 15
ip dhcp snooping
ip dhcp snooping vlan 100
ip source binding 192.168.0.55  00:50:56:81:42:74 vlan 100 interface vethernet 12

Note: Client interfaces Vethernet 1,10-13 are part of port-profile “client-pp”

swtich (config-if)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100
DHCP snooping is operational on the following VLANs:
100
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted               Pkt Limit
------------          -------         --------
Vethernet1            No                     15
Vethernet2            No                     Unlimited
Vethernet3            No                     Unlimited
Vethernet4            No                     Unlimited
Vethernet5            Yes                    Unlimited
Vethernet7            No                     Unlimited
Vethernet8            No                     Unlimited
Vethernet9            No                     Unlimited
Vethernet10           No                    15
Vethernet11           No                    15
Vethernet12           No                    15
Vethernet13           No                    15
```

```
switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------- ----------- ----- -------------
00:50:56:81:42:46   192.168.0.9      28570     dhcp-snoop   100    Vethernet1
00:50:56:81:42:59   192.168.0.69     28591     dhcp-snoop   100    Vethernet10
00:50:56:81:42:6d   192.168.0.251    28559     dhcp-snoop   100    Vethernet11
00:50:56:81:42:72   192.168.0.48     infinite  static       100    Vethernet12
00:50:56:81:42:74   192.168.0.55     infinite  dhcp-snoop   100    Vethernet13
```

（注） DHCP サーバが発行した無制限のリース期間のエントリは、Lease Sec 列が infinite、Type が dhcp-snoop になります。

クライアント インターフェイスがセカンダリ VLAN の一部である場合、対応するプライマリ VLAN のエントリが DHCP バインディング テーブルに表示されます。

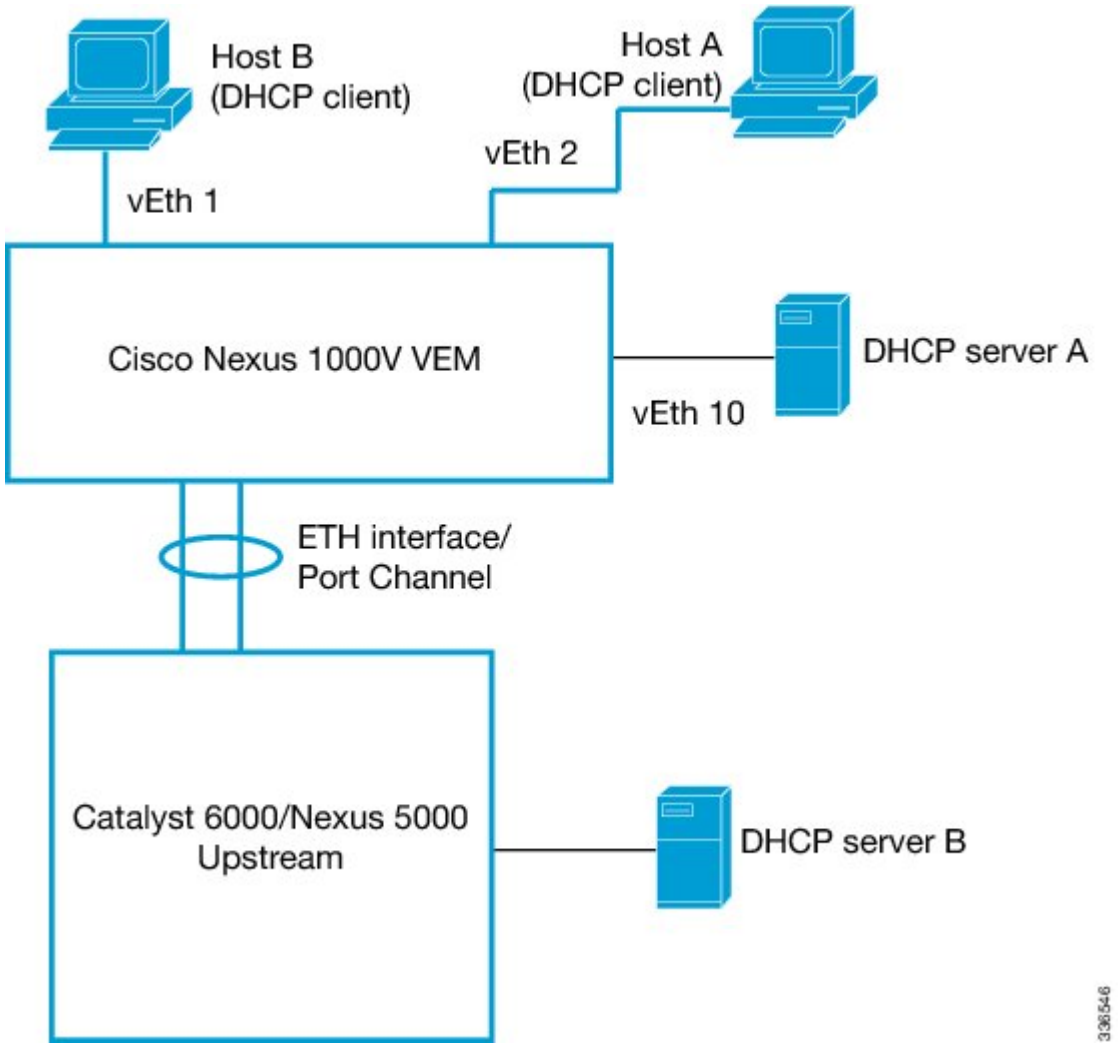
# ネットワークの信頼設定および DHCP サーバ設置の設定例

### Cisco Nexus 1000V ネットワーク内外の DHCP サーバおよび Cisco Nexus 1000V 上のクライアント

次に、Nexus 1000V 上にサーバ A、およびアップストリーム スイッチ上にサーバ B という 2 つの DHCP サーバがある例を示します。Cisco Nexus 1000V 上のイーサネット ポートおよびポートチャネル インターフェイスはデフォルトで信頼されるため、クライアント A および B は信頼設定を追加しなくても DHCP サーバ B から IP アドレスを取得できます。

次の図の場合、DHCP サーバ A を使用するには、サーバが接続されている vEthernet 10 で信頼設定を行う必要があります。

図 *7*： ***Cisco Nexus 1000V*** ネットワーク内外の ***DHCP*** サーバおよび ***Cisco Nexus 1000V*** 上のクライアント

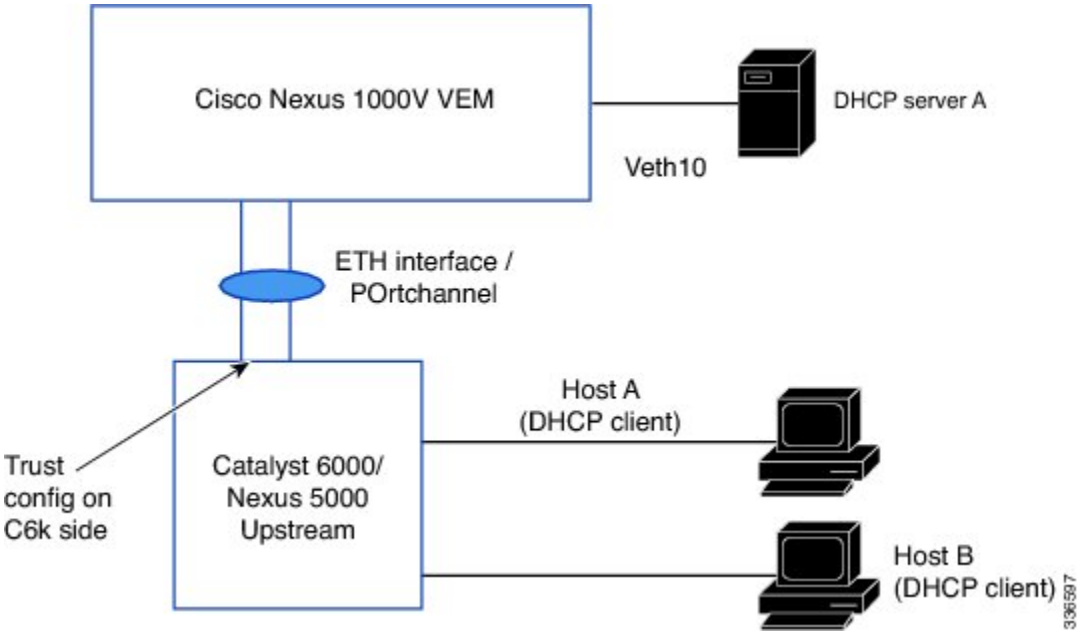



### Cisco Nexus 1000V ネットワーク内の DHCP サーバおよび Cisco Nexus 1000V 外のクライアント

管理者が Cisco Nexus 1000V 上の仮想マシン（VM）で DHCP サーバを稼働させていて、クライアントが Cisco Nexus 1000V 外にある場合は、アップストリーム スイッチ上に信頼できるインターフェイスを設定できます。

次の図ではサーバ A が Cisco Nexus 1000V 上にあり、クライアント A および B は、アップストリーム側のポートで信頼がイネーブルになっている場合にのみサーバ A から IP アドレスを取得できます。

**図 *8*： *Cisco Nexus 1000V* ネットワーク内の *DHCP* サーバおよび *Cisco Nexus 1000V* 外のクライアント**




# 標準

| 標準 | タイトル |
|---|---|
| RFC-2131 | 『Dynamic Host Configuration Protocol』（http://tools.ietf.org/html/rfc2131） |
| RFC-3046 | 『DHCP Relay Agent Information Option』（http://tools.ietf.org/html/rfc3046） |

# DHCP スヌーピングの機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

| 機能名 | リリース | 機能情報 |
|---|---|---|
| DHCP スヌーピング | 5.2(1)SM1(5.1) | この機能が導入されました。 |