CHAPTER 22

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

この章では、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 アドレス割り当て機能を設定する手順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。特に記述がない限り、*スイッチ*という用語はスタンドアロン スイッチとスイッチ スタックを意味しています。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』の「DHCP Commands」を参照してください。

この章で説明する内容は、次のとおりです。

DHCP 機能の概要

DHCP は、中央集中型サーバからホスト IP アドレスをダイナミック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。

- 「Option 82 データ挿入」（P.22-3）
- 「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は、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「*IP Addressing and Services*」にある「*Configuring DHCP*」を参照してください。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上にある特定のアドレス プールから IP アドレスを DHCP クライアントに割り当て、管理します。DHCP サーバが DHCP クライアントによって要求された設定パラメータを、データベースから提供できない場合、その要求は、ネットワーク管理者によって定義された 1 つ以上のセカンダリ 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 メッセージを受信し、新しい DHCP メッセージを生成して出力インターフェイスで送信します。

DHCP スヌーピング

DHCP スヌーピングとは、untrusted（信頼できない）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（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 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、スイッチのローカル 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い場合、スイッチはパケットをドロップします。

次のいずれか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ため、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。

集約スイッチを信頼できないインターフェイスを介してエッジ スイッチに接続でき、**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、集約スイッチはエッジ スイッチから Option 82 情報を持ったパケットを受け付けます。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。ダイナミック ARP インスペクションまたは IP ソース ガードなどの DHCP セキュリティ機能は、ホストが接続されている信頼できない入力インターフェイスで Option 82 情報を持ったパケットをスイッチが受信している間でも、集約スイッチ上で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。

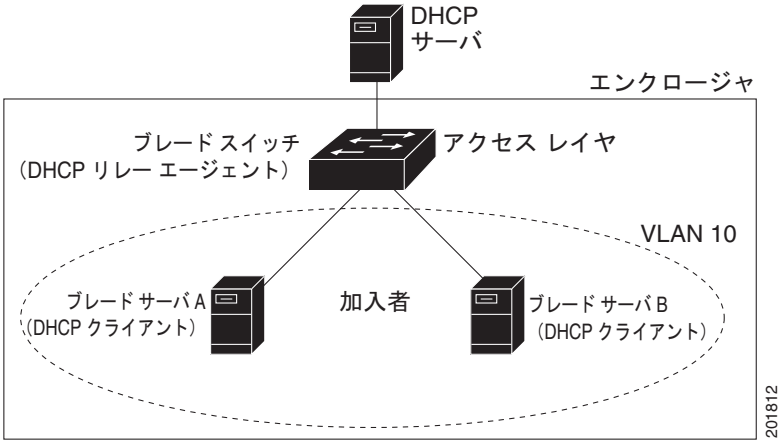
Option 82 データ挿入

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。アクセス スイッチの同じポート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者デバイスが割り当てられている VLAN にある場合に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エンクロージャのブレード スイッチの例を示します。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（ブレード 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



スイッチで 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。

- ブレード サーバ（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。
- ブレード 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 サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションは、パケットの受信ポートの ID である **vlan-mod-port** です。リモート ID と回線 ID を設定することができます。これらのサブオプションの設定については、「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。
- ブレード スイッチは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバ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装します。また、DHCP サーバは、DHCP 応答に含まれる Option 82 フィールドをエコーします。
- ブレード スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチでは、リモート ID あるいは回線 ID フィールドを調べて、自分が挿入した Option 82 データであることを確認します。スイッチは、Option 82 フィールドを削除し、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、前述の一連のイベントが発生したときに、図 22-2 にある次のフィールドの値は変更されません。

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

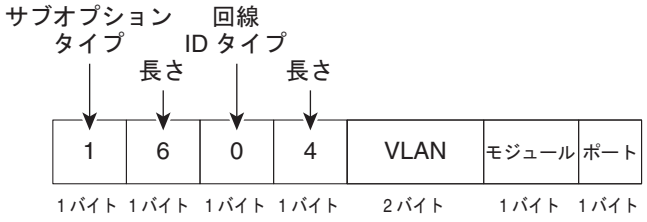
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 1 から始まります。たとえば、ポートが 15 ある Catalyst Switch Module 3110X では、ポート 1 が内部 GigabitEthernet 1/0/1 ポート、ポート 2 が内部 GigabitEthernet 1/0/2 ポートなどのようになります。ポート 15 は 10 GigabitEthernet 1/0/15 ポートです。

図 22-2 に、デフォルト サブオプション設定が使用される場合のリモート 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形式を示します。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た場合に、このパケット形式を使用します。

図 22-2　　サブオプション パケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

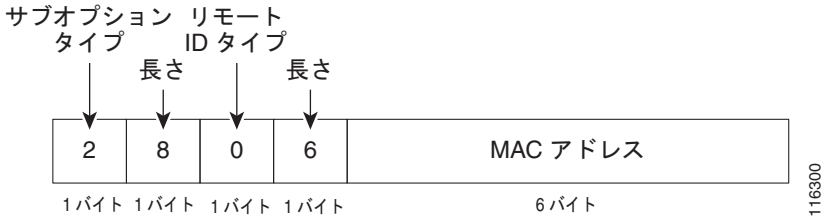


図 22-3 は、ユーザ設定のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチで次のパケット フォーマットが使用されます。

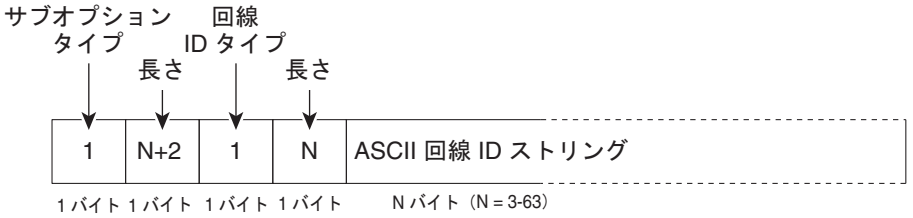
パケット内にあるこれらのフィールドの値は、リモート ID および回線 ID サブオプションを設定するとデフォルト値から次のように変化します。

- 回線 ID サブオプション フィールド

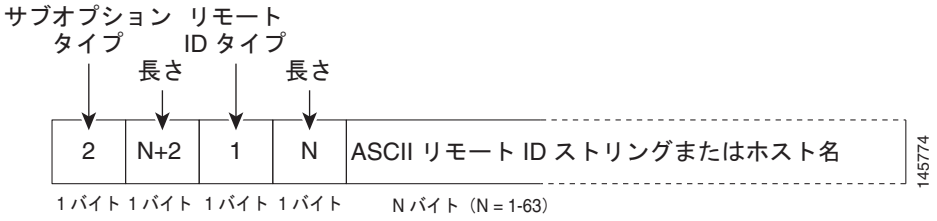
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定したストリングの長さによります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定したストリングの長さによります。

図 22-3　ユーザ設定サブオプション パケット形式

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。

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、8192 のバインディングを含めることができます。

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、その後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であり、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は、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である場合は、スイッチの接続は切断されませんが、DHCP スヌーピングが DHCP スプーフィング攻撃を防止できない場合があります。

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アップデートします。

スイッチが新しいバインディングを学習したり、バインディングを消失した場合には、スイッチはデータベース内のエントリを迅速にアップデートします。スイッチは、バインディング ファイル内のエントリもアップデートします。ファイルをアップデートする頻度は、設定可能な遅延に基づいてアップデートされ、アップデート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）でファイルがアップデートされない場合、アップデートは中止されます。

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 アップデートに関連したエントリを、前のファイル アップデート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のメンバーになると、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け取ります。メンバーがスイッチから離れると、すべての DHCP スヌーピングは、スイッチ エージング アウトに関連するバインディングに対応します。

すべてのスヌーピング統計情報が、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た場合、統計カウンタはリセットされます。

スタック マージが発生すると、スタック マスターのすべての DHCP スヌーピング バインディングは、スタック マスターであっても失われます。スタック パーティションでは、既存のスタック マスターは変更されず、分割スイッチに属するバインディングはエージング アウトします。分割スタックの新しいマスターが、新しい着信 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 7 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

ここでは、次の設定情報について説明します。

DHCP のデフォルト設定

表 22-1 に、DHCP のデフォルト設定を示します。

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 ソフトウェアではイネーブル（設定が必要です）[1]
DHCP リレー エージェント	イネーブル[2]

表 22-1　DHCP のデフォルト設定（続き）

機能	デフォルト設定
DHCP パケット転送アドレス	設定なし
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
DHCP スヌーピング情報オプション	イネーブル
信頼できない入力インターフェイスでパケットを受け付ける 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	設定なし
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（設定が必要です） **（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（設定が必要です）この機能が有効なのは、宛先が設定されている場合だけです。

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 クライアントのスイッチ仮想インターフェイス（SVI）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

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。
- 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。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、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ため、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）サーバにストア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 の設定」（P.5-4）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 と同期化されたときにだけ、スイッチがバインディングの変更内容を書き込みます。
- 信頼できないデバイスが接続されたアグリゲーション 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、信頼できないデバイスが Option 82 情報をスプーフィングする可能性があります。
- Cisco IOS Release 12.2(37)SE 以降のリリースでは、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示できます。また、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報カウンタをクリアできます。
- RSPAN VLAN 上では Dynamic Host Configuration Protocol（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場合があります。

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場合の手順については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」の章にある「Configuring DHCP」を参照してください。

DHCP サーバおよびスイッチ スタック

DHCP バインディング データベースはスタック 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と、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 マスターで障害が発生すると、保存されていないすべてのバインディングが失われます。失われたバインディングに関連付けられている IP アドレスは解放されます。自動バックアップを設定するには、**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ください。

スタック マージが発生すると、スタック メンバーになるスタック マスターは、すべての DHCP リース バインディングを失います。スタック パーティションでは、パーティションの新しいマスターは、既存の DHCP リース バインディングのない新しい DHCP サーバとして機能します。

スイッチ スタックの詳細については、第 7 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 12.2*』の「IP Addressing and Services」にある「*Configuring DHCP*」の部分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 を入力しスイッチ仮想インターフェイスを作成して、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 レンジ コンフィギュレーション モードを開始します。
ステップ 7	**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 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 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力できます。これらはスペースで区切ります。
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 DHCP 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。これは、デフォルト設定です。
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。 デフォルト設定はディセーブルです。 **（注）** 集約スイッチが信頼できるデバイスに接続されている場合にだけ、このコマンドを入力します。
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。 VLAN およびポートの ID を、1 ～ 4094 の範囲の VLAN ID を使用して指定します。デフォルトの回線 ID は、**vlan-mod-port** という形式のポート ID 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）加入者情報を定義するために 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、**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。デフォルト設定は untrusted です。

	コマンド	目的
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毎秒ごとの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されていません。 **（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）信頼できない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 12.2*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」を参照してください。

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

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

	コマンド	目的
ステップ 1	**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 メンバー数を指定するには *number* パラメータを使用します。*number* の範囲は 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*	データベース転送プロセスを打ち切るまでの時間（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。無期限の期間を定義するには、0 を使用します。これは、転送を無期限に続け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。

	コマンド	目的
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。指定できる *vlan-id* 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）**　このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 7	**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 22-2 の特権 EXEC コマンドを 1 つ以上使用します。

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	バインディング テーブルとも呼ばれる DHCP スヌーピング バインディング データベースの中から、ダイナミック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 ステートに変更された場合、静的に設定されたバインディングは削除されません。

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 ガードを使用して、ホストがネイバーの IP アドレスを使用しようとすることによるトラフィック攻撃を回避できます。

DHCP スヌーピングが信頼できないインターフェイスでイネーブルの場合に IP ソース ガードをイネーブルにできます。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; 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するルータ ACL や VLAN マップに優先します。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルの場合にだけ 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 ポートだけでサポートされます。IPSG を、送信元 IP フィルタリングや送信元 IP および MAC アドレス フィルタリングとともに設定できます。

- 「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.22-17）
- 「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 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。送信元 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 スヌーピングでダイナミック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、送信元 IP 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だけ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 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場合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 は、アップリンク ポートまたはトランク ポートでは使用しないでください。

スタティック ホストの IPSG は、IPSG 機能を非 DHCP およびスタティック環境に拡張します。以前の IPSG は、DHCP スヌーピングにより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を検証していました。有効な DHCP バインディング エントリ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は、非ルーテッド レイヤ 2 インターフェイスの IP トラフィックを制限します。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、および手動で設定された IP 発信元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。以前のバージョンの IPSG では、IPSG を使用するために DHCP 環境が必要でした。

スタティック ホストの IPSG では、DHCP なしで IPSG を使用できます。スタティック ホストの IPSG は、IP デバイス トラッキング テーブル エントリに依存して、ポート ACL をインストールします。スイッチは、ARP 要求または他の 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、特定のポートの有効なホストのリストを保守します。特定のポートにトラフィックを送信できるホストの数を指定することもできます。これは、レイヤ 3 でのポート セキュリティに相当します。

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 テーブルで使用できる DHCP により割り当てられた IP アドレスを受信すると、同じエントリが IP デバイス トラッキング テーブルで学習されます。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 ポートに接続されているスタティック 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場合、IP デバイス トラッキング テーブルでエントリが ACTIVE として表示されます。

（注）　複数ネットワーク インターフェイスを持つ一部の IP ホストは、一部の無効パケットをネットワーク インターフェイスに投入することがあります。これらの無効パケットには、送信元アドレスとしてのホストの別のネットワーク インターフェイスの IP または MAC アドレスを含みます。これにより、ホストに接続しているスタティック ホストの IPSG が、無効な 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します。無効パケットの投入を回避するには、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相談してください。

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 メカニズムを介してダイナミックに IP と MAC のバインディングを学習します。IP または MAC のバインディングは、ARP および IP パケットを経由してスタティック ホストから学習され、デバイス トラッキング データベースを使用して保存されます。指定ポートでダイナミックに学習された、またはスタティックに設定された IP アドレスの数が最大限度に達すると、新しい IP アドレスを持つパケットはハードウェアでドロップされます。何らかの理由で移動されたまたは消去されたホストを扱うために、スタティック ホストの IPSG は IP デバイス トラッキングを使用して、ダイナミックに学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングと同時に使用できます。複数のバインディング

が、DHCP とスタティック ホストの両方に接続されているポート上で確立されます たとえば、バインディングは、デバイス トラッキング データベースだけでなく、DHCP スヌーピング バインディング データベースにも保存されます。

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

IP ソース ガードの設定時の注意事項は次のとおりです。

- 非ルーテッド ポートでだけスタティック 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でイネーブルの場合、DHCP スヌーピングは、インターフェイスが属するアクセス VLAN でイネーブルでなければなりません。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードがイネーブルで、DHCP スヌーピングがすべての VLAN でイネーブルの場合、送信元 IP アドレス フィルタがすべての VLAN に適用されます。

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

- IP ソース ガードと送信元 IP および MAC アドレス フィルタリングがイネーブルの場合、DHCP スヌーピングおよびポート セキュリティがインターフェイスでイネーブルでなければなりません。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。
- IEEE 802.1x ポートベース認証がイネーブルである場合、IP ソース ガードの機能をイネーブルにできます。

- 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 インターフェイスで設定されていて、**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そのスイッチのコンフィギュレーションを削除する場合、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** コマンドを使用して再びスイッチをプロビジョニングすると、バインディングが復元されます。

  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** 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。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るときにスイッチがリロードすると、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、第 7 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** 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したときは、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*]	すべてのインターフェイスまたは特定のインターフェイスに対して IP ソース ガード設定を表示します。

	コマンド	目的
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 ホストを使用するには、IPSG で **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。IP デバイス トラッキングをグローバルにイネーブルにせずに、またはそのインターフェイスで最大 IP デバイス トラッキングを設定して、このコマンドをポートだけで設定する場合、スタティック ホストを使用する IPSG は、その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 ポートのスタティック ホストを使用する IPSG にも適用されます。

特権 EXEC モードを開始します。

	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。

	コマンド	目的
ステップ 2	**ip device tracking**	IP ホスト テーブルを有効にして、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**	MAC アドレス フィルタリングでスタティック ホストの IPSG 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したときは、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。
ステップ 7	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポートで許可するスタティック IP の最大制限数を指定します。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 アドレスの最大数を指定します。
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*	設定を確認して、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特定のホストの IP および MAC のバインディングを表示して、設定を表示します。 • **all active**：アクティブ 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 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 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でスタティック ホストを使用する 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、ポート上でスタティック ホストを使用する 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 ポートで IP フィルタリングを使用しスタティック ホストの IPSG をイネーブルにして、インターフェイス Gi1/0/3 で有効な 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 ポートで IP-MAC フィルタリングを使用しスタティック ホストの IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP-MAC バインディングを確認して、このインターフェイスのバインディング数が最大数に達していること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
---------  -----------  -----------  ---------------  -----------------  ----
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 は、アクティブおよび非アクティブのすべてのエントリを表示します。ホストがインターフェイスで学習されると、新しいエントリはアクティブとマーキングされます。同じホストがインターフェイスから切断され、別のインターフェイスに接続される場合、ホストが検出されるとすぐに、新しい IP または MAC バインディング エントリが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でのこのホストの古いエントリは INACTIVE とマーキングされます。

```
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のすべてのアクティブ 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のすべての非アクティブ 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。このホストは、まず GigabitEthernet 1/0/1 で学習されてから、GigabitEthernet 1/0/2 に移動します。GigabitEthernet1/ 0/1 で学習された IP または MAC バインディング エントリには非アクティブとマーキングされます。

```
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    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 ホストを使用するには、IPSG で **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。IP デバイス トラッキングをグローバルにイネーブルにせずに、またはそのインターフェイスで最大 IP デバイス トラッキングを設定して、このコマンドをポートだけで設定する場合、スタティック ホストを使用する IPSG は、その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 ポートのスタティック ホストを使用する IPSG にも適用されます。

レイヤ 2 アクセス ポートで IP フィルタリングを使用してスタティック ホストの IPSG 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 ポートでプライマリ VLAN を確立します。
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 のコンフィギュレーション VLAN モードを開始します。
ステップ 6	**private-vlan isolated**	プライベート VLAN ポートで独立 VLAN を確立します。
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 VLAN 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 ホストとして確立します。
ステップ 13	**switchport private-vlan host-association** *vlan-id1 vlan-id2*	（任意）対応するプライベート VLAN とこのポートを関連付けます。

	コマンド	目的
ステップ 14	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポートで許可するスタティック IP の最大数を指定します。 最大数は 10 です。 （注）　スタティック ホストを使用するには、IPSG で **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]**	このポートで MAC アドレス フィルタリングを使用するスタティック ホストの IPSG 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、プライベート VLAN ホスト ポートで IP フィルタリングを使用してスタティック ホストの IPSG をイネーブルにする例を示します。

```
Switch(config)# 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 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
```

出力は、インターフェイス GigabitEthernet 1/0/3 で 5 つの有効な IP と MAC のバインディングが学習されたことを示しています。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 に関連付けられます。そのため、この例では、プライマリ VLAN ID、200 がテーブルに示されています。

```
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
```

出力は、プライマリおよびセカンダリの両方の VLAN に 5 つの有効な IP と MAC のバインディングがあることを示しています。

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 22-3 に示す、1 つ以上の特権 EXEC コマンドを使用します。

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 アドレス割り当て機能により、DHCP は接続されているデバイスのクライアント ID またはクライアントのハードウェア アドレスに関わらず、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ことができます。

イーサネット スイッチがネットワーク内に配置されている場合、スイッチは直接接続されたデバイスとの接続を提供します。工場現場など一部の環境では、デバイスに障害が発生した場合、代替デバイスが既存ネットワークで即座に稼動する必要があります。現在の DHCP 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という保証はありません。コントロール、モニタリング、およびその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 アドレスを期待します。デバイスが交換された場合、DHCP クライアントが変更されたとしてもアドレス割り当ては安定性を維持する必要があります。

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ると、ポート上で受信される 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 アドレスが変更された場合でも、同じ接続先ポートには常に同じ IP アドレスを供給できます。DHCP プロトコルでは、DHCP パケット内のクライアント ID 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 ID オプションを含まないクライアントの場合、クライアント ハードウェア アドレスにより識別されます。この機能が設定されている場合、インターフェイスのポート名によりクライアント ID またはハードウェア アドレスが上書きされ、実際の接続ポイントであるスイッチ ポートがクライアント ID となります。

いかなる場合でも、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、DHCP を経由して同じ IP アドレスが接続先デバイスに割り当てられます。

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 サーバでだけサポートされ、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 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 アドレス割り当てのデフォルト設定」（P.22-28）
- 「ポートベース アドレス割り当ての設定時の注意事項」（P.22-28）
- 「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」（P.22-28）

ポートベース 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に設定されています。

ポートベース アドレス割り当ての設定時の注意事項

DHCP ポートベース アドレス割り当ての設定時の注意事項は、次のとおりです。

- IP アドレスは、ポートごとに 1 つだけ割り当てることができます。
- 予約されたアドレス（事前割り当てされる）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クリアすることはできません。
- 事前割り当てされたアドレスは、通常のダイナミック IP アドレス割り当てから自動的に排除されます。ホスト プールでは事前割り当てされたアドレスを使用できませんが、DHCP アドレス プールごとに複数のアドレスが事前割り当てされます。
- DHCP プールからの割り当てを事前に設定されている予約数まで制限するには（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プールのサービスが提供されません）、**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 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に加入者 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 メッセージのクライアント ID として加入者 ID をグローバルに使用するように、DHCP サーバを設定します。

	コマンド	目的
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスのショート ネームに基づいて、自動的に加入者 ID を生成します。 特定のインターフェイスで設定される加入者 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 メッセージのクライアント ID として加入者 ID を使用するように、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。

スイッチ上で 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 アドレスを事前割り当てし、これら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に設定されている予約数まで制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを使用する必要します。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。

事前割り当てした IP アドレスを、インターフェイス名によって特定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 モードを開始して、DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
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 ネットワーク番号および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り識別される 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 進値を使用できます。
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 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。インターフェイス上の加入者 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 アドレス予約を解除するには、**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 プールを無制限に変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。

この例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージ内のすべてのクライアント ID フィールドを無視する代わりに、この加入者 ID を使用します。加入者 ID は、インターフェイスのショート ネームおよびクライアントに事前割り当てされた 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、事前割り当てされたアドレスが DHCP プールで適切に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詳細については、Cisco.com の、Serch フィールドの *Cisco IOS IP Addressing Services* から、Cisco IOS ソフトウェア マニュアル参照してください。この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 アドレス割り当ての表示

DHCP サーバのポートベース アドレス割り当て情報を表示するには、表 22-4 の特権 EXEC コマンドを 1 つ以上使用します。

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 サーバのアドレス バインディングを表示します。