



DHCP 機能および IP ソース ガードの 設定

この章では、Catalyst 3560 スイッチに DHCP 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。また、IP ソース ガード機能の設定方法も説明しています。



(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*』の「DHCP Commands」を参照してください。『*Addressing and Services*』 Release 12.2 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.21-2)
- DHCP 機能の設定 (p.21-9)
- DHCP スヌーピング情報の表示 (p.21-16)
- IP ソース ガードの概要 (p.21-17)
- IP ソース ガードの設定 (p.21-19)
- IP ソース ガード情報の表示 (p.21-21)

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 環境で幅広く使われており、これにより IP アドレスの管理のオーバーヘッドを大幅に軽減できます。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 \(p.21-2\)](#)
- [DHCP リレー エージェント \(p.21-2\)](#)
- [DHCP スヌーピング \(p.21-2\)](#)
- [Option 82 データ挿入 \(p.21-4\)](#)
- [Cisco IOS DHCP サーバデータベース \(p.21-7\)](#)
- [DHCP スヌーピング バインディング データベース \(p.21-7\)](#)

DHCP クライアントに関する詳細は、『*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間で DHCP パケットを転送するレイヤ 3 のデバイスです。各リレー エージェントは、同一の物理サブネット上にはないクライアントとサーバ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透過的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 \(p.21-16\)](#)」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 ネットワーク外のデバイス（お客様のスイッチなど）から送信されます。不明なデバイス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デバイス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デバイスの 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。

Cisco IOS Release 12.2(25)SEA より前のソフトウェア リリースでは、エッジスイッチにより Option 82 情報が挿入された場合、DHCP スヌーピング バインディング データベースが正しく読み込まれないため、集約スイッチ上で DHCP スヌーピングを設定できません。また、スタティック バインディングや Address Resolution Protocol（ARP; アドレス解決プロトコル）Access Control List（ACL; アクセスコントロールリスト）を使用しない場合、スイッチ上で IP 送信元ガードやダイナミック ARP 検査も設定できません。

Cisco IOS Release 12.2(25)SEA 以降では、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。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に、Option 82 情報を含むパケットが着信する場合は、集約スイッチ上でダイナミック ARP 検査や IP ソース ガードなどの DHCP 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デバイスを識別できます。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。

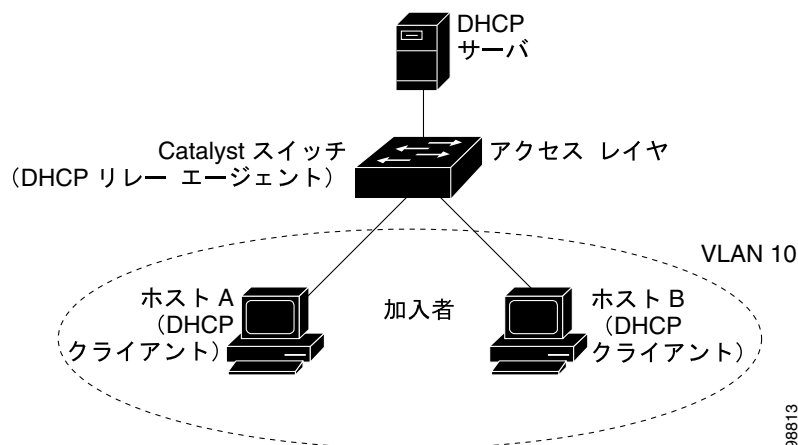


(注)

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デバイスが VLAN に割り当てられている場合のみ、サポートされます。

図 21-1 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 21-1 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、ネットワークヘ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。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID (**vlan-mod-port**) です。Cisco IOS Release 12.2(25)SEE 以降では、リモート ID と回線 ID を設定できます。これらのサブオプションの詳細については、「[DHCP スヌーピングおよび Option 82 のイネーブル化](#)」(p.21-12) を参照してください。
- 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。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、[図 21-2](#)にある次のフィールドの値は変化しません。

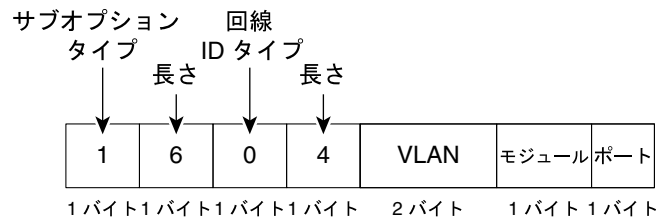
- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

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 の 10/100 ポートおよび Small Form-Factor Pluggable (SFP) モジュール スロットを含むスイッチでは、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 ポートとなり、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 21-2](#) に、デフォルトのサブオプション設定が使用されている場合のリモート 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 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 **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ると、このパケット フォーマットを使用します。

図 21-2 サブオプションのパケット フォーマット

回線 ID サブオプション フレーム形式



リモート ID サブオプション フレーム形式

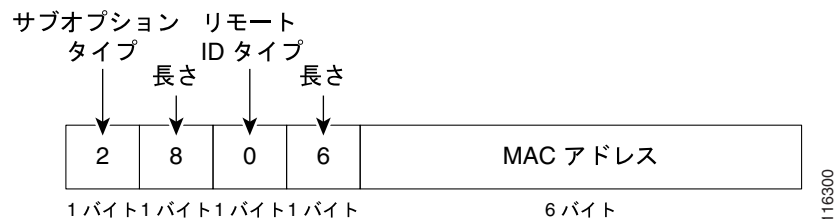


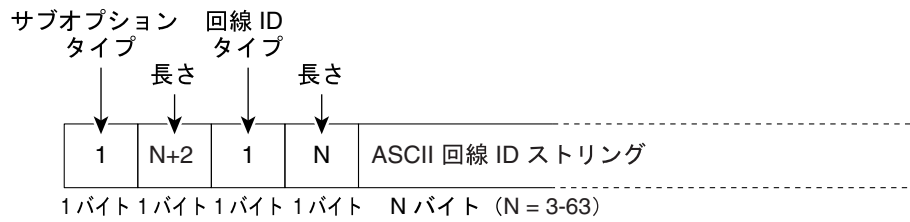
図 21-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力されると、スイッチにより、パケット フォーマットが使用されます。

パケット内にあるこれらのフィールドの値は、リモート ID および 回線 ID サブオプションを設定するとデフォルト値から次のように変化します。

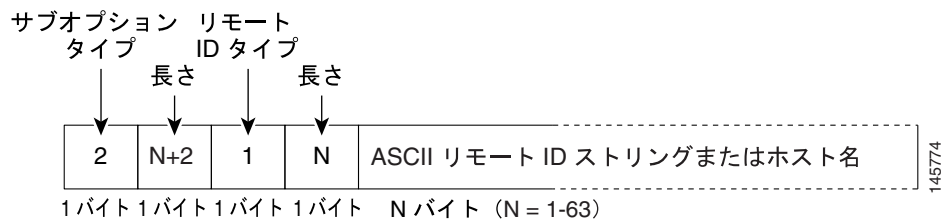
- 回線 ID サブオプション フィールド
 - 回線 ID タイプは 1 です。
 - 長さの値は変数で、設定したストリングの長さによります。
- リモート ID サブオプション フィールド
 - リモート ID タイプは 1 です。
 - 長さの値は変数で、設定したストリングの長さによります。

図 21-3 ユーザ設定サブオプション パケット フォーマット

回線 ID サブオプション フレーム フォーマット (ユーザ設定ストリング)



リモート ID サブオプション フレーム フォーマット (ユーザ設定ストリング)



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバデータベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバデータベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てるのが可能で、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることもできます。手動および自動アドレス バインディングの詳細については、『Cisco IOS IP Configuration Guide』Release 12.2 の「Configuring DHCP」の章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

DHCP スヌーピングがイネーブルの場合、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信頼できないインターフェイスに関する情報を保存します。データベースには最大で 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 (*binding*) には、IP アドレス、関連 MAC アドレス、およびリース時間 (16 進数表記)、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 があります。データベース エージェントは設定された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はチェックサムがあり、ファイルの最初からエントリの終わりまでのすべてのバイト数を計上します。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。

スイッチをリロードしたときにバインディングを維持するには、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。エージェントがディセーブルで、ダイナミック ARP 検査または IP ソース ガードがイネーブルに設定されていて、DHCP スヌーピング バインディング データベースにダイナミック バインディングがある場合、スイッチの接続が切断されます。エージェントがディセーブルで、DHCP スヌーピングのみがイネーブルの場合、スイッチの接続は切断されませんが、DHCP スヌーピングでは DHCP スプーフィング攻撃を防止できないことがあります。

リロードしたとき、スイッチは DHCP スヌーピング バインディング データベースを構築するため、バインディング ファイルを読み込みます。データベースが変更されると、スイッチがファイルを更新します。

スイッチが新しいバインディングを学習したり、バインディングを消失した場合には、スイッチはデータベース内のエントリを迅速に更新します。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。ファイルを更新する頻度は、設定可能な遅延に基づいて更新され、更新はバッチ処理されます。指定された時間 (write-delay および abort-timeout 値によって設定) でファイルが更新されない場合、更新は中止されます。

バインディングのある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
```

ファイル内の各エントリはチェックサム値でタグ付けされていて、スイッチはファイルの読み取り時にこの値を使用してエントリを確認します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連したエントリを、前のファイル更新に関連したエントリと区別するものです。

バインディング ファイルの例は次のとおりです。

```
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
```

スイッチが開始されて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等しい場合、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取ってバインディングを 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に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って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異なる場合。エントリとその後続のものが無視されます。
- エントリがリース時間を超過した場合 (リース時間が超過してもスイッチはバインディング エントリを削除しない場合があります)
- エントリ内のインターフェイスがシステムに存在しない場合
- インターフェイスがルーテッド インターフェイスか DHCP スヌーピング信頼インターフェイスの場合

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.21-9)
- DHCP スヌーピング設定時の注意事項 (p.21-10)
- DHCP サーバの設定 (p.21-11)
- DHCP リレー エージェントの設定 (p.21-11)
- パケット転送アドレスの指定 (p.21-11)
- DHCP スヌーピングおよび Option 82 のイネーブル化 (p.21-12)
- プライベート VLAN での DHCP スヌーピングのイネーブル化 (p.21-14)
- Cisco IOS DHCP サーバデータベースのイネーブル化 (p.21-14)
- 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.21-15)

DHCP のデフォルト設定

表 21-1 に、DHCP のデフォルト設定を示します。

表 21-1 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です(設定が必要) ¹ 。
DHCP リレー エージェント	イネーブル ²
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) ² 。
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。 ²
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 ³	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
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブルです(設定が必要)。  (注) スイッチは、DHCP サーバとして設定されているデバイスからのみ、ネットワーク アドレスおよび設定パラメータを取得します。
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	Cisco IOS ソフトウェアではイネーブルです(設定が必要)。宛先が設定されている場合のみ、この機能は有効です。

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デバイスおよび 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デバイス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、およびデバイスの DHCP オプションの設定が必要です。
- スイッチに数多くの回線 ID を設定する際は、NVRAM またはフラッシュ メモリ上の冗長な文字列の影響を考慮してください。他のデータと組み合わせて回線 ID を設定する場合、NVRAM またはフラッシュ メモリの容量を超過すると、エラー メッセージが表示されます。
- スイッチに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりすることができる IP アドレスを指定するか、デバイスに DHCP オプションを設定するか、または DHCP データベース エージェント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場合に次の注意事項に従ってください。
 - NVRAM (不揮発性 RAM) およびフラッシュ メモリのストレージ容量に制限があるので、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 URL (TFTP や FTP [ファイル転送プロトコル] など) の場合、スイッチが設定した 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む前に、その URL で空のファイルを作成しておく必要があります。先にサーバで空のファイルを作成する必要があるかどうかを判断するには、TFTP サーバのマニュアルを参照してください。一部の TFTP サーバはこの方法では設定することができません。
 - データベースのリース時間を正確にするには、Network Time Protocol (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.6-5) を参照してください。
 - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期している場合のみ、スイッチはバインディング変更をバインディング ファイルに書き込みます。
- **untrusted** デバイス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** デバイスは Option 82 情報をスプーフィングします。

DHCP サーバの設定

スイッチは DHCP サーバとして機能します。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェント機能はスイッチ上でイネーブルですが、設定されていません。これらの機能は動作しません。

スイッチを DHCP サーバとして設定する場合の手順については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Addressing and Services」の章にある「Configuring DHCP」を参照してください。

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>	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」の部分参照してください。

- 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

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを `ip helper-address address` インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的な規則は、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。`ip helper-address` コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにできます。ネットワーク アドレスを使用することでどの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、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>interface vlan vlan-id</code>	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、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 3	<code>ip address ip-address subnet-mask</code>	インターフェイスに IP アドレスおよび IP サブネットを設定します。




	コマンド	目的
ステップ 4	<code>ip helper-address address</code>	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバアドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにできます。ネットワーク アドレスを使用することで、ほかのサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	<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 6	<code>interface range port-range</code> または <code>interface interface-id</code>	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス レンジ 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>switchport mode access</code>	ポートの VLAN メンバーシップ モードを定義します。
ステップ 8	<code>switchport access vlan vlan-id</code>	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show running-config</code>	設定を確認します。
ステップ 11	<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 転送アドレスを削除するには、`no ip helper-address address` インターフェイス 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でイネーブルにします。
ステップ 3	<code>ip dhcp snooping vlan vlan-range</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	ip dhcp snooping information option format remote-id [string <i>ASCII-string</i> hostname]	<p>(任意) リモート ID サブオプションを設定します。</p> <p>次のようにリモート ID を設定できます。</p> <ul style="list-style-type: none"> 63 文字までの ASCII 文字列 (スペースなし) スイッチに設定されたホスト名 <p> (注) ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。</p> <p>デフォルトのリモート ID はスイッチ MAC アドレスです。</p>
ステップ 6	ip dhcp snooping information option allow-untrusted	<p>(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。</p> <p>デフォルトではディセーブルに設定されています。</p> <p> (注) このコマンドは trusted デバイスに接続された集約スイッチ上でのみ入力してください。</p>
ステップ 7	interface <i>interface-id</i>	<p>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。</p>
ステップ 8	ip dhcp snooping vlan <i>vlan</i> information option format-type circuit-id string <i>ASCII-string</i>	<p>(任意) 指定したインターフェイスで回線 ID サブオプションを設定します。</p> <p>1 ~ 4094 の範囲の VLAN ID を使用して VLAN およびポート ID を指定します。デフォルトの回線 ID は vlan-mod-port 形式のポート ID です。</p> <p>回線 ID を 3 ~ 63 の ASCII 文字 (スペースなし) を設定できます。</p>
ステップ 9	ip dhcp snooping trust	<p>(任意) インターフェイスを trusted または 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。</p>
ステップ 10	ip dhcp snooping limit rate <i>rate</i>	<p>(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。</p> <p> (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らない可能性があります。</p>
ステップ 11	exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>

	コマンド	目的
ステップ 12	<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 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show running-config</code>	設定を確認します。
ステップ 15	<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 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
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライベート VLAN で DHCP スヌーピングをイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN および関連付けられているセカンダリ VLAN の両方に伝播します。DHCP スヌーピングがプライマリ VLAN でイネーブルの場合、セカンダリ VLAN でもイネーブルに設定されています。

DHCP スヌーピングがすでにプライマリ VLAN に設定されていて DHCP スヌーピングをセカンダリ VLAN とは異なるように設定した場合、セカンダリ VLAN の設定は有効になりません。プライマリ VLAN に DHCP スヌーピングを設定する必要があります。プライマリ VLAN に DHCP スヌーピングが設定されていない場合は、VLAN 200 などのセカンダリ VLAN に DHCP スヌーピングを設定するときに、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not
take effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is
derived from its primary vlan.
```


`show ip dhcp snooping` 特権 EXEC コマンド出力では、DHCP スヌーピングがイネーブルであるプライマリおよびセカンダリ プライベート VLAN を含む、すべての VLAN を表示します。

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て設定する手順については、『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、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 rcp://user@host/filename} tftp://host/filename</code>	次の形式のいずれかを使用して、データベース エージェントまたはバインディング ファイル用の URL を指定します。 <ul style="list-style-type: none"> <code>flash:/filename</code> <code>ftp://user:password@host/filename</code> <code>http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar</code> <code>rcp://user@host/filename</code> <code>tftp://host/filename</code>
ステップ 3	<code>ip dhcp snooping database timeout seconds</code>	データベース転送処理を停止するまでに待機する時間 (秒) を指定します。 デフォルト値は 300 ミリ秒です。指定できる範囲は 0 ~ 86400 です。時間を無制限に定義するには 0 を使用します。これは、転送の試行を無制限に継続することを意味します。
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たあとの伝送が遅延する期間を指定します。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。 追加する各エントリにこのコマンドを入力します。  (注) スイッチのテストやデバッグを行うとき、このコマンドを使用します。
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と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 ファイルの使用を止めるには、`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。タイムアウト値または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消去するには、`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。削除する各エントリにこのコマンドを入力します。

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 21-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 21-2 DHCP 情報を表示するためのコマンド

コマンド	目的
<code>show ip dhcp snooping</code>	スイッチの DHCP スヌーピングの設定を表示します。
<code>show ip dhcp snooping binding</code>	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。
<code>show ip dhcp snooping database</code>	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。
<code>show ip source binding</code>	ダイナミックおよびスタティックに設定されたバインディングを表示します。



(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。

IP ソース ガードの概要

IP ソース ガードは、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで、実現しています。IP ソース ガードを使用して、ホストがネイバの IP アドレスを使用しようとすることによるトラフィック攻撃を回避できます。

DHCP スヌーピングが信頼できないインターフェイスでイネーブルの場合に IP ソース ガードをイネーブルにできます。IP ソース ガードがインターフェイスでイネーブルになったあと、スイッチは、DHCP スヌーピングで許可された DHCP パケットを除く、インターフェイスで受信されたすべての IP トラフィックをブロックします。ポート Access Control List (ACL; アクセス コントロール リスト) はインターフェイスに適用されます。ポート ACL により、IP 送信元バインディングテーブル内の送信元 IP アドレスの IP トラフィックのみを許可し、他のトラフィックを拒否できます。



(注) ポート ACL は、同じインターフェイスに影響するルータ ACL や VLAN マップに優先します。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング (スタティック IP 送信元バインディング) があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルの場合にのみ IP 送信元バインディングテーブルを使用します。

IP ソース ガードは、アクセス ポートやトランク ポートなどのレイヤ 2 ポートでのみサポートされます。IP ソース ガードを、送信元 IP フィルタリングや送信元 IP および MAC アドレス フィルタリングとともに設定できます。

ここでは、次の情報について説明します。

- [送信元 IP アドレス フィルタリング \(p.21-17\)](#)
- [送信元 IP および MAC アドレス フィルタリング \(p.21-18\)](#)

送信元 IP アドレス フィルタリング

IP ソース ガードがこのオプションでイネーブルの場合、IP トラフィックは送信元 IP アドレスに基づいてフィルタリングされます。送信 IP アドレスが DHCP スヌーピング バインディング データベースのエントリまたは IP 送信元バインディング テーブル内のバインディングと一致した場合、スイッチは IP トラフィックを転送します。

DHCP スヌーピング バインディングまたはスタティック IP 送信元バインディングがインターフェイスで追加、変更、削除された場合、スイッチは IP 送信元バインディングを変更してポート ACL を修正し、ポート ACL をインターフェイスに適用します。

(DHCP スヌーピングで動的に学習されたか手動で設定された) IP 送信元バインディングが設定されていないインターフェイスで IP ソース ガードをイネーブルにする場合、スイッチはインターフェイス上のすべての IP トラフィックを拒否するポート ACL を作成し、適用します。IP ソース ガードをディセーブルにする場合、スイッチはポート ACL をインターフェイスから削除します。

送信元 IP および MAC アドレス フィルタリング

IP ソース ガードがこのオプションでイネーブルの場合、IP トラフィックは送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスおよび MAC アドレスが IP 送信元バインディング テーブルのエントリと一致する場合にトラフィックを転送します。

IP ソース ガードと送信元 IP および MAC アドレス フィルタリングがイネーブルの場合、スイッチは IP および非 IP トラフィックをフィルタリングします。IP または非 IP パケットの送信元 MAC アドレスが有効な IP 送信元バインディングと一致する場合、スイッチはパケットを転送します。スイッチは、DHCP パケットを除く他のすべてのタイプのパケットを廃棄します。

スイッチは、ポートセキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポートセキュリティ違反が発生する際にインターフェイスをシャットダウンできます。

IP ソース ガードの設定

ここでは、次の設定情報について説明します。

- デフォルトの IP ソース ガードの設定 (p.21-19)
- IP ソース ガード設定時の注意事項 (p.21-19)
- IP ソース ガードのイネーブル化 (p.21-20)

デフォルトの IP ソース ガードの設定

デフォルトでは、IP ソース ガードはディセーブルに設定されています。

IP ソース ガード設定時の注意事項

IP ソース ガードの設定時の注意事項は次のとおりです。

- 非ルーテッドポートでのみスタティック IP バインディングを設定できます。 **ip source binding mac-address vlan vlan-id ip-address interface interface-id** グローバルコンフィギュレーションコマンドをルーテッドインターフェイスに入力した場合、このエラーメッセージが表示されます。
Static IP source binding can only be configured on switch port.
- IP ソース ガードと送信元 IP フィルタリングが VLAN でイネーブルの場合、DHCP スヌーピングは、インターフェイスが所属するアクセス VLAN でイネーブルでなければなりません。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードがイネーブルで、DHCP スヌーピングがすべての VLAN でイネーブルの場合、送信元 IP アドレス フィルタがすべての VLAN に適用されます。




(注) IP ソース ガードがイネーブルでトランク インターフェイス上の VLAN で DHCP スヌーピングがディセーブルの場合、スイッチは適切にトラフィックをフィルタリングできません。

- IP ソース ガードと送信元 IP および MAC アドレス フィルタリングがイネーブルの場合、DHCP スヌーピングおよびポート セキュリティがインターフェイスでイネーブルでなければなりません。
- プライベート VLAN が設定されているインターフェイスで IP ソース ガードを設定する場合、ポート セキュリティはサポートされません。
- IP ソース ガードは EtherChannel でサポートされません。
- IEEE 802.1x ポートベース認証がイネーブルである場合、IP ソース ガードの機能をイネーブルにできません。
- Ternary CAM (TCAM) エントリ数が最大数を越えた場合、CPU の使用量が増加します。

■ IP ソース ガードの設定

IP ソース ガードのイネーブル化

インターフェイス上で IP ソース ガードをイネーブルにして設定するには、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>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 3	<code>ip verify source</code> または <code>ip verify source port-security</code>	<p>IP ソース ガードと送信元 IP アドレス フィルタリングをイネーブルにします。</p> <p>IP ソース ガードと送信元 IP および MAC アドレス フィルタリングをイネーブルにします。</p> <p> (注) ip verify source port-security インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポートセキュリティの両方をイネーブルにする場合は、次の 2 つの注意事項があります。</p> <ul style="list-style-type: none"> • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されません。スイッチが DHCP 以外のデータトラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 4	<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 5	<code>ip source binding mac-address vlan vlan-id ip-address interface interface-id</code>	<p>スタティック IP 送信元バインディングを追加します。</p> <p>各スタティック バインディングに対してこのコマンドを入力します。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip verify source [interface interface-id]</code>	すべてのインターフェイスまたは特定のインターフェイスに対して IP ソース ガード設定を表示します。
ステップ 8	<code>show ip source binding [ip-address] [mac-address] [dhcp-snooping static] [interface interface-id] [vlan vlan-id]</code>	スイッチ、特定の VLAN、または特定のインターフェイス上の IP 送信元バインディングを表示します。
ステップ 9	<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。

IP ソース ガードおよび送信元 IP アドレス フィルタリングをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP 送信元バインディング エントリを削除するには、**no ip source** 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、IP ソース ガードと送信元 IP および MAC フィルタリングを VLAN 10 および VLAN 11 でイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet0/1
Switch(config)# end
```

IP ソース ガード情報の表示

IP ソース ガード情報を表示するには、表 21-3 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 21-3 IP ソース ガード情報の表示用コマンド

コマンド	目的
show ip source binding	スイッチの IP 送信元バインディングを表示します。
show ip verify source	スイッチの IP ソース ガード設定を表示します。

■ IP ソース ガード情報の表示