



## DHCP スヌーピングの設定

この章では、Cisco NX-OS デバイスで Dynamic Host Configuration Protocol (DHCP) スヌーピングを設定する手順について説明します。

- [DHCP スヌーピングの概要, 1 ページ](#)
- [DHCP リレー エージェントの概要, 7 ページ](#)
- [DHCP スヌーピングの注意事項および制約事項, 8 ページ](#)
- [DHCP スヌーピングのデフォルト設定, 10 ページ](#)
- [DHCP スヌーピングの設定, 10 ページ](#)
- [DHCP スヌーピング設定の確認, 22 ページ](#)
- [DHCP バインディングの表示, 22 ページ](#)
- [DHCP スヌーピング バインディング データベースのクリア, 23 ページ](#)
- [DHCP スヌーピングの設定例, 24 ページ](#)

## 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な機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できないソースからの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外する。
- DHCP スヌーピング バインディング データベースを構築し、管理する。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する。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1 つの VLAN 上または VLAN の特定の範囲でイネーブルにできます。

## 機能のイネーブル化とグローバルなイネーブル化

DHCP スヌーピングを設定するときは、DHCP スヌーピング機能のイネーブル化と DHCP スヌーピングのグローバルなイネーブル化の違いを理解することが重要です。

### 機能のイネーブル化

DHCP スヌーピング機能は、デフォルトではディセーブルです。DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングまたはこれに依存する機能を設定できません。DHCP スヌーピングおよびその依存機能を設定するコマンドは、DHCP スヌーピングがディセーブルになっているときは使用できません。

DHCP スヌーピング機能をイネーブルにすると、スイッチで DHCP スヌーピング バインディング データベースの構築と維持が開始されます。DHCP スヌーピング バインディング データベースに依存する機能は、その時点から使用できるようになり、設定も可能になります。

DHCP スヌーピング機能をイネーブルにしても、グローバルにイネーブルになるわけではありません。DHCP スヌーピングをグローバルにイネーブルにするには、個別に行う必要があります。

DHCP スヌーピング機能をディセーブルにすると、スイッチから DHCP スヌーピングの設定がすべて削除されます。DHCP スヌーピングをディセーブルにして設定を維持したい場合は、DHCP スヌーピング機能をディセーブルにするのではなく、DHCP スヌーピングをグローバルにディセーブル化します。

### グローバルなイネーブル化

DHCP スヌーピングのイネーブル化の実行後、DHCP スヌーピングはデフォルトでグローバルにディセーブルになります。グローバルなイネーブル化は第 2 レベルのイネーブル化です。これにより、DHCP スヌーピング バインディング データベースのイネーブル化とは別に、スイッチがアクティブに DHCP スヌーピングを実行しているかどうかを個別に制御できます。

DHCP スヌーピングをグローバルにイネーブルにすると、DHCP スヌーピングがイネーブルになっている VLAN の信頼できない各インターフェイスについて、受信した DHCP メッセージの検証が開始され、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。

DHCP スヌーピングをグローバルにディセーブルにすると、DHCP メッセージの検証と、信頼できないホストからの以降の要求の検証を停止します。DHCP スヌーピング バインディング データベースも削除されます。DHCP スヌーピングをグローバルにディセーブルにしても、DHCP スヌーピングの設定や、DHCP スヌーピング機能に依存するその他の機能の設定は削除されません。

## 信頼できるソースおよび信頼できないソース

DHCP スヌーピングがトラフィックの送信元を信頼するかどうかを設定できます。信頼できないソースの場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。こうした攻撃を防ぐため、DHCP スヌーピングは信頼できない送信元からのメッセージをフィルタリングします。

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スイッチです。これらのスイッチには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるスイッチやネットワーク外のスイッチは信頼できない送信元です。一般的に、ホストポートは信頼できない送信元として扱われます。

サービスプロバイダーの環境では、サービスプロバイダーネットワークにないスイッチは、信頼できない送信元です（カスタマースイッチなど）。ホストポートは、信頼できないソースです。

Cisco Nexus デバイスでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態です。DHCP サーバインターフェイスは、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。ユーザのネットワーク内でスイッチ（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホストポートインターフェイスは、通常、信頼できるインターフェイスとしては設定しません。



(注) DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

## 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した情報を使用し、ダイナミックにデータベースを構築し維持します。ホストが、DHCP スヌーピングがイネーブルになっている VLAN に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 アドレスを含む信頼できない各ホス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。

スイッチが特定の 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、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、データベースにエントリが追加されます。IP アドレスのリース期限が切れると、また

はホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベースのエントリが削除されます。

DHCP スヌーピング バインディング データベース内の各エントリには、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、およびホストに関連付けられた VLAN 番号とインターフェイスの情報が含まれています。

**clear ip dhcp snooping binding** コマンドを使用すると、バインディング データベースからエントリ削除できます。

## DHCP スヌーピングの Option 82 データの挿入

DHCP は多数の加入者に対する IP アドレスの割り当てを一元的に管理できます。Option 82 をイネーブルにすると、デバイスは、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 NX-OS デバイスで Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- 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 NX-OS デバイスは、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）と、受信されたパケットの発信元のポート ID である `vlan-mod-port`（回線 ID サブオプション）が含まれます。ポート チャネルの背後に存在するホストの場合、回線 ID には、そのポート チャネルの `if_index` が入力されます。



(注)

vPC ピア スイッチの場合、リモート ID サブオプションには、両方のスイッチで一意である vPC スイッチ MAC アドレスが含まれます。この MAC アドレスは、vPC ドメイン ID を使用して計算されます。Option 82 情報は、DHCP 要求が最初に受信されたスイッチで挿入された後、他の vPC ピア スイッチに転送されます。

- 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 NX-OS デバイスに送信します。Cisco NX-OS デバイスは、リモート ID フィールドや、場合によっては回線 ID フィールドを検査することによって、そのデバイスが Option 82 データを最初に挿入したことを確認します。Cisco NX-OS デバイスは、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。

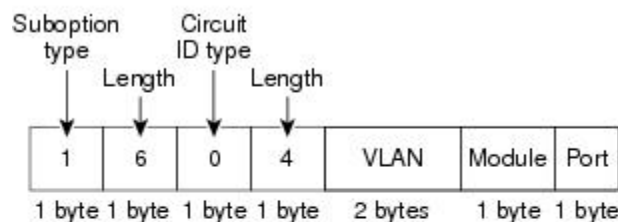
上記の一連のイベントが発生した場合、次の値は変更されません。

- 回線 ID サブオプションフィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - 回線 ID タイプの長さ

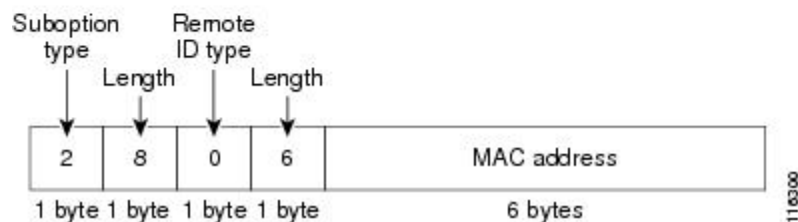
次の図は、リモート ID サブオプションおよび回線 ID サブオプションの packets 形式を示しています。Cisco NX-OS デバイスは、DHCP スヌーピングをグローバルにイネーブルにしたときや、Option 82 データの挿入と削除をイネーブルにしたときにこれらの packets 形式を使用します。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号になります。

図 1: サブオプションの packets 形式

#### Circuit ID Suboption Frame Format



#### Remote ID Suboption Frame Format



## vPC 環境での DHCP スヌーピング

仮想ポートチャネル (vPC) では、2 台の Cisco NX-OS スイッチを 3 番目のスイッチに 1 つの論理ポートチャネルとして認識させることができます。3 番目のスイッチは、スイッチ、サーバ、またはポートチャネルをサポートするその他のネットワークスイッチのいずれかにすることができます。

標準的な vPC 環境では、DHCP 要求は一方の vPC ピア スイッチに到達でき、応答は他方の vPC ピア スイッチに到達できるため、一方のスイッチには部分的な DHCP (IP-MAC) バインディング エントリが生成され、他方のスイッチにはバインディング エントリが生成されません。Cisco NX-OS Release 5.1 から、この問題は Cisco Fabric Service over Ethernet (CFSoE) 分散を使用して、すべての DHCP パケット (要求および応答) が両方のスイッチに確実に認識されるようにすることで対処されます。これにより、vPC リンクの背後に存在するすべてのクライアントについて、両方のスイッチで同じバインディング エントリが作成および管理されるようになります。

CFSoE 分散ではまた、vPC リンク上の DHCP 要求および応答を 1 台のスイッチのみが転送するようにもできます。vPC 以外の環境では、両方のスイッチが DHCP パケットを転送します。

### DHCP スヌーピング バインディング エントリの同期

ダイナミック DHCP バインディング エントリは、次のシナリオで同期される必要があります。

- リモート vPC がオンラインになったとき、その vPC リンクのすべてのバインディング エントリがピアと同期する必要があります。
- DHCP スヌーピングがピア スイッチでイネーブルの場合、リモートでアップ状態であるすべての vPC リンク用のダイナミック バインディング エントリは、ピアと同期する必要があります。

### パケット検証

スイッチは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。次の条件が発生 (この場合パケットは破棄される) しない限り、スイッチでは、DHCP パケットが転送されます。

- 信頼できないインターフェイスで DHCP 応答パケット (DHCPACK、DHCPNAK、または DHCPPOFFER などのパケット) を受信した場合。
- 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。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。

- リレー エージェントの IP アドレス (0.0.0.0 以外) を含む DHCP パケットを受信した場合。

さらに、DHCP パケットの厳密な検証をイネーブルにすることもできます。これにより、DHCP パケットのオプションフィールドが確認されます。これには、オプションフィールドの最初の 4 バイト内の「マジッククッキー」値も含まれます。デフォルトでは、厳密な検証はディセーブルになっています。これを **ip dhcp packet strict-validation** コマンドによりイネーブルにすると、DHCP スヌーピングで無効なオプションフィールドを含むパケットを処理した場合に、パケットがドロップされます。

## DHCP リレー エージェントの概要

### DHCP リレー エージェント

DHCP リレー エージェントを実行するようにデバイスを設定できます。DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCP メッセージを受信すると、新規の DHCP メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイアドレスを設定し (DHCP パケットの **giaddr** フィールド)、パケットにリレー エージェント情報のオプション (Option 82) を追加して (設定されている場合)、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Option 82 をイネーブルにした後に、デバイスは、デフォルトでバイナリ **ifIndex** 形式を使用します。必要に応じて、符号化された文字列形式を使用するように、Option 82 設定を変更できます。



(注) デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態ですべての要求と一緒に転送します。

### DHCP リレー エージェントに対する VRF サポート

DHCP ブロードキャスト メッセージを Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) インスタンスのクライアントから別の VRF の DHCP サーバに転送するように、DHCP リレー エージェントを設定できます。単一の DHCP サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。

DHCP リレー エージェントに対する VRF サポートをイネーブルにするには、DHCP リレー エージェントに対する Option 82 をイネーブルにする必要があります。

DHCP リレー アドレスと VRF 情報を設定したインターフェイスに DHCP 要求が着信した場合、DHCP サーバのアドレスが、別の VRF のメンバであるインターフェイスのネットワークに属する

ものであれば、デバイスは要求に Option 82 情報を挿入し、サーバの VRF の DHCP サーバに転送されます。Option 82 情報は次のとおりです。

#### VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

#### リンクの選択

DHCP 要求を受信するインターフェイスのサブネットアドレス。

#### サーバ識別子オーバーライド

DHCP 要求を受信するインターフェイスの IP アドレス。



(注) DHCP サーバは、VPN 識別子、リンクの選択、サーバ識別子オーバーライドの各オプションをサポートする必要があります。

デバイスは DHCP 応答メッセージを受信すると、Option 82 情報を取り除き、クライアントの VRF の DHCP クライアントに応答を転送します。

## DHCP リレー バインディング データベース

リレー バインディングは、リレー エージェントのアドレスおよびサブネットに、DHCP または BOOTP クライアントを関連付けるエントリです。各リレー バインディングは、クライアントの MAC アドレス、アクティブなリレー エージェント アドレス、アクティブなリレー エージェント アドレス マスク、クライアントが接続されている論理および物理インターフェイス、giaddr リトライ回数、および合計リトライ回数を格納します。giaddr リトライ回数は、リレー エージェント アドレスに送信される要求パケットの数です。合計リトライ回数は、リレー エージェントによって送信される要求パケットの合計数です。1つのリレー バインディング エントリが、各 DHCP または BOOTP クライアントに対して維持されます。



(注) DHCP スマートリレーをグローバルにイネーブルにするか、または任意のスイッチのインターフェイス レベルでイネーブルにする場合、すべてのスイッチのリレー バインディングは vPC ピアと同期する必要があります。

## DHCP スヌーピングの注意事項および制約事項

DHCP スヌーピングを設定する場合は、次の注意事項および制約事項を考慮してください。

- DHCP スヌーピング データベースには 2,000 のバインディングを格納できます。



- DHCP をグローバルにイネーブル化し、さらに少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにするまで、DHCP スヌーピングはアクティブになりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するスイッチが設定され、イネーブルになっていることを確認してください。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL (VACL) が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- デフォルトで、DHCP バインディングは、スイッチの再起動後に永続的に保存されません。スイッチの再起動後も永続的なバインディングを保持するには、**copy rs** コマンドを使用します。**copy rs** コマンドが発行されると、その時点で存在するすべてのバインディングは、スイッチの再起動後も永続的な状態になります。
- vPC リンク内のスイッチ間で DHCP 設定が同期されていることを確認します。同期されていないと、ランタイムエラーが発生し、パケットがドロップされる場合があります。
- リモート DHCP サーバとローカル DHCP サーバの両方を使用するには、DHCP リレー機能を設定し、ローカル DHCP サーバのユニキャストアドレスを定義し、またはローカル DHCP サーバが常駐するサブネットのローカルブロードキャストアドレスを設定する必要があります。DHCP サーバのユニキャストアドレスを定義せず、またはサブネットのローカルブロードキャストアドレスを設定しない場合、ローカル DHCP パケットは配信できません。たとえば、この状況は SVI に IP DHCP アドレスを適用する場合に発生することがあります。

次の注意事項および制約事項は、FabricPath を含む実装に適用されます。

- DHCP スヌーピングは、CE-Fabric 境界スイッチ上でイネーブルにする必要があります。
- アクセスレイヤでネットワークを保護するために、DHCP スヌーピングはすべてのアクセスレイヤスイッチ上でイネーブルになっています。
- DHCP は、FabricPath モードで設定されたポート上のバインディングエントリを学習しません。DHCP スヌーピングは、すべてのアクセスレイヤスイッチで手動でイネーブルにする必要があります。
- ダイナミック ARP インスペクション (DAI) がイネーブルになっている場合、FabricPath ポート上で受信された ARP パケットは許可されます。
- FabricPath モードでは、ポート上で IPSG をイネーブルにすることはできません。
- システムのすべての FabricPath ポートは、信頼できるポートとして設定する必要があります。
- FabricPath の DHCP スヌーピングは、スイッチに設定されたすべての VLAN でイネーブルにする必要があります。スイッチ上のすべての VLAN の FabricPath をイネーブルにしない場合、DHCP がイネーブルにされていない VLAN で DHCP パケットはドロップされます。DHCP パケットがドロップされないようにするには、次の設定すべてを実行する必要があります。

◦ **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにします。

- ° **feature-set fabricpath** および **feature-set fabricpath** コマンドを使用して FabricPath フィーチャセットをインストールします。
- ° **ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにイネーブルにします。
- ° **ip dhcp snooping vlan vlan** コマンドを使用して、スイッチの設定済み VLAN ごとに DHCP スヌーピングをイネーブルにします。

## DHCP スヌーピングのデフォルト設定

次の表に、DHCP スヌーピング パラメータのデフォルト設定を示します。

表 1: DHCP スヌーピング パラメータのデフォルト値

パラメータ	デフォルト
DHCP スヌーピング機能	ディセーブル
DHCP スヌーピングのグローバルなイネーブル化	No
DHCP スヌーピング VLAN	なし
DHCP スヌーピングの Option 82 サポート	ディセーブル
DHCP スヌーピング信頼状態	信頼できない

## DHCP スヌーピングの設定

### DHCP スヌーピングの最小設定

手順

	コマンドまたはアクション	目的
ステップ 1	DHCP スヌーピング機能をイネーブルにします。	DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングを設定できません。 詳細については、 <a href="#">DHCP スヌーピング機能のイネーブル化またはディセーブル化</a> 、(11 ページ)を参照してください。

	コマンドまたはアクション	目的
ステップ 2	DHCP スヌーピングをグローバルにイネーブル化します。	詳細については、 <a href="#">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</a> 、(12 ページ) を参照してください。
ステップ 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。 詳細については、 <a href="#">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</a> 、(13 ページ) を参照してください。
ステップ 4	DHCP サーバとスイッチが、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。	詳細については、 <a href="#">インターフェイスの信頼状態の設定</a> 、(15 ページ) を参照してください。

## DHCP スヌーピング機能のイネーブル化またはディセーブル化

スイッチの DHCP スヌーピング機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP スヌーピングはディセーブルです。

### はじめる前に

DHCP スヌーピング機能をディセーブルにすると、DHCP スヌーピングの設定がすべて消去されます。DHCP スヌーピングをオフにして DHCP スヌーピングの設定を維持したい場合は、DHCP をグローバルにディセーブル化します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	<b>[no] feature dhcp</b>  例： switch(config)# feature dhcp	DHCP スヌーピング機能をイネーブルにします。 <b>no</b> オプションを使用すると、DHCP スヌーピング機能がディセーブルになり、DHCP スヌーピングの設定がすべて消去されます。

	コマンドまたはアクション	目的
ステップ 3	<b>show running-config dhcp</b>  例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 4	<b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	(任意) 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。

## 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

スイッチに対して DHCP スヌーピング機能のグローバルなイネーブル化またはディセーブル化が可能です。DHCP スヌーピングをグローバルにディセーブルにすると、DHCP スヌーピングの実行や DHCP メッセージのリレーはスイッチで停止されますが、DHCP スヌーピングの設定は維持されます。

### はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	<b>[no] ip dhcp snooping</b>  例： switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブル化します。 <b>no</b> 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。
ステップ 3	<b>show running-config dhcp</b>  例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	<b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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。

## 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

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。

### はじめる前に

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。

DHCP スヌーピングがイネーブルになっていることを確認してください。



(注) DHCP スヌーピングを使用して設定を行っている VLAN で VACL が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例 : <pre>switch# config t 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	<b>[no] ip dhcp snooping vlan <i>vlan-list</i></b>  例 : <pre>switch(config)# ip dhcp snooping vlan 100,200,250-252</pre>	<i>vlan-list</i> で指定する VLAN の DHCP スヌーピングをイネーブルにします。 <b>no</b> 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 3	<b>show running-config dhcp</b>  例 : <pre>switch(config)# show running-config dhcp</pre>	(任意) DHCP スヌーピングの設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	<b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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。

## Option 82 データの挿入および削除のイネーブル化またはディセーブル化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除をイネーブルまたはディセーブルに設定できます。

### はじめる前に

デフォルトでは、スイッチは DHCP パケットに Option 82 情報を挿入しません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例 : <pre>switch# config t 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	<b>[no] ip dhcp snooping information option</b>  例 : <pre>switch(config)# ip dhcp snooping information option</pre>	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。 <b>no</b> オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	<b>show running-config dhcp</b>  例 : <pre>switch(config)# show running-config dhcp</pre>	DHCP スヌーピングの設定を表示します。
ステップ 4	<b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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。

## DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP スヌーピング機能では、DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	<b>[no] ip dhcp packet strict-validation</b>  例： switch(config)# ip dhcp packet strict-validation	DHCP スヌーピング機能で、DHCP パケットの厳密な検証をイネーブルにします。 <b>no</b> オプションを使用すると、DHCP パケットの厳密な検証がディセーブルになります。
ステップ 3	<b>show running-config dhcp</b>  例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 4	<b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	(任意) 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。

## インターフェイスの信頼状態の設定

各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かどうかを設定できます。DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

### はじめる前に

デフォルトでは、すべてのインターフェイスは信頼できません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	次のいずれかのコマンドを入力します。  • <b>interface ethernet port/slot</b>  • <b>interface port-channel channel-number</b>  例： switch(config)# interface ethernet 2/1 switch(config-if)#	<ul style="list-style-type: none"> <li>• 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。<i>port/slot</i>は、DHCP スヌーピングで <i>trusted</i> または <i>untrusted</i> に設定するレイヤ 2 イーサネット インターフェイスです。</li> <li>• 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。<i>port/slot</i>は、DHCP スヌーピングで <i>trusted</i> または <i>untrusted</i> に設定するレイヤ 2 ポートチャネル インターフェイスです。</li> </ul>
ステップ 3	<b>[no] ip dhcp snooping trust</b>  例： switch(config-if)# 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。 <b>no</b> 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。
ステップ 4	<b>show running-config dhcp</b>  例： switch(config-if)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 5	<b>copy running-config startup-config</b>  例： switch(config-if)# copy running-config startup-config	(任意) 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。

## DHCP リレー エージェントのイネーブル化またはディセーブル化

DHCP リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP リレー エージェントはイネーブルです。

## はじめる前に

DHCP 機能がイネーブルであることを確認します。



## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	<b>[no] ip dhcp relay</b>  例： switch(config)# ip dhcp relay	DHCP リレーエージェントをイネーブルにします。 <b>no</b> オプションを使用すると、DHCP リレーエージェントがディセーブルになります。
ステップ 3	<b>show ip dhcp relay</b>  例： switch(config)# show ip dhcp relay	(任意) DHCP リレーの設定を表示します。
ステップ 4	<b>show running-config dhcp</b>  例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 5	<b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	(任意) 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。

## DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除をイネーブルまたはディセーブルに設定できます。

デフォルトでは、DHCP リレー エージェントは DHCP パケットに Option 82 情報を挿入しません。

### はじめる前に

DHCP 機能がイネーブルであることを確認します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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] <b>ip dhcp relay information option</b>	DHCP リレーエージェントによって転送されるパケットに対する Option 82 情報の挿入および削除をイネーブルにします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。no オプションを使用すると、この動作がディセーブルになります。
ステップ 3	switch(config)# <b>ip dhcp relay information sub-option circuit-id format-type string</b>	(任意) デフォルトの ifIndex バイナリ形式の代わりに符号化されたストリング形式を使用するように、オプション 82 を設定します。
ステップ 4	switch(config)# <b>show ip dhcp relay</b>	(任意) DHCP リレーの設定を表示します。
ステップ 5	switch(config)# <b>show running-config dhcp</b>	(任意) DHCP 設定を表示します。
ステップ 6	switch(config)# <b>copy running-config startup-config</b>	(任意) リポ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。

## DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF の DHCP サーバにリレーする機能をサポートするように、デバイスを設定できます。

### はじめる前に

DHCP リレー エージェントの Option 82 をイネーブルに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	<b>config t</b>  例： switch# config t 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	<b>[no] ip dhcp relay information option vpn</b>  例： switch(config)# ip dhcp relay information option vpn	DHCP リレー エージェントに対して VRF サポートをイネーブルにします。 <b>no</b> オプションを使用すると、この動作がディセーブルになります。
ステップ 3	<b>[no] ip dhcp relay sub-option type cisco</b>  例： switch(config)# ip dhcp relay sub-option type cisco	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェント Option 82 サブオプションを設定する場合は、DHCP をイネーブルにして、シスコ独自の番号である 150、152、および 151 を使用します。 <b>no</b> オプションを使用すると、DHCP では、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID サブオプションに対して、RFC 番号 5、11、151 が使用されるようになります。
ステップ 4	<b>show ip dhcp relay</b>  例： switch(config)# show ip dhcp relay	(任意) DHCP リレーの設定を表示します。
ステップ 5	<b>show running-config dhcp</b>  例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 6	<b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	(任意) 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。

## レイヤ3 インターフェイスの DHCP リレー エージェントに対するサブ ネット ブロードキャスト サポートのイネーブル化またはディセー ブル化

クライアントからのサブネットのブロードキャスト IP アドレスに DHCP パケットのリレーをサポートするように、デバイスを設定できます。この機能がイネーブルの場合、VLANACL (VACL) は、IPブロードキャストパケット、すべてのサブネットブロードキャスト（プライマリサブネットブロードキャストおよびセカンダリ サブネットブロードキャスト）パケットを許容します。

### はじめる前に

DHCP 機能がイネーブルであることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例： switch# config t 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	<b>interface interface slot/port</b>  例： switch(config)# interface ethernet 2/2 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。slot/port は、DHCP リレーエージェントに対するサブネットブロードキャストサポートをイネーブルまたはディセーブルにするインターフェイスです。
ステップ 3	<b>[no] ip dhcp relay subnet-broadcast</b>  例： switch(config-if)# ip dhcp relay subnet-broadcast	DHCP リレー エージェントに対するサブネットブロードキャストサポートをイネーブルにします。no オプションを使用すると、この動作がディセーブルになります。
ステップ 4	<b>exit</b>  例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーションモードを終了します。
ステップ 5	<b>exit</b>  例： switch(config)# exit switch#	グローバルコンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
ステップ 6	<b>show ip dhcp relay</b>  例 : switch# show ip dhcp relay	(任意) DHCP リレーの設定を表示します。
ステップ 7	<b>show running-config dhcp</b>  例 : switch# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 8	<b>copy running-config startup-config</b>  例 : switch# copy running-config startup-config	(任意) 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。

## DHCP スタティック バインディングの作成

レイヤ 2 インターフェイスにスタティック DHCP ソース バインディングを作成できます。

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>  例 : switch# config t 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	<b>ip source binding IP-address MAC-address vlan vlan-id {interface ethernet slot/port   port-channel channel-no}</b>  例 : switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3	レイヤ 2 イーサネット インターフェイスにスタティックな送信元アドレスをバインドします。

	コマンドまたはアクション	目的
ステップ 3	<b>show ip dhcp snooping binding</b>  例： switch(config)# ip dhcp snooping binding	(任意) DHCP スヌーピングのスタティックおよびダイナミックバインディングを示します。
ステップ 4	<b>show ip dhcp snooping binding dynamic</b>  例： switch(config)# ip dhcp snooping binding dynamic	(任意) DHCP スヌーピングのダイナミックバインディングを示します。
ステップ 5	<b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	(任意) 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、イーサネットインターフェイス 2/3 上に、VLAN 100 に関連付ける固定 IP ソースエントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

## DHCP スヌーピング設定の確認

DHCP スヌーピング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。これらのコマンドの出力フィールドの詳細については、ご使用の Cisco Nexus デバイスの『*System Management Configuration Guide*』を参照してください。

コマンド	目的
<b>show running-config dhcp</b>	DHCP スヌーピング設定を表示します。
<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。

## DHCP バインディングの表示

DHCP スタティックおよびダイナミックバインディングテーブルを表示するには、**show ip dhcp snooping binding** コマンドを使用します。DHCP ダイナミックバインディングテーブルを表示するには、**show ip dhcp snooping binding dynamic** を使用します。

このコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『*System Management Configuration Guide*』を参照してください。

次に、スタティック DHCP バインディングを作成してから、**show ip dhcp snooping binding** コマンドを使用してバインディングを確認する例を示します。

```
switch# configuration terminal
switch(config)# ip source binding 10.20.30.40 0000.1111.2222 vlan 400 interface port-channel
500

switch(config)# show ip dhcp snooping binding
-----
MacAddress      IpAddress      LeaseSec      Type          VLAN      Interface
-----
00:00:11:11:22:22  10.20.30.40    infinite      static        400      port-channel500
```

## DHCP スヌーピング バインディング データベースのクリア

DHCP スヌーピング バインディング データベースからエントリを削除できます。1つのエントリ、インターフェイスに関連するすべてのエントリ、データベース内のすべてのエントリなどを削除することが可能です。

### はじめる前に

DHCP スヌーピングがイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>clear ip dhcp snooping binding</b>  例： switch# clear ip dhcp snooping binding	(任意) DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	<b>clear ip dhcp snooping binding interface ethernet slot/port[.subinterface-number]</b>  例： switch# clear ip dhcp snooping binding interface ethernet 1/4	(任意) DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	<b>clear ip dhcp snooping binding interface port-channel channel-number[.subchannel-number]</b>  例： switch# clear ip dhcp snooping binding interface port-channel 72	(任意) DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。

	コマンドまたはアクション	目的
ステップ 4	<pre>clear ip dhcp snooping binding vlan <i>vlan-id</i> mac <i>mac-address</i> ip <i>ip-address</i> interface {ethernet <i>slot/port</i>[<i>.subinterface-number</i>   port-channel channel-number[<i>.subchannel-number</i>] }</pre> <p>例 :</p> <pre>switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11</pre>	<p>(任意)</p> <p>DHCP スヌーピング バインディング データベースから、特定のエントリをクリアします。</p>
ステップ 5	<pre>show ip dhcp snooping binding</pre> <p>例 :</p> <pre>switch# show ip dhcp snooping binding</pre>	<p>(任意)</p> <p>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。</p>

## DHCP スヌーピングの設定例

次に、2つの VLAN 上で DHCP スヌーピングをイネーブルにして、Option 82 サポートをイネーブルにし、さらに DHCP サーバがイーサネット インターフェイス 2/5 に接続されているためにその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例を示します。

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```