



## DHCP 機能の設定

この章では、Catalyst 2960 スイッチで DHCP スヌーピングと Option 82 データ挿入機能を設定する方法について説明します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』の「DHCP Commands」を参照してください。このコマンドリファレンスには、Cisco.com ホームページ ([Documentation > Cisco IOS Software > 12.2 Mainline > Command References](#)) からアクセスできます。

この章で説明する内容は、次のとおりです。

- 「DHCP 機能の概要」(P.19-1)
- 「DHCP 機能の設定」(P.19-7)
- 「DHCP スヌーピング情報の表示」(P.19-12)

## DHCP 機能の概要

DHCP は、中央のサーバからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。DHCP では、ネットワークに接続されたホストだけが IP アドレスを使用し、IP アドレスを永続的にホストに割り当てる必要がなくなるため、限られた IP アドレス空間を節約できます。

ここでは、次の情報について説明します。

- 「DHCP サーバ」(P.19-2)
- 「DHCP リレー エージェント」(P.19-2)
- 「DHCP スヌーピング」(P.19-2)
- 「Option 82 データ挿入」(P.19-3)
- 「DHCP スヌーピング バインディング データベース」(P.19-5)

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「*IP Addressing and Services*」にある「*Configuring DHCP*」を参照してください。このガイドには、Cisco.com ホームページ ([Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides](#)) からアクセスできます。

## DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。

## DHCP リレー エージェント

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 パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

## DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと 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 バインディング テーブルとも呼ばれる) の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。このデータベースの詳細については、「[DHCP スヌーピング情報の表示](#)」(P.19-12) を参照してください。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンド ユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。



(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。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外側から送信されたメッセージのことです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク上にないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信頼できないインターフェイスとなります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合 (デフォルト)、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットを廃棄します。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットを廃棄します。

- DHCP OFFER パケット、DHCP ACK パケット、DHCP NAK パケット、DHCP LEASE QUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCP RELEASE または DHCP DECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スイッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットを廃棄します。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入された Option 82 情報を含むパケットを受け入れません。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジ スイッチとの接続ポートは、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。

## Option 82 データ挿入

住宅地域にあるメトロポリタンイーサネット アクセス環境では、DHCP により、多数の加入者の IP アドレス割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。加入者 LAN 上の複数のホストをアクセス スイッチの同一ポートに接続でき、これらは一意に識別されます。

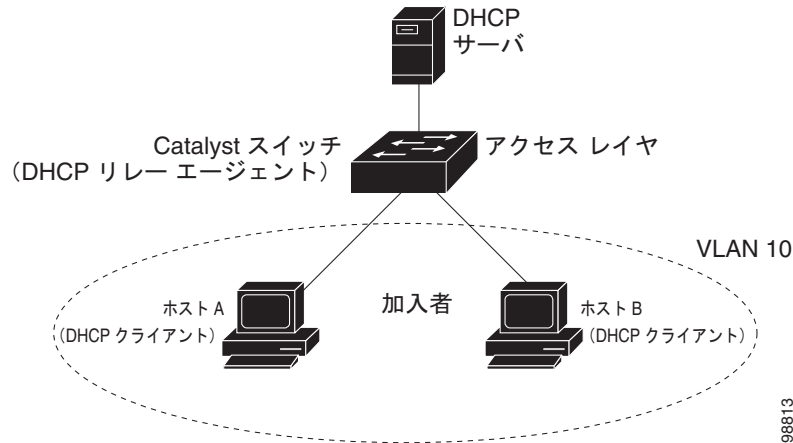


(注)

DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、この機能を使用する加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 19-1 に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタンイーサネット ネットワークの例を示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント (Catalyst スイッチ) にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 19-1 メトロポリタンイーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、以下のイベントがこの順序で発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、ネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。リモート ID サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションはパケットを受信したポートの識別子 `vlan-mod-port` です。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバがこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、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 に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に、DHCP サーバは DHCP 応答内に Option 82 フィールドをエコーします。
- 要求がスイッチによってサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

この一連のイベントが発生する間、図 19-2 に示す以下のフィールド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

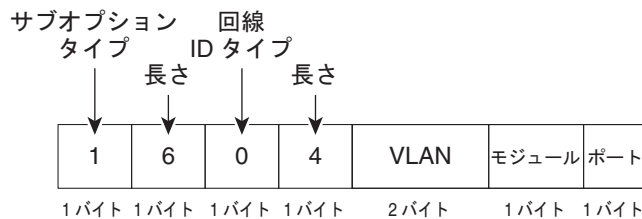
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、24 個の 10/100 ポートと Small Form-Factor Pluggable (SFP) モジュール スロットを備えたスイッチでは、ポート 3 がファストイーサネット 0/1 ポート、ポート 4 がファストイーサネット 0/2 ポートなどとなります。さらに、ポート 27 は SFP モジュール スロット 0/1 などとなります。

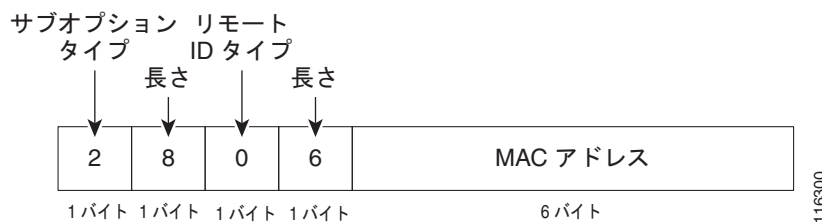
図 19-2 は、リモート ID サブオプションおよび回線 ID サブオプションの packets 形式を示します。スイッチがこれらの packets 形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、`ip dhcp snooping information option` グローバル コンフィギュレーション コマンドを入力した場合です。

図 19-2 サブオプションの packets 形式

### 回線 ID サブオプション フレーム フォーマット



### リモート 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 バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。このデータベースには最大 8192 のバインディングを保存できます。

各データベース エントリ (バインディング) は、IP アドレス、それに関連付けられた MAC アドレス、リース期間 (16 進形式)、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、直ちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。以下のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スwitchがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できる インターフェイスである。

# DHCP 機能の設定

ここでは、次の設定情報について説明します。

- 「DHCP のデフォルト設定」 (P.19-7)
- 「DHCP スヌーピング設定時の注意事項」 (P.19-7)
- 「DHCP リレー エージェントの設定」 (P.19-9)
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」 (P.19-9)
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」 (P.19-11)

## DHCP のデフォルト設定

表 19-1 に、DHCP のデフォルト設定を示します。

表 19-1 DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。 <sup>1</sup>
DHCP リレー エージェント	イネーブル。 <sup>2</sup>
DHCP パケット転送アドレス	未設定。
リレー エージェント情報の確認	イネーブル (無効なメッセージは廃棄)。 <sup>2</sup>
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。 <sup>2</sup>
DHCP スヌーピングをグローバルにイネーブル	ディセーブル。
DHCP スヌーピング情報オプション	イネーブル。
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション <sup>3</sup>	ディセーブル。
DHCP スヌーピング レート制限	未設定。
DHCP スヌーピング信頼状態	untrusted。
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 バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
3. この機能は、スイッチがエッジスイッチによって Option 82 が挿入されたパケットを受信する集約スイッチである場合に使用します。

## DHCP スヌーピング設定時の注意事項

ここでは、DHCP の設定時の注意事項を説明します。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN で DHCP スヌーピングがイネーブルになるまで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デバイスが設定され、イネーブルになっていることを確認してください。
- 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と、スヌーピングをディセーブルにするまで以下の Cisco IOS コマンドは使用できません。これらのコマンドを入力すると、スイッチがエラー メッセージを返し、設定は適用されません。
  - **ip dhcp relay information check** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information policy** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trust-all** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trusted** インターフェイス コンフィギュレーション コマンド
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルである場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- DHCP スヌーピング バインディング データベースを設定するときには、次の注意事項に従ってください。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することをお勧めします。
  - ネットワーク ベースの URL (TFTP や FTP など) については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、NTP をイネーブルにし、設定することをお勧めします。詳細については、「[NTP の設定](#)」(P.6-3) を参照してください。
  - NTP を設定した場合、スイッチは、スイッチのシステム クロックが NTP と同期したときにだけバインディングの変更をバインディング ファイルに書き込みます。
- 信頼できないデバイスが接続された集約スイッチでは、**ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスが偽装した Option 82 情報を提供する可能性があります。
- Cisco IOS Release 12.2(37)SE から、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。



## DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>service dhcp</code>	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。この機能はデフォルトでイネーブルです。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP サーバおよび DHCP リレー エージェントをディセーブルにするには、`no service dhcp` グローバル コンフィギュレーション コマンドを使用します。

以下の手順については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」にある「Configuring DHCP」を参照してください。このガイドには、Cisco.com ホームページ ([Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides](#)) からアクセスできます。

- リレー エージェント情報のチェック (検証)
- リレー エージェント転送ポリシーの設定

## DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip dhcp snooping</code>	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	<code>ip dhcp snooping vlan <i>vlan-range</i></code>	1 つの VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ~ 4094 です。  VLAN ID 番号で示される 1 つの VLAN ID、カンマで区切られた一連の VLAN ID、ハイフンで区切られた VLAN ID の範囲、またはスペースで区切られた開始 VLAN ID と終了 VLAN ID で示される VLAN ID の範囲を指定できます。
ステップ 4	<code>ip dhcp snooping information option</code>	スイッチが DHCP サーバへの DHCP 要求メッセージにおいて DHCP リレー情報 (Option 82 フィールド) を挿入および削除できるようにします。これがデフォルトの設定です。

	コマンド	目的
ステップ 5	<b>ip dhcp snooping information option allow-untrusted</b>	(任意) スイッチがエッジスイッチに接続された集約スイッチである場合、スイッチがエッジスイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを受け入れるようにします。 デフォルト設定はディセーブルです。 <b>(注)</b> このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ 6	<b>interface interface-id</b>	設定するインターフェイスを指定し、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 7	<b>ip dhcp snooping trust</b>	(任意) インターフェイスを信頼できるインターフェイスまたは信頼できないインターフェイスとして設定します。 <b>no</b> キーワードを使用すると、信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定できます。デフォルト設定は <b>untrusted</b> です。
ステップ 8	<b>ip dhcp snooping limit rate rate</b>	(任意) インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは、レート制限は設定されません。 <b>(注)</b> 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することをお勧めします。信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングがイネーブルである複数の VLAN に割り当てられたトランクポートでは、レート制限の値を大きくすることが必要になることがあります。
ステップ 9	<b>exit</b>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	<b>ip dhcp snooping verify mac-address</b>	(任意) 信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 11	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 12	<b>show running-config</b>	設定を確認します。
ステップ 13	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。1 つの VLAN または VLAN の範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan vlan-range** グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジスイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを廃棄するように集約スイッチを設定するには、**no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを使用します。

次に、DHCP スヌーピングをグローバルおよび VLAN 10 でイネーブルにし、ポートのレート制限を 1 秒あたり 100 パケットに設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

## Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにし、設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring DHCP」にある「DHCP Configuration Task List」を参照してください。このガイドには、Cisco.com ホームページ ([Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides](#)) からアクセスできます。

## DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip dhcp snooping database {flash:/filename   ftp://user:password@host/filename   http://[[username:password]@]{hostname   host-ip}[/directory] /image-name.tar   rtp://user@host/filename} tftp://host/filename</code>	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 <ul style="list-style-type: none"> <li>• <code>flash:/filename</code></li> <li>• <code>ftp://user:password@host/filename</code></li> <li>• <code>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</code></li> <li>• <code>rtp://user@host/filename</code></li> <li>• <code>tftp://host/filename</code></li> </ul>
ステップ 3	<code>ip dhcp snooping database timeout seconds</code>	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。  デフォルト値は 300 秒です。指定できる範囲は 0 ~ 86400 です。無限の時間を定義し、転送の試行を無期限に続けるには、0 を使用します。
ステップ 4	<code>ip dhcp snooping database write-delay seconds</code>	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ~ 86400 秒です。デフォルト値は 300 秒（5 分）です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</code>	(任意) DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。vlan-id の範囲は 1 ~ 4904 です。seconds の範囲は 1 ~ 4294967295 です。  このコマンドは、追加するエントリごとに入力します。  (注) このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 7	<code>show ip dhcp snooping database [detail]</code>	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウトまたは遅延時間の値をリセットするには、**ip dhcp snooping database timeout seconds** または **ip dhcp snooping database write-delay seconds** グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアするには、**clear ip dhcp snooping database statistics** 特権 EXEC コマンドを使用します。データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからバインディング エントリを削除するには、**no ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id** 特権 EXEC コマンドを使用します。このコマンドは、削除するエントリごとに入力します。

## DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 19-2 に示す特権 EXEC コマンドを使用します。

表 19-2 DHCP 情報を表示するためのコマンド

コマンド	目的
<b>show ip dhcp snooping</b>	スイッチの DHCP スヌーピング設定を表示します。
<b>show ip dhcp snooping binding</b>	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
<b>show ip dhcp snooping database</b>	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
<b>show ip dhcp snooping statistics</b>	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。



(注)

DHCP スヌーピングがイネーブルであり、インターフェイスがダウン ステートに変わった場合、スイッチは静的に設定されたバインディングを削除しません。