



## DHCP 機能の設定

---

この章では、Catalyst 2960 スイッチ上で Dynamic Host Configuration Protocol (DHCP; ダイナミックホスト コンフィギュレーション プロトコル) スヌーピングおよび 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。

---

この章で説明する内容は、次のとおりです。

- [DHCP 機能の概要 \(p.19-2\)](#)
- [DHCP 機能の設定 \(p.19-8\)](#)
- [DHCP スヌーピング情報の表示 \(p.19-14\)](#)

## DHCP 機能の概要

DHCP は、中央集中型サーバからホスト IP アドレスを動的に割り当てるために LAN 環境で幅広く使用されており、これにより IP アドレスの管理のオーバーヘッドを著しく軽減できます。DHCP は、制限のある IP アドレス空間の節約にもなります。IP アドレスをホストに永続的に割り当てる必要がなく、IP アドレスを使用するのはネットワークに接続されているホストだけになるからです。

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 \(p.19-4\)](#)
- [DHCP スヌーピング バインディング データベース \(p.19-6\)](#)

DHCP クライアントに関する詳細については、『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。

## DHCP サーバ

DHCP サーバは、スイッチまたはルータ上にある特定のアドレス プールから IP アドレスを DHCP クライアントに割り当て、管理します。DHCP サーバが DHCP クライアントによって要求された設定パラメータを、データベースから提供できない場合、その要求は、ネットワーク管理者によって定義された 1 つまたは複数のセカンダリ DHCP サーバへ転送されます。

## 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 の装置です。各リレー エージェントは、同一の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 エージェントの転送方法は、通常のレイヤ 2 の転送方法 (IP データグラムがネットワーク間でトランスペアレントにスイッチングされる) とは異なります。リレー エージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して出力インターフェイスから送信します。

## DHCP スヌーピング

DHCP スヌーピングとは、untrusted(信頼性のない)DHCP メッセージをフィルタリングして、DHCP スヌーピング バインディング データベース (別名 DHCP スヌーピング バインディング テーブル) を作成、維持することにより、ネットワークにセキュリティを提供する DHCP セキュリティ機能です。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.19-14) を参照してください。

DHCP スヌーピングは、untrusted ホストと DHCP サーバの間でファイアウォールのような機能を果たします。DHCP スヌーピングを使用すると、エンドユーザに接続された untrusted インターフェイスと、DHCP サーバや別のスイッチと接続された trusted インターフェイスを区別できます。



(注)

DHCP スヌーピングを適切に機能させるには、すべての DHCP サーバを trusted インターフェイスを介してスイッチと接続する必要があります。

untrusted 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部から受信したメッセージです。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と、untrusted メッセージがサービス プロバイダー ネットワーク外の装置（お客様のスイッチなど）から送信されます。不明な装置からのメッセージは、トラフィック攻撃の原因となる可能性があるため untrusted となります。

DHCP スヌーピング バインディング データベースには、MAC（メディア アクセス制御）アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN（仮想 LAN）番号、スイッチの untrusted インターフェイスに対応したインターフェイス情報が登録されています。ただし、trusted インターフェイスに相互接続されたホストに関する情報は含まれていません。

サービス プロバイダー ネットワーク内において、trusted インターフェイスは同一ネットワーク内の装置上のポートに接続されています。untrusted インターフェイスは、ネットワーク内の untrusted インターフェイスまたはネットワーク外のデバイス上のインターフェイスに対して接続されています。

スイッチは untrusted インターフェイス上でパケットを受信した場合、そのインターフェイスが DHCP スヌーピングを有効にした VLAN に属していれば、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）、スイッチはそのパケットを転送します。アドレスが一致しなかった場合、スイッチはそのパケットを廃棄します。

次の状況が発生すると、スイッチは DHCP パケットを廃棄します。

- DHCP OFFER、DHCP ACK、DHCP NAK、または DHCP REQUEST パケットなど、DHCP サーバからのパケットを、ネットワークまたはファイアウォールの外部から受信した場合。
- パケットが untrusted インターフェイスで受信され、送信元 MAC アドレスおよび 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。
- DHCP スヌーピング バインディング データベースに MAC アドレスを持つ DHCP RELEASE または DHCP DECLINE ブロードキャスト メッセージをスイッチが受信したが、バインディング データベース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のものと一致しない場合。
- DHCP リレー エージェントが、リレーエージェント IP アドレス（0.0.0.0 以外）を含む DHCP パケットを転送する場合。またはリレー エージェントが、Option 82 情報を含むパケットを untrusted ポートへ転送する場合。

スイッチが DHCP スヌーピングをサポートする集約スイッチで、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場合、パケットが untrusted インターフェイスで受信されると、スイッチは Option 82 情報を持ったパケットを廃棄します。DHCP スヌーピングがイネーブルでパケットが trusted ポートで受信される場合、集約スイッチは接続されている装置の DHCP スヌーピング バインディングを学習しないので、完全な DHCP スヌーピング バインディング データベースを構築できません。

untrusted インターフェイスを介して集約スイッチをエッジスイッチに接続している場合、`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ことで、集約スイッチは Option 82 情報を持ったパケットをエッジスイッチから受信できます。集約スイッチは untrusted 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学習します。スイッチが Option 82 情報を持ったパケットを、ホストが接続された untrusted 入力インターフェイス上で受信する間、集約スイッチ上で DHCP のセキュリティ機能をイネーブルにできます。集約スイッチに接続されているエッジスイッチ上のポートは、trusted 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

住宅地のメトロポリタンイーサネットアクセス環境では、DHCP を使用して、多数の加入者への IP アドレスの割り当てを集中管理できます。スイッチ上で DHCP Option 82 機能がイネーブルの場合、(MAC アドレスのほかにも)ネットワークに接続されたスイッチポートにより加入する装置を識別できます。同じアクセススイッチに接続されている加入者 LAN の複数のホストを、一意に識別できます。

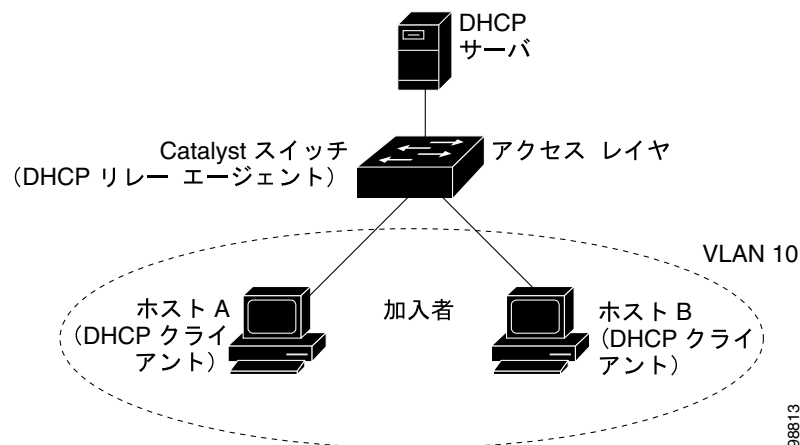


(注)

DHCP Option 82 機能は、DHCP スヌーピングがグローバルおよび VLAN 上でイネーブルで、この機能を使用している加入装置が VLAN に割り当てられている場合のみ、サポートされます。

図 19-1 に、アクセスレイヤでスイッチに接続されている加入者に中央集中型 DHCP サーバが 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、それに関連付けられた DHCP サーバが、同じ IP ネットワークまたは同じサブネットに属していないため、DHCP リレー エージェント (Catalyst スイッチ) には、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の間の DHCP メッセージの転送を行うヘルパー アドレスが設定されています。

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



スイッチの DHCP スヌーピング情報 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。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、ネットワークへブロードキャストします。
- スイッチは DHCP 要求を受信すると、パケットに Option 82 情報を追加します。Option 82 情報は、スイッチの MAC アドレス (リモート ID サブオプション)、ポート ID、パケットの受信側である `vlan-mod-port` (回線 ID サブオプション) 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 パケット内に追加します。
- スイッチは、Option 82 フィールドを格納した DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。サーバが Option 82 に対応している場合、リモート ID または回線 ID、あるいはその両方を使用して IP アドレスを割り当て、単一のリモート ID または回線 ID に割り当てる IP アドレス数を制限するなどのポリシーを実行します。その後、DHCP サーバは、DHCP の応答内に Option 82 フィールドをエコーします。

- スイッチにより要求が DHCP サーバにリレーされると、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、あるいは回線 ID フィールドを検査して、スイッチ自身が Option 82 データを挿入したことを確認します。スイッチは、Option 82 フィールドを削除し、そのパケットを DHCP 要求の送信元である DHCP クライアントに接続されたスイッチ ポートに転送します。

前述のイベントが発生したとき、[図 19-2](#) の次のフィールドの値は変化しません。

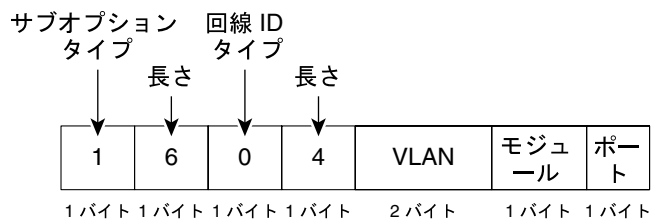
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポートフィールドでは、ポート番号が 3 から始まります。たとえば 24 個の 10/100/1000 ポートおよび Small Form-Factor Pluggable (SFP) モジュール スロットを搭載したスイッチの場合、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、というようになり、以降同様に続きます。ポート 27 は SFP モジュール スロット 0/1 となり、以降同様に続きます。

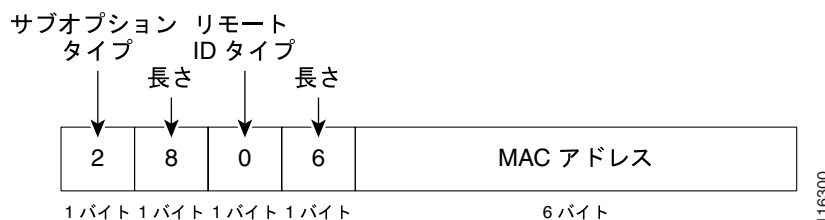
[図 19-2](#) に、リモート ID のサブオプションおよび回線 ID のサブオプションに対応したパケットフォーマットを示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで、さらに `ip dhcp snooping information option` グローバル コンフィギュレーション コマンドが入力された場合、このパケットフォーマットを使用します。

図 19-2 サブオプションのパケットフォーマット

回線 ID のサブオプション フレームフォーマット



リモート ID のサブオプション 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 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 untrusted インターフェイスに関する情報を保存します。データベースに保存できるバインディングは、最大 8192 個です。

各データベース エントリ (バインディング) の内容は、IP アドレス、関連する MAC アドレス、リース時間 (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、インターフェイスが属する VLAN です。データベース エージェントは、設定した保存場所にあるファイルにバインディングを保存します。各エントリの最後に、ファイルの最初からエントリの最後までのもすべてのバイトを管理するチェックサムが登録されます。各エントリは 72 バイトで、そのあとに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時にバインディングの情報が消えないようにするには、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。エージェントがディセーブルになっていて DHCP スヌーピングだけがイネーブルになっている場合、スイッチの接続は切れませんが、DHCP スヌーピングが DHCP スプーフィング攻撃を防止できないことがあります。

スイッチは、リロード時にバインディング ファイルを読み込んで 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。データベースが変更されると、スイッチは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学習したとき、またはバインディングが消失したとき、ただちにデータベースのエントリを更新します。バインディング ファイルのエントリも更新します。ファイルの更新間隔は、設定可能な遅延によって決まり、更新はバッチ処理されます。指定した時間 (write-delay および abort-timeout 値で設定) の間にファイルが更新されないと、更新は停止します。

バインディングを記述したファイルのフォーマットは、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
```

ファイルの各エントリには、チェックサム値のタグが付いています。これは、スイッチがファイルを読み込むときにエントリを検証するためのものです。最初の行の *initial-checksum* エントリは、ファイルの最終更新に関連するエントリと、ファイルの以前の更新に関連するエントリを区別するためのものです。

次に、バインディング ファイルの一例を示します。

```
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
```

スイッチの起動時に、計算したチェックサム値と保存されているチェックサム値が等しければ、スイッチはバインディング ファイルからエントリを読み込み、それらのバインディングを 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。次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がエントリを読み込んだときに、計算したチェックサム値と保存されているチェックサム値が等しくない場合。エントリとそれに続く内容は無視されます。
- エントリのリース時間が時間切れになっている場合（リース時間が時間切れになったときにスイッチによってバインディング エントリが削除されなかった可能性があります）。
- エントリのインターフェイスがすでにシステム上に存在しなくなっている場合。
- インターフェイスが、ルーティングされたインターフェイス、または DHCP スヌーピングの trusted インターフェイスである場合。

## 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.19-8)
- DHCP スヌーピング設定時の注意事項 (p.19-9)
- DHCP リレー エージェントの設定 (p.19-10)
- DHCP スヌーピングおよび Option 82 のイネーブル化 (p.19-10)
- 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.19-12)

### 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 ソフトウェアでイネーブルにされず (設定が必要です)。
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されます。) <sup>2</sup>
DHCP リレー エージェントの転送ポリシー	既存のリレー エージェント情報を置き換えます <sup>2</sup> 。
DHCP スヌーピングをグローバルでイネーブルにする	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
untrusted 入力インターフェイスの packets を受信する DHCP スヌーピング オプション <sup>3</sup>	ディセーブル
DHCP スヌーピングの制限レート	未設定
DHCP スヌーピングの信頼性	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 ソフトウェアでイネーブルにされず (設定が必要です)。この機能は、送信先が設定されている場合のみ利用できます。

1. スイッチは、DHCP サーバとして設定されている場合のみ、DHCP 要求に応答します。
2. DHCP サーバの IP アドレスが、DHCP クライアントの Switched Virtual Interface (SVI) 上で設定されている場合のみ、スイッチは DHCP パケットをリレーします。
3. スイッチが、エッジスイッチから Option 82 情報を持っ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 スヌーピングの設定時の注意事項について説明します。

- スイッチの DHCP スヌーピングは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 上で 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。
- DHCP スヌーピングをスイッチ上でグローバルにイネーブルにする前に、DHCP サーバとして動作する装置および DHCP リレー エージェントが設定されてイネーブルであ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 Cisco IOS コマンドは使用できません。次のコマンドを入力しても、スイッチからはエラー メッセージが返され、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
- DHCP スヌーピング情報オプションをスイッチ上で設定する前に、DHCP サーバとして機能させる装置を設定してください。たとえば、DHCP サーバによる割り当てまたは除外の対象にする IP アドレスの指定、および装置の DHCP オプションの設定が必要です。
- 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の場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチのポートが DHCP サーバに接続されている場合、`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 `trusted` として設定してください。
- スイッチのポートが DHCP クライアントに接続されている場合、`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 `untrusted` 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 (不揮発性 RAM) もフラッシュ メモリも、保存容量の制約があるため、バインディング ファイルは TFTP サーバに保存することを推奨します。
  - ネットワークベースの URL (TFTP、FTP など) の場合、スイッチが URL のバインディング ファイルにバインディングを書き込めるようにするには、設定した URL に空のファイルを作成しておく必要があります。サーバに空のファイルを作成しておく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、この設定ができないものもあります。
  - データベースのリース時間を正確にするため、NTP をイネーブルにして設定することを推奨します。詳細については、「[NTP の設定](#)」(p.6-4) を参照してください。
  - NTP を設定した場合、スイッチのシステム クロックが NTP と同期化されている場合のみ、スイッチは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。
- `untrusted` 装置が接続されている集約スイッチに `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、`untrusted` 装置は Option 82 情報をスプーフィングします。

## 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、イネーブル 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 サーバおよびリレー エージェントをイネーブルにします。デフォルトで、この機能はイネーブルに設定されています。
ステップ 3	<code>end</code>	イネーブル 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 ファイルにエントリを保存します。

DHCP サーバとリレー 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。



次の手順については、『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。

- リレー エージェント情報の確認 (検証)
- リレー エージェントのフォワーディング 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、イネーブル 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でイネーブルにします。
ステップ 3	<code>ip dhcp snooping vlan <i>vlan-range</i></code>	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 には、VLAN ID 番号で識別される 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、開始 VLAN ID と終了 VLAN ID をスペースで区切った VLAN ID の範囲を入力できます。
ステップ 4	<code>ip dhcp snooping information option</code>	スイッチで、DHCP サーバ宛に転送される要求メッセージ内の DHCP リレー情報 (Option 82 フィールド) の挿入および削除をイネーブルにします。これがデフォルトの設定です。

	コマンド	目的
ステップ 5	<code>ip dhcp snooping information option allow-untrusted</code>	(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、エッジスイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを受信できるようスイッチをイネーブルにします。  デフォルトではディセーブルに設定されています。   (注) このコマンドは trusted 装置に接続された集約スイッチ上でのみ入力する必要があります。
ステップ 6	<code>interface interface-id</code>	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	<code>ip dhcp snooping trust</code>	(任意)インターフェイスを trusted と untrusted のいずれかに設定します。untrusted クライアントからのメッセージをインターフェイスが受信できるようにするには、no キーワードを使用します。デフォルトでは untrusted に設定されています。
ステップ 8	<code>ip dhcp snooping limit rate rate</code>	(任意)インターフェイスが受信できる DHCP パケット数 / 秒の上限を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは無制限に設定されています。   (注) untrusted レート制限は、100 パケット / 秒以下にすることを推奨します。trusted インターフェイスにレート制限を設定する場合、ポートが複数の VLAN (DHCP スヌーピングがイネーブル) に割り当てられているトランクポートであれば、レート制限を増やさなければなりません。
ステップ 9	<code>exit</code>	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	<code>ip dhcp snooping verify mac-address</code>	(任意) untrusted ポート上で受信した DHCP パケットにある送信元 MAC アドレスが、パケット内のクライアントのハードウェアアドレスと一致するかどうかを確認するように、スイッチを設定します。デフォルトでは、パケット内の送信元 MAC アドレスとクライアントのハードウェアアドレスの一致を確認するように設定されています。
ステップ 11	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 12	<code>show running-config</code>	設定を確認します。
ステップ 13	<code>copy running-config startup-config</code>	(任意)コンフィギュレーション ファイルにエントリを保存します。

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。VLAN または VLAN 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。エッジスイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを廃棄するよう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、VLAN 10 上で DHCP スヌーピングをグローバルでイネーブルにし、ポート上でレート制限を 100 パケット / 秒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のイネーブル化および設定の手順については、『Cisco IOS IP Configuration Guide』Release 12.2 の「Configuring DHCP」の章にある「DHCP Configuration Task List」を参照してください。

## DHCP スヌーピング バインディング データベース 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て設定するには、イネーブル 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   rcp://user@host/filename}   tftp://host/filename</code>	次の形式を使用して、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>rcp://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>	データベースの転送処理の完了を待機する（完了しない場合に処理を停止させるまでの期間）（秒）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。待ち時間を無制限として定義するには 0 を指定します。この場合、転送を無制限に試行し続けます。
ステップ 4	<code>ip dhcp snooping database write-delay seconds</code>	バインディング データベース変更後の転送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 秒です（5 分）。
ステップ 5	<code>end</code>	イネーブル 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。指定できる <code>vlan-id</code> の範囲は 1 ~ 4904 です。指定できる <code>seconds</code> の範囲は 1 ~ 4294967295 秒です。  追加するエントリごとにこのコマンドを入力します。
		 <p><b>(注)</b> スイッチのテストまたはデバッグ時に、このコマンドを使用してください。</p>

	コマンド	目的
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 ファイルにエントリを保存します。

データベース エージェントおよびバインディング ファイルの使用を中止するには、`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。タイムアウト値や遅延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` イネーブル 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` イネーブル 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` イネーブル EXEC コマンドを使用します。削除するエントリごとにこのコマンドを入力してください。

## 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 のイネーブル EXEC コマンドを 1 つまたは複数使  
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
show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース (バインディング テーブル) で動的に設定されたバインディングのみを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベース ステータスと統計情報を表示します。



(注)

DHCP スヌーピングがイネーブルで、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。