CHAPTER 23

Dynamic Host Configuration Protocol（DHCP）機能および IP ソース ガード（IPSG）機能の設定

この章では、Catalyst 3750 スイッチに、DHCP スヌーピング機能、Option 82 データ挿入機能、および DHCP サーバのポートベースの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*という用語はスタンドアロン スイッチおよびスイッチ 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 DHCP Command Reference, Volume 1 of 3:Multicast*』Release 12.2 の「DHCP Commands」のセクションを参照してください。これには、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）からアクセス可能です。

この章で説明する内容は、次のとおりです。

DHCP スヌーピングの概要

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。また DHCP は、制限のある IP アドレス空間を節約します。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ためです。

ここでは、次の情報について説明します。

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「*IP Addressing and Services*」セクションにある「*Configuring DHCP*」セクションを参照してください。これには、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]）からアクセス可能です。

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。

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。

- 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 よりも前のソフトウェア 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 ソースガードやダイナミック ARP インスペクションも設定できません。

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。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。

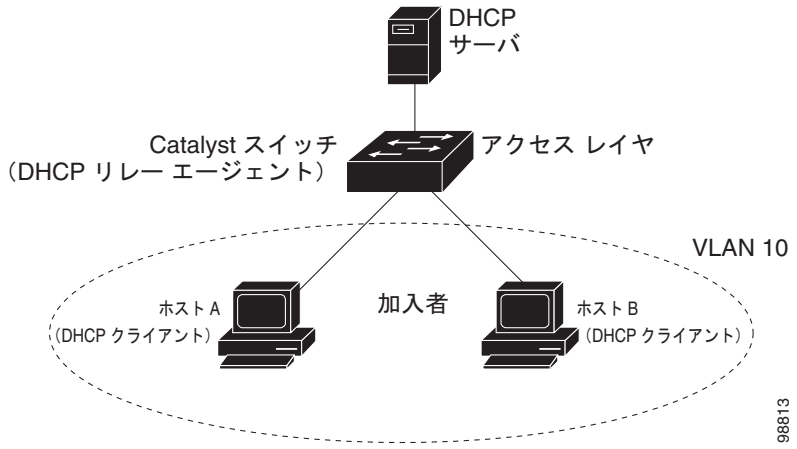
Option 82 データ挿入

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に限り、サポートされます。

図 23-1 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 23-1　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 23-2 にある次のフィールドの値は変化しません。

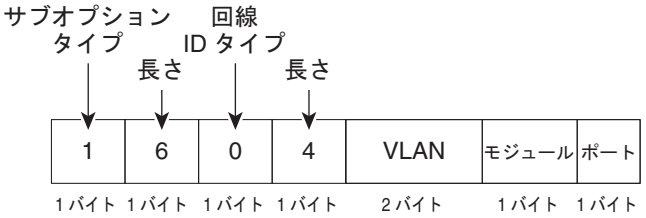
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 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; 着脱可能小型フォーム ファクタ）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 x/0/1 ポート、ポート 4 がファスト イーサネット x/0/2 ポートとなり、以降同様に続きます。x はスタック メンバー番号です。ポート 27 は SFP モジュール スロット x/0/1 となり、以降同様に続きます。

図 23-2 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 23-2　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

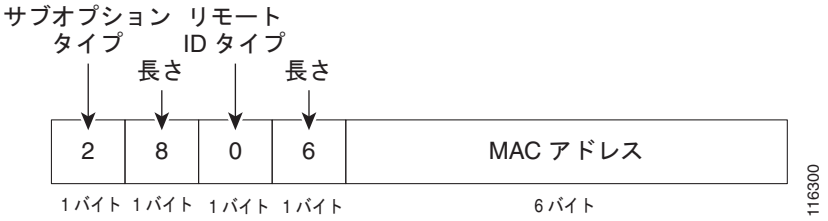


図 23-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力されると、スイッチにより、パケット フォーマットが使用されます。

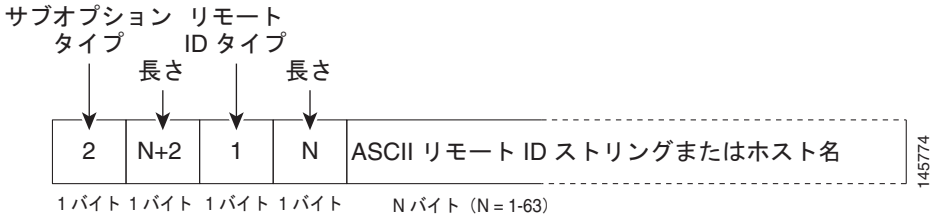
パケット内にあるこれらのフィールドの値は、リモート ID および 回線 ID サブオプションを設定するとデフォルト値から次のように変化します。

- 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 23-3　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。これには、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]）からアクセス可能です。

DHCP スヌーピング バインディング データベース

DHCP スヌーピング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 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 interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 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参加すると、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 バインディングが無効になります。

すべてのスヌーピング統計情報は、スタック マスターで生成されます。新しいスタック マスターが選出されると、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、無効になります。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 スヌーピングの設定

ここでは、次の設定情報について説明します。

DHCP スヌーピングのデフォルト設定

表 23-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 23-1　DHCP スヌーピングのデフォルト設定

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

表 23-1　DHCP スヌーピングのデフォルト設定 （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だけから、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に限り、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に限り、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に限り、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。
- 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 Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）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.7-4）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に限り、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。
- **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。

（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。RSPAN VLAN 上で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN 宛先ポートに到達しないことがあります。

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、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。

これらの手順については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」セクションにある「*Configuring DHCP*」セクションを参照してください。これには、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]）からアクセス可能です。

- リレー エージェント情報の確認（検証）
- リレー エージェントの転送ポリシーの設定

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	**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。

	コマンド	目的
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 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 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*	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。

	コマンド	目的
ステップ 4	**ip dhcp snooping information option**	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。
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。 次のようにリモート ID を設定できます。 • 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してください。
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、フォーマットは **vlan-mod-port** です。 回線 ID を 3 ～ 63 の ASCII 文字（スペースなし）を設定できます。 （任意）登録情報を定義する TLV フォーマットに回線 ID サブオプションを挿入しない場合は **override** キーワードを使用します。
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 DHCP スヌーピングを行う VLAN 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。

	コマンド	目的
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 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の詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「Configuring DHCP」の章にある「DHCP Configuration Task List」セクションを参照してください。これには、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]）からアクセス可能です。

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

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにして設定するには、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*
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 秒です。 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

DHCP スヌーピング情報を表示するには、表 23-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-2　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	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

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、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 ガードを使用することで、ホストがネイバーの IP アドレスを使用しようとする場合の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。IPSG 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）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 テーブルのバインディングは、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）です。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限り 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 ポートに限りサポートされます。IPSG を、送信元 IP アドレス 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。

- 「送信元 IP アドレス フィルタリング」（P.23-18）
- 「送信元 IP および MAC アドレス フィルタリング」（P.23-18）
- 「スタティック ホストの IP ソース ガード」（P.23-18）

送信元 IP アドレス フィルタリング

IPSG 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 IPSG 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 トラフィックは発信元 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。

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 トラフィックおよび非 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。

スタティック ホストの IP ソース ガード

（注）　アップリンク ポートまたはトランク ポートに、スタティック ホストの IPSG（IP ソース ガード）を使用しないでください。

スタティック ホストの IPSG は、IPSG の機能を非 DHCP 環境およびスタティック環境に拡張します。以前の IPSG は、スイッチに接続されたホストの検証に DHCP スヌーピングによって作成されたエントリを使用しました。有効な DHCP バインディング エントリのないホストから受信したトラフィックは破棄されます。このセキュリティ機能は、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します。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します。IPSG の以前のバージョンでは、IPSG が機能するために DHCP 環境が必要でした。

スタティック ホストの IPSG によって DHCP がない場合も IPSG は機能します。スタティック ホストの IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリを利用します。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なエントリを作成し、所定のポートに有効なホストの一覧を維持します。所定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も指定できます。これは、レイヤ 3 ポート セキュリティと等価です。

スタティック ホストの IPSG は、ダイナミック ホストもサポートします。ダイナミック ホストが IP DHCP スヌーピング テーブルで入手できる DHCP 割り当て IP アドレスを受信した場合、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 フェールオーバーが発生すると、メンバー ポートに対応付けられたスタティック ホストの IP ソース ガード エントリが維持されます。**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 テーブルが、ACTIVE としてエントリを表示します。

（注） 複数のネットワーク インターフェイスのある一部の IP ホストでは、無効なパケットをネットワーク インターフェイスに注入することもできます。無効なパケットは、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 アドレスを発信元アドレスとして含みます。無効なパケットが原因になって、スタティック ホストの IPSG がそのホストに接続し、不正な IP または MAC アドレス バインディングを学習し、有効なバインディングを拒否することがあります。ホストによる無効なパケットの挿入を防止するには、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ご相談ください。

スタティック ホストの IPSG は、最初に ACL ベースのスヌーピング メカニズムによって IP または MAC バインディングを動的に学習します。IP または MAC バインディングは、ARP および IP パケットによってスタティック ホストから学習されます。それらは、デバイス トラッキング データベースに保存されます。動的に学習された、または所定のポートに静的に設定された IP アドレスの数が最大値に達したとき、ハードウェアは新しい IP アドレスのあるパケットを破棄します。何らかの理由で移動または削除されたホストを解決するため、スタティック ホストは IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングを無効にします。この機能は、DHCP スヌーピングと共に使用できます。DHCP とスタティック ホストの両方に接続されたポート上に複数のバインディングが確立されます。たとえば、バインディングは DHCP スヌーピング バインディング データベースに加えて、両方のデバイスのトラッキング データベースに保存されます。

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 ポートに限りスタティック 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、インターフェイスのアクセス 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。また、**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 をサポートするように設定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。パケットがサーバからホストに転送される場合、DHCP スヌーピングでは Option 82 の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。
- 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す。
- Ternary Content Addressable Memory（TCAM）エントリ数が最大数を超えた場合、CPU の使用量が増加します。
- 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 コマンドを入力してこのスイッチ設定を削除する場合、インターフェイス スタティック バインディングがバインディング テーブルから削除されます。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** コマンドを入力してスイッチを再びプロビジョニングする場合、バインディングが元に戻されます。バインディングを実行コンフィギュレーションから削除するには、**no switch provision** 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前に IP ソース ガードを無効にしなければいけません。インターフェイスがバインディング テーブルから削除されている間にスイッチをリロードする場合、コンフィギュレーションも削除されます。プロビジョニングされたスイッチの詳細については、「スタックのオフライン設定」（P.5-7）を参照してください。

IP ソース ガードのイネーブル化

特権 EXEC モードで実行します。

	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** または **ip verify source port-security**	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。 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。 （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。 • 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、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 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 ポートでのスタティック 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。ポート上で IP デバイス トラッキングをグローバルにイネーブルに設定することなくこのコマンドだけを設定すると（つまり、該当するインターフェイス上で IP デバイス トラッキング最大数を設定することによって）、スタティック ホストの IPSG は、該当するインターフェイスからのすべての IP トラフィックを拒否します。この要件は、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 IPSG にも適用されます。

特権 EXEC モードで実行します。

	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 テーブルをオンにして、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 と MAC アドレス フィルタリングを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場合は、次の注意事項があります。 • 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。

	コマンド	目的
ステップ 7	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の数の最大限度を設定します。指定できる範囲は 1 ～ 10 です。最大数は 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）このポートのポート 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）このポートの MAC アドレスの最大値を設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ip verify source interface** *interface-id*	設定を確認し、スタティック ホストの IPSG 許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイスの所定のホストのための IP と MAC のバインディングを表示することで設定を確認します。 • **all active**：アクティブな 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**：非アクティブな 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**：アクティブまたは非アクティブの IP または MAC バインディング エントリを表示します。

次に、インターフェイス上のスタティック ホストの IPSG を停止する方法を示します。

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

次に、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方法を示します。

```
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 ポート上のスタティック ホストの IPSG および IP フィルタリングをイネーブルにする方法、および、インターフェイス Gi0/3 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 gigabitethernet 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
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG および IP-MAC フィルタリングをイネーブルにする方法、および、インターフェイス Gi0/3 の有効な IP-MA バインディングを確認し、最大値に到達したインターフェイス上のバインディングの数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 gigabitethernet 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
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Gi0/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Gi0/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Gi0/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Gi0/3      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に対するすべての 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 はすべてのアクティブなエントリおよび非アクティブなエントリを表示します。インターフェイスでホストが学習された場合、新しいエントリはアクティブとしてマークされます。同じホストがそのインターフェイスから接続解除され別のインターフェイスに接続される場合、新しい IP または MAC バインディング エントリは、ホストが検出されるとすぐにアクティブとして表示されます。以前のインターフェイス上のこのホストの古いエントリ非アクティブとしてマークされます。

```
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    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次に、すべてのインターフェイスに対するすべてのアクティブな 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。

```
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    GigabitEthernet0/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/1     ACTIVE
```

次に、すべてのインターフェイスに対するすべての非アクティブな 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。ホストは GigabitEthernet 0/1 上で最初に学習され、次に GigabitEthernet 0/2 に移動されました。GigabitEthernet 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してマークされます。

```
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    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次に、すべてのインターフェイスに対するすべての 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
-----------------------------------------------------------------------
Gi0/3                  5
```

プライベート VLAN ホスト ポートでのスタティック 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。ポート上で IP デバイス トラッキングをグローバルにイネーブルに設定することなくこのコマンドだけを設定すると（つまり、該当するインターフェイス上で IP デバイス トラッキング最大数を設定することによって）、スタティック ホストの IPSG は、該当するインターフェイスからのすべての IP トラフィックを拒否します。この要件は、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG にも適用されます。

レイヤ 2 アクセス ポート上でスタティック ホストの IPSG と IP フィルタリングを設定するには、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	**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**	プライベート VLAN ポートにプライマリ VLAN を設定します。
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**	プライベート VLAN ポートに独立 VLAN を設定します。
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*	コンフィギュレーション VLNA モードを開始します。
ステップ 9	**private-vlan association 201**	独立プライベート VLAN ポートの VLAN を関連付けます。
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。
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）このポートを対応するプライベート VLAN と関連付けます。
ステップ 14	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の数の最大値を設定します。 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]**	このポートのスタティック ホストの IPSG および 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**	コンフィギュレーション インターフェイス 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 許可 ACL を表示します。

次に、スタティック ホストの IPSG と IP フィルタリングをプライベート VLAN ホスト ポートでイネーブルにする方法を示します。

```
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)# int fastEthernet 4/3
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  FastEthernet0/3        ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3        ACTIVE
```

出力は、インターフェイス Fa0/3 で学習された 5 つの有効な IP MAC バインディングを示しています。プライベート VLAN の場合、バインディングはプライマリ VLAN ID と対応付けられています。したがって、この例では、プライマリ VLAN ID、200 が表に示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3      ip trk       active       40.1.1.22                           201
```

出力は、プライマリ VLAN とセカンダリ VLAN の両方に存在する 5 つの有効な IP MAC バインディングを示しています。

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 23-3 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 23-3　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 device tracking	すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリを表示します。
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のアドレス割り当ての概要

DHCP サーバのポートベースのアドレス割り当ては、接続しているデバイス クライアント ID またはクライアント ハードウェアのアドレスにかかわらず、DHCP が 1 つのイーサネット スイッチ ポート上で同じ IP アドレスを保持できるようにする機能です。

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は、直接接続しているデバイスに接続できます。工場の床などの環境によっては、デバイスが故障したときに、代替のデバイスを既存のネットワークで即時に動作させる必要があります。現在の DHCP 実装では、DHCP が代替のデバイスに同じ IP アドレスを提供することは保証されていません。制御ソフトウェア、モニタリング ソフトウェアなどのソフトウェアは、スタティック IP アドレスが各デバイスに関連していることを前提としています。デバイスを交換する場合は、DHCP クライアントが変更されてもアドレス割り当ては固定のままとなる必要があります。

DHCP サーバのポートベースのアドレス割り当て機能を設定すると、ポートに到着する DHCP メッセージのクライアント ID またはクライアント ハードウェアのアドレスが変わっても、同じ IP アドレスが同じ接続ポートに常に提供されるようになります。DHCP プロトコルは DHCP パケットのクライアント ID オプションによって DHCP クライアントを認識します。クライアント ID オプションを持たないクライアントは、クライアント ハードウェアのアドレスによって特定されます。この機能を設定すると、インターフェイスのポート名によってクライアント ID またはハードウェア アドレスは無効になり、実際の接続ポイント、スイッチ ポートがクライアント ID となります。

どのような場合であっても、同じポートにイーサネット ケーブルを接続することで、DHCP によって同じ IP アドレスが接続しているデバイスに割り当てられます。

DHCP サーバのポートベースのアドレス割り当て機能は、Cisco IOS DHCP サーバに限りサポートされ、サードパーティ製のサーバではサポートされません。

DHCP サーバのポートベースのアドレス割り当ての設定

ここでは、次の設定情報について説明します。

- 「ポートベースのアドレス割り当てのデフォルト設定」（P.23-28）
- 「ポートベースのアドレス割り当ての設定時の注意事項」（P.23-28）
- 「DHCP サーバのポートベースのアドレス割り当てのイネーブル化」（P.23-29）

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、DHCP サーバのポートベースのアドレス割り当てはディセーブルです。

ポートベースのアドレス割り当ての設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当ての設定時の注意事項について説明します。

- ポートごとに、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（事前に割り当てられた）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もクリアできません。
- 事前に割り当てられたアドレスは、通常のダイナミック IP アドレス割り当てから自動的に除外されます。事前に割り当てられたアドレスはホスト プールで使用できませんが、DHCP アドレス プールごとに複数のアドレスを事前に割り当てることができます。

- DHCP プールから予約済みのアドレスへの割り当てを制限するには（予約済みでないアドレスはクライアントには提供されず、その他のクライアントはプールから供給されません）、**reserved-only** 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。

DHCP サーバのポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルでイネーブルにし、インターフェイスで加入者 ID 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**	すべての着信 DHCP メッセージにおいて、加入者 ID をクライアント ID としてグローバルで使用するように DHCP サーバを設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの略称に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドより優先されます。
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**	インターフェイス上のすべての着信 DHCP メッセージにおいて、加入者 ID をクライアント ID として使用するように DHCP サーバを設定します。
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。

DHCP ポートベースのアドレス割り当てをスイッチでイネーブルにしてから、**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 アドレスを事前に割り当てて、それをクライアントに関連付けます。DHCP プールから予約済みのアドレスへの割り当てを制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。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 アドレスを事前に割り当てて、それをインターフェイス名によって特定された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。プール名には、文字列（例：Engineering）または整数（例：0）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特定される 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 進数値を設定できます。
ステップ 5	**reserved-only**	（任意）DHCP アドレス プール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 ポートベースの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 ID 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。インターフェイスで加入者 ID 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 アドレスの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 プールを制限されない状態に変更するには、**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 ID が自動的に生成され、DHCP サーバは DHCP メッセージのクライアント ID フィールドを無視して、その代わりに加入者 ID を使用します。加入者 ID は、インターフェイスの略称および事前に割り当てられたクライアント IP アドレス 10.1.1.7 に基づいて決定されます。

```
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、事前に割り当てられたアドレスが DHCP プールで正しく予約されている例を示します。

```
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のアドレス割り当て機能の設定の詳細については、Cisco.com にアクセスして検索フィールドに *Cisco IOS IP Addressing Services* と入力して Cisco IOS ソフトウェア マニュアルを参照してください。マニュアルには次の URL からもアクセスできます。

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のアドレス割り当ての表示

DHCP サーバのポートベースのアドレス割り当て情報を表示するには、表 23-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-4　DHCP サーバのポートベースのアドレス割り当て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 サーバのアドレス バインディングを表示します。