CHAPTER 22

DHCP 機能および IP ソース ガードの設定

この章では、Catalyst 3750-E または 3560-E スイッチに Dynamic Host Configuration Protocol（DHCP）スヌーピングと Option 82 データ挿入機能、および DHCP サーバのポートベース アドレス割り当て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。特に明記しないかぎり、*スイッチ*という用語は Catalyst 3750-E または 3560-E スタンドアロン スイッチおよび Catalyst 3750-E スイッチ スタックを意味します。

（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 12.4*』の「DHCP Commands」を参照してください。

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 スヌーピングおよびスイッチ スタック」（P.22-8）
- 「Cisco IOS DHCP サーバ データベース」（P.22-6）
- 「DHCP スヌーピング バインディング データベース」（P.22-6）

DHCP クライアントに関する詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』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.22-16）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（カスタマーのスイッチなど）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 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 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ドロップします。

次の状況が発生すると、スイッチは DHCP パケットをドロップします。

- DHCPOFFER、DHCPACK、DHCPNAK、または DHCPLEASEQUERY 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 DHCPRELEASE または DHCPDECLINE 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ドロップします。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。

untrusted インターフェイスを介して集約スイッチをエッジ スイッチに接続することができ、**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 Option 82 情報を持ったパケットをエッジ スイッチから受信します。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 インスペクションや 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。

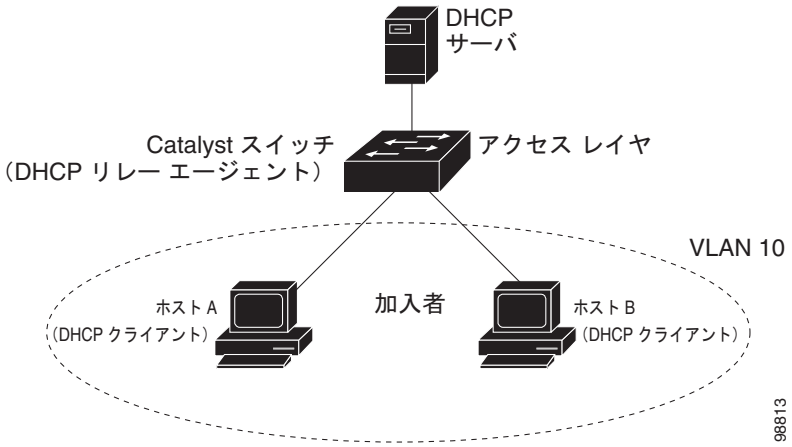
Option 82 データ挿入

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 アドレスの他にも）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、グローバルにイネーブルで、この機能を使用している加入デバイスが割り当てられている VLAN 上にある場合だけ、サポートされます。

図 22-1 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 22-1　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。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。リモート ID および回線 ID は設定できます。サブオプションの設定の詳細については、を参照してください。サブオプションの設定の詳細については、「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.22-13）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 22-2 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

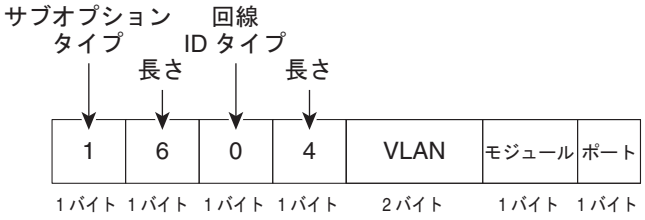
- リモート ID タイプ
- リモート ID タイプの長さ

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 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール スロットを搭載する Catalyst 3750-E スイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 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 スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図 22-2 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。回線 ID サブオプションの場合、モジュール番号がスタック内のスイッチ番号に対応します。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 22-2　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 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

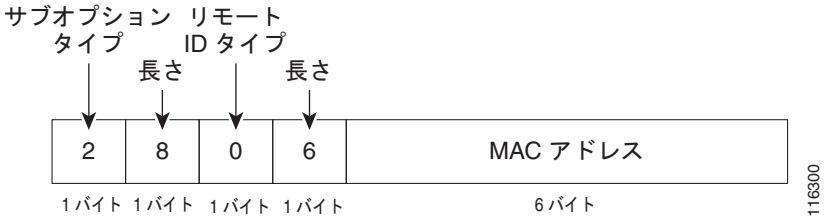


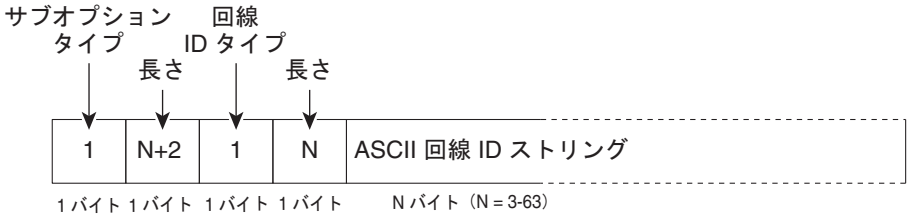
図 22-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力されると、スイッチにより、パケット フォーマットが使用されます。

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。

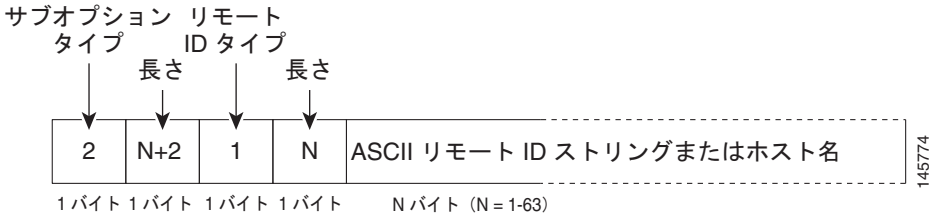
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定したストリングの長さによります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定したストリングの長さによります。

図 22-3　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（ユーザ設定のストリング）



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



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こと、または、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が可能です。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 12.4*』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 untrusted インターフェイスに関する情報を保存します。データベースには最大で 64,000 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 インスペクションまたは 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 スヌーピングだけ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 DCHP 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りした場合には、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 Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 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。

- スイッチ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 スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに加入すると、スイッチはスタック マスターから DHCP スヌーピング設定を受信します。メンバーがスタックから脱退した場合は、スイッチに関連付けられたすべての DHCP スヌーピング アドレス バインディングがエージング アウトします。

すべてのスヌーピング統計情報は、スタック マスター上で生成されます。新しいスタック マスターが選択されると、統計情報カウンタはリセットされます。

スタック マージが発生し、スタック マスターがもはやスタック マスターでなくなると、そのスタック マスター内のすべての DHCP スヌーピング バインディング（スタック マスターは除く）が失われます。スタック分割により、既存のスタック マスターは変更されませんが、分割されたスイッチに所属するバインディングは、エージング アウトします。分割されたスタックの新しいマスターは、新たに着信する DHCP パケットの処理を開始します。スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

DHCP 機能の設定

DHCP のデフォルト設定

表 22-1　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（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ドロップされます）。[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。

表 22-1　DHCP のデフォルト設定 （続き）

機能	デフォルト設定
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パケットを受信する 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（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だけ、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（設定が必要）。宛先が設定されている場合だけ、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だけ、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; スイッチ仮想インターフェイス）上で設定されている場合だけ、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

- スイッチの DHCP スヌーピングはグローバルで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。
- 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 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 Trivial File Transfer Protocol（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 File Transfer Protocol（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; ネットワーク タイム プロトコル）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 の概要」（P.7-2）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だけ、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。
- Cisco IOS Release 12.2(37)SE 以降では、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力すると DHCP スヌーピングの統計情報を表示でき、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力するとスヌーピング統計情報カウンタをクリアできます。
- DHCP スヌーピング スマート ロギングを設定すると、DHCP によってドロップされたパケットの内容が、NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。スマート ロギングの詳細については、「スマート ロギングの設定」（P.32-15）を参照してください。

（注）　RSPAN VLAN 上で DHCP スヌーピングをイネーブルにしないでください。DHCP スヌーピングが RSPAN VLAN 上でイネーブルになっている場合、DHCP パケットが RSPAN 宛先ポートに到達しない可能性があります。

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ときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の「Configuring DHCP」を参照してください。

DHCP サーバとスイッチ スタック

データベースをバインドする DHCP は、スタック マスターで管理されます。新しいスタック マスターが割り当てられる場合は、新しいマスターは保存されているバインディング データベースを TFTP サーバからダウンロードします。スタック マスターに障害が生じると、保存されていないバインディング データベースは失われます。失われたバインディングに関連する IP アドレスは、解除されます。**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] グローバル コンフィギュレーション コマンドを使用して、自動バックアップを設定する必要があります。

スタック マージが発生すると、スタック メンバーとなるスタック マスターは、すべての DHCP リースのバインディングを失います。スタックを分割すると、分割された新しいマスターは、既存の DHCP リースのバインディングではなく、新しい DHCP サーバの動作をします。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」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	**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	**service dhcp**	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	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（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 12.4*』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

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。一般的なルールは、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 アドレスにすることができます。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	**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	**interface vlan** *vlan-id*	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	**ip address** *ip-address subnet-mask*	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。
ステップ 4	**ip helper-address** *address*	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 アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも 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	**exit**	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	**interface range** *port-range* または **interface** *interface-id*	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、インターフェイス範囲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 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	**switchport mode access**	ポートの VLAN メンバシップ モードを定義します。
ステップ 8	**switchport access vlan** *vlan-id*	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	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（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 パケット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	**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	**ip dhcp snooping**	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	**ip dhcp snooping vlan** *vlan-range* [**smartlog**]	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。 • （任意）ドロップされたパケットの内容を NetFlow 収集装置に送信するようにスイッチを設定するには、**smartlog** を入力します。
ステップ 4	**ip dhcp snooping information option**	スイッチで、DHCP サーバ宛て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。
ステップ 5	**ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**]	（任意）リモート ID サブオプションを設定します。 リモート ID は次のように設定できます。 • 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 **（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。 デフォルトのリモート ID はスイッチ MAC アドレスです。
ステップ 6	**ip dhcp snooping information option allow-untrusted**	（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 デバイスに接続された集約スイッチ上でだけ入力する必要があります。
ステップ 7	**interface** *interface-id*	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 8	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string*	（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。 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 はポート ID で、**vlan-mod-port** の形式です。 回線 ID は 3 ～ 63 の ASCII 文字列（スペースなし）を設定できます。 （任意）**override** キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。

	コマンド	目的
ステップ 9	**ip dhcp snooping trust**	（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。
ステップ 10	**ip dhcp snooping limit rate** *rate*	（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らない可能性があります。
ステップ 11	**exit**	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 12	**ip dhcp snooping verify mac-address**	（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	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show running-config**	設定を確認します。
ステップ 15	**copy running-config startup-config**	（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 パケットをドロップ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、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 gigabitethernet2/0/1
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 12.4*』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	**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	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*	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。 • **flash**[*number*]**:**/*filename* （任意）スタック マスターのスタック メンバー番号を指定するには、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*

	コマンド	目的
ステップ 3	**ip dhcp snooping database timeout** *seconds*	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 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	**ip dhcp snooping database write-delay** *seconds*	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	**end**	特権 EXEC モードに戻ります。
ステップ 6	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*	（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	**show ip dhcp snooping database** [**detail**]	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	**copy running-config startup-config**	（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

表 22-2　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だけを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示します。
show ip source binding	動的および静的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

IPSG 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す。この機能は、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 ガードを使用すると、ホストが自身のネイバーの IP アドレスを使用しようとしたときに発生するトラフィック攻撃を回避できます。

DHCP スヌーピングが untrusted 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。IPSG がインターフェイスでイネーブルになると、スイッチは、そのインターフェイスで受信した IP トラフィックのうち、DHCP スヌーピングで許可された DHCP パケット以外はすべてブロックします。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 トラフィックだけを許可し、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を及ぼすルータ ACL や VLAN マップよりも優先されます。

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だけ IP 送信元バインディング テーブルを使用します。

IPSG は、アクセス ポートやトランク ポートなどのレイヤ 2 ポートでだけサポートされます。IPSG とともに、送信元 IP フィルタリングを使用するか、送信元 IP および MAC アドレス フィルタリングを使用するかを設定できます。

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.22-17）
- 「送信元 IP および MAC アドレス フィルタリング」（P.22-18）
- 「スタティック ホストの IP ソース ガード」（P.22-18）

送信元 IP アドレス フィルタリング

IPSG ソース ガードがこのオプションとともにイネーブルの場合は、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の変更を使用してポート ACL を修正し、ポート ACL をインターフェイスに再適用します。

IPSG をイネーブルにしたインターフェイスに対して IP 送信元バインディング（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）が設定されていない場合は、スイッチはその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 を作成して適用します。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 トラフィックのフィルタリングは、送信元の IP アドレスと MAC アドレスに基づいて行われます。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。

アドレス フィルタリングがイネーブルのときは、スイッチは IP と非 IP の両方の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ドロップします。

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。

スタティック ホストの IP ソース ガード

（注）　スタティック ホストの IPSG（IP ソース ガード）は、アップリンク ポートおよびトランク ポートには使用しないでください。

「スタティック ホストの IPSG」とは、DHCP を使用しないスタティック環境でも IPSG を利用できるようにするための機能です。以前の IPSG では、DHCP スヌーピングで作成されたエントリを使用して、スイッチに接続されたホストの検証が行われていました。有効な DHCP バインディングを持たないホストから受信されたトラフィックは、ドロップされます。このセキュリティ機能によって、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 トラフィックが制限されます。トラフィックのフィルタリングは、DHCP スヌーピング バインディング データベースに基づいて、および手動で設定された IP ソース バインディングに基づいて行われます。以前のバージョンの IPSG は、DHCP 環境でなければ機能しませんでした。

スタティック ホストの IPSG を利用すれば、IPSG は DHCP がなくても機能するようになります。スタティック ホストの IPSG が機能するには、IP デバイス トラッキング テーブルのエントリが必要です。このエントリを使用して、ポート ACL がインストールされます。スイッチは、ARP 要求またはその他の IP パケットに基づいてスタティック エントリを作成して、個々のポートに対する有効なホストのリストを維持します。ポートごとに、そのポートへのトラフィック送信が許可されるホストの数を管理者が指定することもできます。これは、レイヤ 3 でポート セキュリティを有効にするのと同じことになります。

スタティック ホストの IPSG では、ダイナミック ホストもサポートされます。ダイナミック ホストが受信した IP アドレスが DHCP によって割り当てられたものであり、そのアドレスが IP DHCP スヌーピング テーブルに存在する場合は、同じエントリが IP デバイス トラッキング テーブルによって学習されます。スタック環境では、マスターのフェールオーバーが発生したときも、メンバー ポートに接続されたスタティック ホストに対する IP ソース ガードのエントリは維持されます。**show ip device tracking all** EXEC コマンドを入力すると、IP デバイス トラッキング テーブルのエントリが ACTIVE と表示されます。

（注）　複数のネットワーク インターフェイスを持つ IP ホストの中には、無効なパケットをネットワーク インターフェイスに挿入できるものがあります。この無効パケットには、そのホストの別のネットワーク インターフェイスの IP アドレスまたは MAC アドレスが送信元アドレスとして格納されています。この無効なパケットを受け取ると、スタティック ホストの IPSG はそのホストに接続して、無効な IP アドレスまたは MAC アドレスのバインディングを学習するとともに、その無効なバインディングを拒否します。対応するオペレーティング システムおよびネットワーク インターフェイスのベンダーに問い合わせて、ホストによる無効なパケットの挿入を防止してください。

スタティック ホストの IPSG は初めに、IP または MAC バインディングを動的に、ACL ベースのスヌーピング メカニズムを通して学習します。スタティック ホストからの IP または MAC バインディングの学習は、ARP および IP のパケットによって行われます。これらは、デバイス トラッキング データベースに格納されます。そのポートに対して動的に学習された、または静的に設定された IP アドレスの数が最大値に達した後は、新しい IP アドレスを持つパケットはすべてハードウェアによってドロップされます。何らかの理由で移動または除去されたホストを解決するために、スタティック ホストの IPSG は、動的に学習した IP アドレス バインディングを、IP デバイス トラッキングを利用してエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。1 つのポートが DHCP ホストとスタティック ホストの両方に接続されている場合は、複数のバインディングが作成されます。たとえば、バインディングはデバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に格納されます。

IP ソース ガードの設定

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

- 非ルーテッド ポートでだけスタティック 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 フィルタリングがインターフェイス上でイネーブルになっているときは、そのインターフェイスのアクセス VLAN に対して DHCP スヌーピングがイネーブルになっている必要があります。
- 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 フィルタリングをイネーブルにする場合は、そのインターフェイスに対して DHCP スヌーピングおよびポート セキュリティがイネーブルになっている必要があります。**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、DHCP サーバが Option 82 をサポートしていることを確認する必要があります。IP ソース ガードと MAC アドレス フィルタリングがイネーブルの場合、DHCP ホストの MAC アドレスはホストにリースが与えられるまで学習されません。サーバからホストにパケットを転送するときに、DHCP スヌーピングは Option 82 データを使用してホスト ポートを識別します。
- 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。
- この機能をイネーブルにできるのは、802.1x ポートベース認証がイネーブルであるときです。
- Ternary Content Addressable Memory（TCAM; 三値連想メモリ）エントリの数が最大値を超えた場合は、CPU の使用量が増加します。
- IP ソース ガード スマート ロギングを設定すると、指定されたアドレスや DHCP によって学習されたアドレス以外の送信元アドレスを持つパケットは拒否され、そのパケットの内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。スマート ロギングの詳細については、「スマート ロギングの設定」（P.32-15）を参照してください。
- スイッチ スタックでは、IP ソース ガードがスタック メンバー インターフェイスに設定されていて、**no switch** *stack-member-number* **provision** グローバル コンフィギュレーション コマンドの入力によりそのスイッチの設定を削除した場合、インターフェイス スタティック バインディングはバインディング テーブルから削除されますが、実行コンフィギュレーションからは削除されません。**switch** *stack-member-number* **provision** コマンドの入力によりスイッチを再びプロビジョニングすると、バインディングは復元されます。

  実行コンフィギュレーションからバインディングを削除するには、**no switch provision** コマンドを入力する前に IP ソース ガードをディセーブルにする必要があります。バインディング テーブルからインターフェイスを削除中にスイッチをリロードすると、設定も削除されます。プロビジョニングされたスイッチの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

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	**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	**interface** *interface-id*	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	**ip verify source** [**smartlog**]	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。 • （任意）ドロップされたパケットの内容を NetFlow 収集装置に送信するようにスイッチを設定するには、**smartlog** を入力します。

	コマンド	目的
	または **ip verify source port-security**	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。 **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 つの警告があります。 • 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	**exit**	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	**ip source binding** *mac-address* **vlan** *vlan-id ip-address* **inteface** *interface-id*	スタティック IP 送信元バインディングを追加します。 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。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip verify source** [**interface** *interface-id*]	IP ソース ガードの設定を確認します。
ステップ 8	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**inteface** *interface-id*] [**vlan** *vlan-id*]	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	**copy running-config startup-config**	（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、VLAN 10 および 11 上で送信元 IP および MAC のフィルタリングによる IP ソース ガードを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 gigabitethernet1/0/1
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
gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Switch(config)# end
```

スタティック ホストの IP ソース ガードの設定

- 「レイヤ 2 アクセス ポート上のスタティック ホストの IP ソース ガードの設定」（P.22-22）
- 「プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定」（P.22-25）

レイヤ 2 アクセス ポート上のスタティック ホストの IP ソース ガードの設定

（注）　スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がプライベート VLAN ホスト ポート上で使用される場合にも適用されます。

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	**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	**ip device tracking**	IP ホスト テーブルをオンにするとともに、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	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 4	**switchport mode access**	ポートをアクセス ポートとして設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートの VLAN を設定します。
ステップ 6	**ip verify source tracking port-security**	スタティック ホストの IPSG を MAC アドレス フィルタリングとともにイネーブルにします。 （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ときは、次のことに注意してください。 • 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 7	**ip device tracking maximum** *number*	このポートに対して IP デバイス トラッキング テーブルに保持できるスタティック IP の数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートに対してポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートに対する MAC アドレスの最大数を設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show ip verify source interface** *interface-id*	コンフィギュレーションを確認するために、スタティック ホストに対する IPSG 許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	コンフィギュレーションを確認するために、スイッチ インターフェイス上の特定のホストに対する IP-MAC バインディングを表示します。 • **all active** : アクティブの IP または MAC バインディング エントリだけを表示します。 • **all inactive** : 非アクティブの IP または MAC バインディング エントリだけを表示します。 • **all** : アクティブおよび非アクティブの IP または MAC バインディング エントリを表示します。

次に、特定のインターフェイス上のスタティック ホストの IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、特定のポート上のスタティック ホストの IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポートに対してスタティック ホストの IPSG と IP フィルタをイネーブルにしてから、インターフェイス Gi1/0/3 上の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       40.1.1.24                          10
Gi1/0/3      ip trk       active       40.1.1.20                          10
Gi1/0/3      ip trk       active       40.1.1.21                          10
```

次に、レイヤ 2 アクセス ポートに対してスタティック ホストの IPSG と IP-MAC フィルタをイネーブルにしてから、インターフェイス Gi1/0/3 上の有効な IP-MAC バインディングを確認し、さらにこのインターフェイス上のバインディングの数が最大値に達しているかどうかを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi1/0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi1/0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi1/0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi1/0/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

次に、すべてのインターフェイスのすべての IP または MAC バインディング エントリを表示する例を示します。CLI には、すべてのアクティブ エントリに加えて、非アクティブのエントリも表示されます。インターフェイス上でホストが学習されると、その新しいエントリはアクティブになります。ホストとインターフェイスとの接続が切断されて、ホストが別のインターフェイスに接続されたときは、そのホストが検出されるとただちに、新しい IP または MAC バインディング エントリはアクティブとして表示されます。このホストが前に接続していたインターフェイス上での、このホストに対する古いエントリは、非アクティブとなります。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.9       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.10      0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.1       0001.0600.0000  9   GigabitEthernet1/0/2     ACTIVE
200.1.1.1       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.2       0001.0600.0000  9   GigabitEthernet1/0/2     ACTIVE
200.1.1.2       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.3       0001.0600.0000  9   GigabitEthernet1/0/2     ACTIVE
200.1.1.3       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.4       0001.0600.0000  9   GigabitEthernet1/0/2     ACTIVE
200.1.1.4       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.5       0001.0600.0000  9   GigabitEthernet1/0/2     ACTIVE
200.1.1.5       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.6       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.7       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
```

次に、すべてのインターフェイスのアクティブの IP または MAC バインディング エントリをすべて表示する例を示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet1/0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet1/0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet1/0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet1/0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet1/0/1     ACTIVE
```

次に、すべてのインターフェイスの非アクティブの IP または MAC バインディング エントリをすべて表示する例を示します。このホストは、初めに GigabitEthernet 1/0/1 上で学習され、その後で GigabitEthernet 0/2 に移動しました。GigabitEthernet1/0/1 上で学習された IP または MAC バインディング エントリは、非アクティブとなっています。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
```

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.9       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.10      0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.1       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.2       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.3       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.4       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.5       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.6       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
200.1.1.7       0001.0600.0000  8   GigabitEthernet1/0/1     INACTIVE
```

次に、すべてのインターフェイスのすべての IP デバイス トラッキング ホスト エントリの数を表示する例を示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
-----------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
-----------------------------------------------------------------------
Gi1/0/3                 5
```

プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定

（注） スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がレイヤ 2 アクセス ポート上で使用される場合にも適用されます。

特権 EXEC モードで、次に示す手順を実行してレイヤ 2 アクセス ポート上のスタティック ホストの IPSG と IP フィルタを設定します。

	コマンド	目的
ステップ 1	**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	**vlan** *vlan-id1*	VLAN 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	**private-vlan primary**	プライマリ VLAN をプライベート VLAN ポート上に設定します。
ステップ 4	**exit**	VLAN 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	**vlan** *vlan-id2*	別の VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 6	**private-vlan isolated**	独立 VLAN をプライベート VLAN ポート上に設定します。
ステップ 7	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 8	**vlan** *vlan-id1*	VLAN コンフィギュレーション モードを開始します。
ステップ 9	**private-vlan association 201**	VLAN を独立プライベート VLAN ポートに関連付けます。
ステップ 10	**exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 11	**interface fastEthernet** *interface-id*	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。

	コマンド	目的
ステップ 12	**switchport mode private-vlan host**	（任意）ポートをプライベート VLAN ホストとして設定します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）このポートに、対応するプライベート VLAN を関連付けます。
ステップ 14	**ip device tracking maximum** *number*	このポートに対して IP デバイス トラッキング テーブルに保持できるスタティック IP の数の上限を設定します。 最大値は 10 です。 **（注）** スタティック ホストの IPSG を機能させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポート上のスタティック ホストの IPSG と MAC アドレス フィルタリングをアクティブにします。
ステップ 16	**end**	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 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IP ソース ガードの設定を確認します。スタティック ホストの IPSG の許可 ACL を表示します。

次に、プライベート VLAN ホスト ポート上でスタティック ホストの IPSG と IP フィルタをイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface             STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.20       0000.0000.0305  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  GigabitEthernet1/0/3        ACTIVE
40.1.1.22       0000.0000.0307  200   GigabitEthernet1/0/3        ACTIVE
40.1.1.23       0000.0000.0308  200 GigabitEthernet1/0/3        ACTIVE
```

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合は、バインディングにはプライマリ VLAN ID が関連付けられます。したがって、この例ではプライマリ VLAN ID である 200 が表に表示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
```

```
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       40.1.1.23                          200
Gi1/0/3      ip trk       active       40.1.1.24                          200
Gi1/0/3      ip trk       active       40.1.1.20                          200
Gi1/0/3      ip trk       active       40.1.1.21                          200
Gi1/0/3      ip trk       active       40.1.1.22                          200
Gi1/0/3      ip trk       active       40.1.1.23                          201
Gi1/0/3      ip trk       active       40.1.1.24                          201
Gi1/0/3      ip trk       active       40.1.1.20                          201
Gi1/0/3      ip trk       active       40.1.1.21                          201
Gi1/0/3      ip trk       active       40.1.1.22                          201
```

この出力からは、5 つの有効な IP-MAC バインディングはプライマリとセカンダリの両方の VLAN 上にあることがわかります。

IP ソース ガード情報の表示

表 22-3　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。

DHCP サーバのポートベース アドレス割り当ての概要

DHCP サーバのポートベース アドレス割り当ては、DHCP をイネーブルにし、接続されたデバイス クライアント識別情報またはクライアント ハードウェア アドレスに関係なく、イーサネット スイッチ ポート上で同じ IP アドレスを維持する機能です。

イーサネット スイッチがネットワークに配置されている場合、直接接続されているデバイスとの接続が可能です。工場の現場などの一部の環境では、1 つのデバイスが故障した場合、既存のネットワーク内で代替デバイスが即座に動作する必要があります。現在の DHCP の実装では、DHCP が代替デバイスに同じ IP アドレス を提供する保証はありません。制御、モニタリング、および他のソフトウェアでは、各デバイスに関連付けられた安定した IP アドレス を予期します。デバイスが交換された場合、アドレス割り当ては、DHCP クライアントが変わった場合でも安定していなければなりません。

DHCP サーバのポートベース アドレス割り当て機能が設定されている場合、ポートで受信された DHCP メッセージ内のクライアント識別情報またはクライアント ハードウェア アドレスが変わった場合でも、接続された同じポートには常に同じ IP アドレスが提供されます。DHCP プロトコルは、DHCP パケット内のクライアント識別情報オプションにより、DHCP クライアントを認識します。クライアント識別情報オプションが含まれていないクライアントは、クライアント ハードウェア アドレスによって識別されます。この機能を設定すると、インターフェイスのポート名がクライアント識別情報またはハードウェア アドレスを上書きし、実際の接続ポイント、スイッチ ポートがクライアント識別情報になります。

イーサネット ケーブルを同じポートに接続することにより、いかなる場合でも、接続されたデバイスに対する DHCP を通して同じ IP アドレスが割り当てられます。

DHCP サーバのポートベース アドレス割り当て機能は、Cisco IOS DHCP サーバだけでサポートされており、サードパーティ製のサーバではサポートされていません。

DHCP サーバのポートベース アドレス割り当ての設定

ポートベースのアドレス割り当てのデフォルト設定

デフォルトでは、DHCP サーバのポートベース アドレス割り当てはディセーブルです。

ポートベース アドレス割り当ての設定時の注意事項

- ポート単位では、1 つの IP アドレスだけを割り当てることができます。
- 予約された（あらかじめ割り当てられた）アドレスは、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドを使用してはクリアできません。
- あらかじめ割り当てられたアドレスは、通常のダイナミック IP アドレスの割り当てから自動的に除外されます。あらかじめ割り当てられたアドレスはホスト プールでは使用できませんが、DHCP アドレス プール単位で複数のアドレスをあらかじめ割り当てることができます。
- DHCP プールからの割り当てを、事前設定された予約だけに制限する（未予約のアドレスはそのクライアントに割り当てられず、他のクライアントにはそのプールから割り当てられない）には、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

DHCP サーバのポートベース アドレス割り当てのイネーブル化

ポートベース アドレス割り当てをグローバルにイネーブルにし、インターフェイス上で加入者識別情報を自動的に生成するには、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	**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	**ip dhcp use subscriber-id client-id**	加入者識別情報をすべての着信 DHCP メッセージでのクライアント識別情報としてグローバルに使用するように、DHCP を設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの省略名に基づいて、加入者識別情報を自動的に生成します。 特定のインターフェイスに設定された加入者識別情報は、このコマンドよりも優先されます。
ステップ 4	**interface** *interface-id*	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 5	**ip dhcp server use subscriber-id client-id**	加入者識別情報をインターフェイス上のすべての着信 DHCP メッセージでのクライアント識別情報として使用するように、DHCP を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（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。

スイッチ上での DHCP ポートベース アドレス割り当てをイネーブルにしたあと、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスをあらかじめ割り当て、これらのアドレスをクライアントに関連付けます。DHCP プールからの割り当てを、事前定義された予約だけに制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスをあらかじめ割り当て、インターフェイス名によって識別されるクライアントに関連付けるには、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	**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	**ip dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名は、シンボリック文字列（Engineering など）または整数（0 など）を使用できます。
ステップ 3	**network** *network-number* [*mask* | */prefix-length*]	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。
ステップ 4	**address** *ip-address* **client-id** *string* [**ascii**]	インターフェイス名によって識別される DHCP クライアントの IP アドレスを予約します。 *string* : ASCII 値または 16 進値
ステップ 5	**reserved-only**	（任意）DHCP アドレス プール内の予約済みアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip dhcp pool**	DHCP プールの設定を確認します。
ステップ 8	**copy running-config startup-config**	（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 ポートベース アドレス割り当てをディセーブルにするには、**no ip dhcp use subscriber-id client-id** 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。加入者識別情報の自動生成をディセーブルにするには、**no ip dhcp subscriber-id interface-name** 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。インターフェイス上の加入者識別情報をディセーブルにするには、**no ip dhcp server use subscriber-id client-id** 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 プールから IP アドレス予約を削除するには、**no address** *ip-address* **client-id** *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限なしに変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者識別情報が自動的に生成され、DHCP サーバは DHCP メッセージ内の任意のクライアント識別情報フィールドを無視し、その代わりに加入者識別情報を使用します。加入者識別情報は、インターフェイスの省略名およびクライアントのあらかじめ割り当てられた IP アドレス 10.1.1.7 に基づいています。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
```

```
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id “Et1/0” ascii
<output truncated>
```

次に、あらかじめ割り当てられたアドレスが DHCP プールに正しく予約された例を示します。

```
switch# show ip dhcp pool dhcppool
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
 Current index   IP address range         Leased/Excluded/Total
 10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
 1 reserved address is currently in the pool
 Address         Client
 10.1.1.7 Et1/0
```

DHCP サーバのポートベース アドレス割り当て機能の設定の詳細については、Cisco.com の検索フィールドで *Cisco IOS IP Addressing Services* と入力し、Cisco IOS ソフトウェアのマニュアルを入手してください。マニュアルは次の URL からも入手できます。
http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバのポートベース アドレス割り当ての表示

表 22-4　DHCP ポートベース アドレス割り当て情報を表示するコマンド

コマンド	目的
show interface *interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバでのアドレス バインディングを表示します。