CHAPTER 26

DHCP 機能と IP ソース ガード機能の設定

この章では、IE 3000 スイッチに、DHCP スヌーピング機能、DHCP 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についても説明します。

（注）この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*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 スヌーピングの概要

DHCP は、中央のサーバからホストの IP アドレスをダイナミックに割り当てるために、LAN 環境で広範に使用されている機能です。この機能により、IP アドレス管理のオーバーヘッドを大幅に軽減できます。また、DHCP を使用すると、IP アドレスをホストに永続的に割り当てる必要がなくなり、ネットワークに接続しているホストだけが IP アドレスを使用するようになるので、限られた IP アドレス空間を節約するのに役立ちます。

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.26-3）
- 「Cisco IOS DHCP サーバ データベース」（P.26-6）
- 「DHCP スヌーピング バインディング データベース」（P.26-7）

DHCP クライアントの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「*IP Addressing and Services*」の「*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にある指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理します。DHCP サーバが要求された設定パラメータをデータベースから DHCP クライアントに付与できない場合、その要求は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに転送されます。

DHCP リレー エージェント

DHCP リレー エージェントは、DHCP パケットをクライアントとサーバの間で転送するレイヤ 3 装置です。リレー エージェントは、クライアントとサーバが同じ物理サブネット上にない場合に、両者の間で要求と応答の転送を行います。リレー エージェント転送は、IP データグラムがネットワークの間でトランスペアレントにスイッチングされる通常のレイヤ 2 転送とは異なります。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 スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、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 バインディング テーブルとも呼ばれる）を構築および維持することでネットワーク セキュリティを実現するセキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間のファイアウォールのように機能します。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信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続された、信頼できるインターフェイスとを差別化できます。

（注）　DHCP スヌーピングが正しく機能するには、すべての DHCP サーバが、信頼できるインターフェイスを介してスイッチに接続されている必要があります。

信頼できない 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。DHCP スヌーピングをサービス プロバイダー環境で使用する場合は、信頼できないメッセージは、サービス プロバイダー ネットワーク内には存在しない装置（カスタマーのスイッチなど）から送信されたものです。不明な装置からのメッセージは、この装置がトラフィック攻撃の起点である可能性もあるため、信頼できません。

DHCP スヌーピング バインディング データベースには、Media Access Control（MAC; メディア アクセス制御）アドレス、IP アドレス、リース期間、バインディングの種類、virtual LAN（VLAN; LAN）番号、およびインターフェイス情報が保存されます。インターフェイス情報は、スイッチの信頼できないローカル インターフェイスに対応する情報です。これには、信頼できるインターフェイスに相互接続しているホストに関する情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスは、同じネットワーク内にある装置のポートに接続されています。信頼できないインターフェイスは、ネットワーク内の信頼できないインターフェイス、またはネットワーク内には存在しない装置のインターフェイスに接続されています。

スイッチが信頼できないインターフェイス上でパケットを受信し、このインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルにされている場合、スイッチは送信元 MAC アドレスを DHCP クライアント ハードウェアのアドレスと比較します。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廃棄します。

スイッチは、次のような状況が発生した場合に DHCP パケットを廃棄します。

- ネットワークまたはファイアウォール外部の DHCP サーバから、DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY などのパケットを受信した場合。
- 信頼できないインターフェイスでパケットを受信し、送信元 MAC アドレスと 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 データベース内の MAC アドレスを持つ DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信したが、バインディング データベース内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- DHCP リレー エージェントが 0.0.0.0 でないリレー エージェント IP アドレスが含まれる DHCP パケットを転送するか、またはリレー エージェントが Option 82 情報が含まれるパケットを信頼できないポートに転送する場合。

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あり、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、スイッチは、信頼できないインターフェイスでパケットを受信すると、Option 82 情報を含むパケットを廃棄します。DHCP スヌーピングがイネーブルで、信頼できるポートでパケットを受信した場合、集約スイッチは、接続先装置の DHCP スヌーピング バインディングを学習せず、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。

信頼できないインターフェイスを介して集約スイッチをエッジ スイッチに接続できる場合、**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と、集約スイッチはエッジ スイッチから Option 82 情報を含むパケットを受け付けます。集約スイッチは信頼できないスイッチ 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 Address Resolution Protocol（ARP; アドレス解決プロトコル）検査や IP ソース ガードなどの DHCP セキュリティ機能は、スイッチが、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 情報を含むパケットを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るエッジ スイッチ上のポートは、信頼できるインターフェイスとして設定する必要があります。

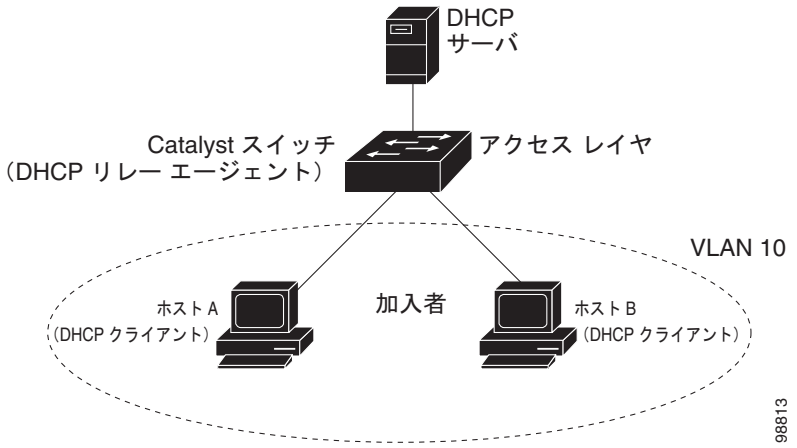
Option 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、この装置をネットワークに接続するスイッチ ポートによっても識別されます。加入者 LAN 上の複数のホストをアクセス スイッチの同一ポートに接続でき、これらは一意に識別されます。

（注）　Option 82 機能は、この機能を使用する加入者の装置が割り当てられている VLAN で DHCP スヌーピングがグローバルにイネーブルになっている場合だけサポートされます。

図 26-1 は、メトロポリタン イーサネット ネットワーク内において、アクセス レイヤのスイッチに接続されている各加入者の IP アドレスを、一元的な DHCP サーバが割り当てる例を示しています。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェント（Catalyst スイッチ）をヘルパー アドレスによって設定することで、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で DHCP メッセージを転送します。

図 26-1　メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報の 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、これをネットワーク上にブロードキャストします。
- スイッチはこの DHCP 要求を受信すると、パケット内に 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、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 DHCP パケット内にこの IP アドレスを追加します。
- スイッチは、オプション 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は、リモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシー（単一のリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するなど）の実装を行うことができます。また、DHCP サーバは、DHCP 応答に含まれるオプション 82 フィールドをエコーします。
- 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。スイッチは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データが挿入されていることを確認します。スイッチは、オプション 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、上記の一連のイベントが発生したときに、図 26-2 にある次のフィールドの値は変更されません。

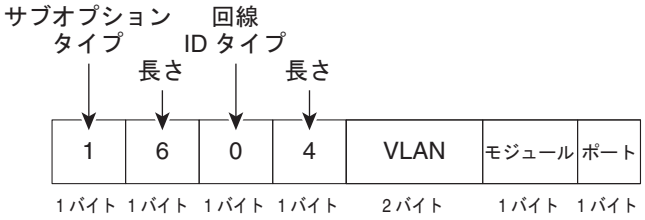
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、8 つの 10/100 ポートと Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュール スロットを備えたスイッチでは、ポート 3 が Fast Ethernet 1/1 ポート、ポート 4 が Fast Ethernet 1/2 ポートなどのようになります。ポート 11 は SFP モジュール スロット 1/1 などになります。

図 26-2 に、デフォルト設定のリモート 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。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 26-2　サブオプションのパケット形式

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

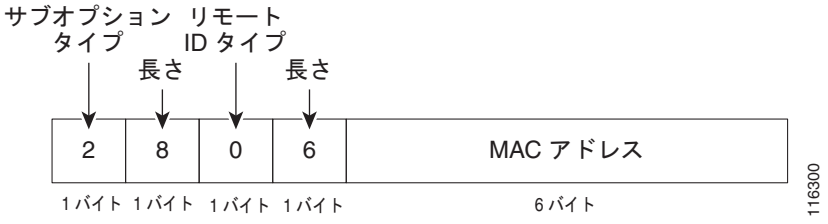


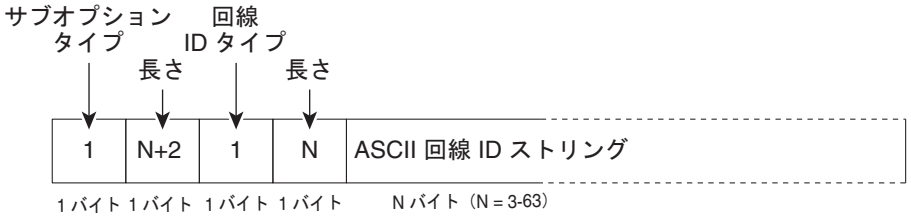
図 26-3 に、ユーザ設定のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドと **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力された場合に、このパケット形式を使用します。

リモート ID サブオプションと回線 ID サブオプションを設定すると、パケットの次のフィールドの値がデフォルト値から変更されます。

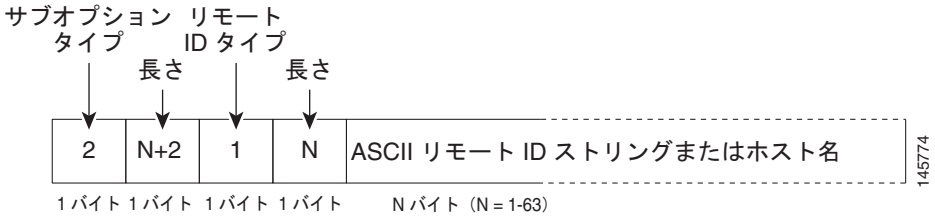
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。

図 26-3　ユーザ設定サブオプションのパケット形式

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、指定された DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。このデータベースには、IP アドレス、*アドレス バインディング*、ブート ファイルなどの設定パラメータが格納されています。

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 アドレスは手動で割り当てることも、DHCP サーバを使用して DHCP アドレス プールから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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』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（*バインディング*）には、IP アドレス、関連付けられた MAC アドレス、リース時間（16 進数形式）、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 が含まれます。データベース エージェントは、設定された場所の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示されるチェックサムは、ファイルの冒頭から、エントリに関連付けられたすべてのバイトの合計に基づいて計算されます。各エントリは 72 バイトで、そのあとにスペースとチェックサム値が続きます。

スイッチがリロードされたときにバインディングを維持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP 検査または IP ソース ガードがイネーブルであり、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 DCHP スプーフィング攻撃を防止できないことがあります。

リロード時に、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にバインディング ファイルを読み込みます。スイッチは、データベースの変更時にファイルを更新します。

スイッチは、新しいバインディングを学習した場合や、バインディングを消失した場合には、データベース内のエントリを更新します。スイッチはまた、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決定され、更新はバッチ処理されます。ファイルが（write-delay および abort-timeout 値によって設定された）指定の時間に更新されない場合は、更新が停止します。

バインディングを含む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には、スイッチがファイルを読み込んだときにエントリの確認に使用するチェックサム値がタグ付けされます。1 行めの *initial-checksum* エントリは、最新のファイル更新に関連するエントリと前のファイル更新に関連するエントリを区別します。

次に、バインディング ファイルの例を示します。

```
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、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、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。そのエントリとそのあとのエントリが無視されます。
- エントリに期限切れのリース時間がある場合（リース時間が期限切れになっても、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 インターフェイスまたは DHCP スヌーピングの信頼できるインターフェイスの場合。

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 26-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 26-1　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。設定が必要です。[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	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廃棄されます）。[2]
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置き換えます。[2]
グローバルにイネーブルにされる DHCP スヌーピング	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 レート制限	設定なし。
DHCP スヌーピング信頼状態	信頼しない。
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。

表 26-1　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
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装置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 ソフトウェアでイネーブル。設定が必要です。この機能は、宛先が設定されている場合にだけ使用できます。

1. スイッチは、DHCP サーバとして設定されている場合にだけ DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上に設定されている場合にだけ DHCP パケットをリレーします。
3. この機能は、スイッチがエッジ スイッチから Option 82 情報を含む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を説明します。

- スイッチで DHCP スヌーピングをグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN 上で DHCP スヌーピングをイネーブルにしない限りアクティブになりません。
- スイッチで DHCP スヌーピングをグローバルにイネーブルにするには、DHCP サーバおよび DHCP リレー エージェントとして機能する装置を、事前に設定してイネーブルにしておく必要があります。
- スイッチに DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能する装置を必ず設定してください。たとえば、DHCP サーバによる割り当てまたは除外が可能な IP アドレスを指定したり、装置に DHCP オプションを設定したりする必要があります。
- スイッチに多数の回線 ID を設定する場合は、長い文字列が NVRAM またはフラッシュ メモリに与える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装置を必ず設定してください。たとえば、DHCP サーバによる割り当てまたは除外が可能な IP アドレスを指定したり、装置に DHCP オプションを設定したり、データベース エージェントを設定したり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も、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 ポートが DHCP サーバに接続されている場合は、**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、ポートを信頼できるポートとして設定します。
- スイッチ ポートが DHCP クライアントに接続されている場合は、**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、ポートを信頼できないポートとして設定します。
- 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は、次の注意事項に従ってください。
  - NVRAM とフラッシュ メモリの両方のストレージ容量には限りがあるため、バインディング ファイルを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上に保存することを推奨します。

  - ネットワークベースの URL（TFTP や FTP など）の場合、設定した URL のバインディング ファイルにスイッチがバインディングを書き込めるようにするには、その URL に空のファイルを作成する必要があります。最初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、使用している 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、この方法で設定できません。
  - データベース内のリース時間を正確な時間にするには、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.7-3）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。

- 信頼できない装置が接続された集約スイッチに **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、信頼できない装置がオプション 82 情報をスプーフィングする可能性があります。
- DHCP スヌーピング統計情報を表示するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力します。スヌーピング統計情報を消去するには、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力します。

（注）　RSPAN VLAN で 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 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 の宛先ポートに到達しなくなることがあります。

DHCP リレー エージェントの設定

スイッチで 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**	スイッチで DHCP サーバとリレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
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）設定をコンフィギュレーション ファイルに保存します。

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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」の「*Configuring DHCP*」を参照してください。

- リレー エージェント情報の確認（検証）
- リレー エージェント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は、**ip helper-address** *address* インターフェイス コンフィギュレーション コマンドを使用してスイッチを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** コマンドで使用するアドレスには、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 アドレスを指定できます。ネットワーク アドレスを使用すると、すべての DHCP サーバが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*	IP アドレスと IP サブネットを使用してインターフェイスを設定します。
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 アドレスには、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 アドレスを指定できます。ネットワーク アドレスを使用すると、他のサーバが 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は、サーバごとに 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 メンバーシップ 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 VLAN にポートを割り当てます。
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）設定をコンフィギュレーション ファイルに保存します。

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に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**	スイッチをイネーブルにして、DHCP サーバに転送される DHCP 要求メッセージの DHCP リレー情報（Option 82 フィールド）を挿入または削除します。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。 リモート ID は次のいずれかに設定することができます。 • 63 文字までの ASCII 文字列（スペースなし） • スイッチの設定済みホスト名 **（注）** ホスト名が 63 文字を超える場合、リモート ID 設定では 64 文字以降が切り捨てられます。 デフォルトのリモート ID はスイッチの 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の場合、スイッチが Option 82 情報を含む着信 DHCP スヌーピング パケットをエッジ スイッチから受け入れることができるようにします。 デフォルト設定は、ディセーブルです。 **（注）** このコマンドは、集約スイッチが信頼できる装置に接続されている場合に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の回線 ID サブオプションを設定します。 VLAN およびポート 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 は、3 ～ 63 文字の ASCII 文字（スペースなし）を使用して設定できます。 （任意）TLV 形式の回線 ID サブオプションを挿入せずに加入者情報を定義する場合は、**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信頼できる状態または信頼できない状態に設定します。信頼できないクライアントからメッセージを受信するようにインターフェイスを設定するには、**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 1 秒あたりの 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）** 信頼できないインターフェイスでのレートは、100 パケット/秒以下に制限することを推奨します。信頼できる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、DHCP スヌーピングをイネーブルにしている複数の VLAN に割り当てられたトランク ポートであれば、レート制限を高い値に設定するとこを推奨します。
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で受信された DHCP パケットの送信元 MAC アドレスが、パケットのクライアント ハードウェア アドレスと一致すること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、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
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）設定をコンフィギュレーション ファイルに保存します。

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 情報を含む着信 DHCP スヌーピング パケットを廃棄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 で DHCP スヌーピングをグローバルにイネーブルにし、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 gigabitethernet1/1
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

DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。DHCP スヌーピングをイネーブルにすると、その設定はプライマリ VLAN およびそれに関連付けられているセカンダリ VLAN の両方に伝播します。プライマリ VLAN で DHCP スヌーピングをイネーブルにすると、セカンダリ VLAN でも DHCP スヌーピングがイネーブルになります。

プライマリ VLAN で DHCP スヌーピングがすでに設定されていて、セカンダリ VLAN で DHCP スヌーピングを別の値で設定した場合、セカンダリ VLAN の設定は有効になりません。DHCP スヌーピングは、プライマリ VLAN で設定する必要があります。プライマリ VLAN で DHCP スヌーピングが設定されていない場合に、VLAN 200 などのセカンダリ VLAN で DHCP スヌーピングを設定しようとすると、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 コマンドの出力には、DHCP スヌーピングがイネーブルになっているすべての VLAN（プライマリおよびセカンダリ プライベート VLAN を含む）が示されます。

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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring DHCP」の「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:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイル用の URL を指定します。 • **flash:**/*filename* • **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に、転送を遅らせ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* に指定できる範囲は 1 ～ 4904 です。*seconds* に指定できる範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 **（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。

	コマンド	目的
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）設定をコンフィギュレーション ファイルに保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウト値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。このコマンドは、削除するエントリごとに入力し 1 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 26-2 に示す各特権 EXEC コマンドを使用します。

表 26-2　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と統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの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、スタティック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（IPSG）の概要

IPSG は、DHCP スヌーピング バインディング データベースと手動で設定された IP 送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することで、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能です。IP ソース ガードを使用すると、ホストがネイバーの IP アドレスを使用しようとした場合のトラフィック攻撃を防ぐことができます。

IP ソース ガードは、信頼できないインターフェイスで DHCP スヌーピングがイネーブルになっている場合にイネーブルにできます。インターフェイスで IPSG をイネーブルにすると、スイッチは、インターフェイスで受信した IP トラフィックを、DHCP スヌーピングで許可された DHCP パケットを除いてすべてブロックします。インターフェイスには、ポート Access Control List（ACL; アクセス制御リスト）が適用されます。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 アドレスを持つ IP トラフィックだけが許可され、他のトラフィックがすべて拒否されます。

（注）　ポート ACL は、同じインターフェイスに影響を与える ルータ ACL または VLAN マップよりも優先されます。

IP 送信元バインディング テーブルのバインディングは、DHCP スヌーピングによって学習されたバインディングか、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、それに関連付けられた MAC アドレスおよび 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だけ、IP 送信元バインディング テーブルを使用します。

IPSG は、アクセス ポートやトランク ポートなどのレイヤ 2 ポートでだけサポートされます。IPSG は、送信元 IP アドレス フィルタリングまたは送信元 IP および MAC アドレス フィルタリングを使用して設定できます。

- 「送信元 IP アドレス フィルタリング」（P.26-16）
- 「送信元 IP および MAC アドレス フィルタリング」（P.26-17）
- 「スタティック ホストの IP ソース ガード」（P.26-17）

送信元 IP アドレス フィルタリング

このオプションを使用して IPSG をイネーブルにした場合、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。スイッチは、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に 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、または削除された場合、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、そのポート ACL をインターフェイスに再度適用します。

IP 送信元バインディング（DHCP スヌーピングでによってダイナミックに学習されるか、手動で設定される）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と、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 を作成して適用します。IP ソース ガードをディセーブルにすると、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した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 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 パケット以外のパケットをすべて廃棄します。

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した場合は、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 ポートでは、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 機能を、DHCP が使用されないスタティックな環境に拡張します。以前の IPSG では、DHCP スヌーピングによって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ました。有効な DHCP バインディング エントリがないホストからのトラフィックはすべて廃棄されます。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トラフィックを制限します。トラフィックは、DHCP スヌーピング バインディング データベースと手動で設定された IP 送信元バインディングに基づいてフィルタリングされます。以前のバージョンの IPSG では、IPSG を機能させるために DHCP 環境が必要でした。

スタティック ホストの IPSG を使用すると、DHCP なしで IPSG を機能させることができます。スタティック ホストの IPSG では、ポート ACL のインストールに IP 装置追跡テーブルのエントリが使用されます。スイッチは、ARP 要求またはその他の IP パケットに基づいてスタティック エントリを作成し、指定のポートの有効なホストのリストを保持します。指定のポートへのトラフィックの送信を許可す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 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 では、ダイナミック ホストもサポートされます。ダイナミック ホストが IP DHCP スヌーピング テーブルで使用可能な 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 装置追跡テーブルによって学習されます。**show ip device tracking all** EXEC コマンドを入力すると、IP 装置追跡テーブルでエントリが ACTIVE と表示されます。

（注） 複数のネットワーク インターフェイスを備えた一部の 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送信することがあります。この無効パケットには、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 アドレスが送信元アドレスとして含まれています。この無効パケットにより、スタティック ホストの IPSG がホストに接続し、無効な IP または MAC アドレス バインディングを学習して、有効なバインディングを拒否することがあります。無効パケットの送信を防ぐ方法については、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問い合わせてください。

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 IP または MAC バインディングをダイナミックに学習します。IP または MAC バインディングは、ARP および IP パケットを介してスタティック ホストから学習され、装置追跡データベースに保存されます。指定のポートでダイナミックに学習された IP アドレス、またはスタティックに設定された IP アドレスの数が上限に達すると、ハードウェアは新しい IP アドレスを持つパケットをすべて廃棄します。スタ

ティック ホストの IPSG では、何らかの理由で移動または除去されたホストを解決するために、IP 装置追跡を使用して、ダイナミックに学習した IP アドレス バインディングを期限切れにします。この機能は DHCP スヌーピングと併用できます。DHCP ホストとスタティック ホストの両方に接続されているポートでは、複数のバインディングが設定されます。たとえば、バインディングは装置追跡データベースと DHCP スヌーピング データベースの両方に保存されます。

IP ソース ガードの設定

IP ソース ガードのデフォルト設定

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

- スタティック IP バインディングは、非ルーテッド ポートでだけ設定できます。ルーテッド インターフェイスで **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 コマンドを入力すると、次のエラー メッセージが表示されます。

  ```
  Static IP source binding can only be configured on switch port.
  ```

- インターフェイスで送信元 IP フィルタリングによる IP ソース ガードをイネーブルにする場合は、そのインターフェイスのアクセス VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードをイネーブルにしていて、すべての VLAN で DHCP スヌーピングがイネーブルになっている場合は、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になっている場合に、トランク インターフェイス上の VLAN で DHCP スヌーピングをイネーブルまたはディセーブルにすると、スイッチのトラフィック フィルタリングが正しく動作しなくなることがあります。

- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにする場合は、インターフェイスで DHCP スヌーピングとポート セキュリティをイネーブルにする必要があります。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力して、DHCP サーバで Option 82 がサポートされるようにする必要があります。MAC アドレス フィルタリングによる IP ソース ガードがイネーブルになっている場合、DHCP ホストの MAC アドレスは、ホストにリースが付与されるまで学習されません。DHCP スヌーピングは、サーバからホストにパケットを転送するときに、Option 82 データを使用してホストの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 ではサポートされません。
- この機能は、802.1X ポートベースの認証がイネーブルの場合にイネーブルにできます。

- ternary content addressable memory（TCAM; 三値連想メモリ）のエントリの数が上限を超えると、CPU の使用率が上昇します。

IP ソース ガードのイネーブル化

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**	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガード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 つの点に注意してください。 • DHCP サーバは Option 82 をサポートしている必要があります。そうでない場合は、クライアントに 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す。DHCP クライアントの MAC アドレスは、スイッチが非 DHCP データ トラフィックを受信するときにだけ、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。 このコマンドは、スタティック バインディングごとに入力します。
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*]	（任意）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）設定をコンフィギュレーション ファイルに保存します。

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

スタティック IP 送信元バインディング エントリを削除するには、**no ip source** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 および VLAN 11 で送信元 IP および MAC フィルタリングによる IP ソース ガードをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
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
gigabitethernet1/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/1
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 コマンドを設定する必要があります。IP 装置追跡のグローバルなイネーブル化またはインターフェイス上での IP 装置の上限の設定を行わずに、ポートでこのコマンドの設定だけを行った場合、スタティック ホストの IPSG は、そのインターフェイスからの IP トラフィックをすべて拒否します。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 モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP ホスト テーブルをオンにし、IP 装置追跡をグローバルにイネーブルにします。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポートを アクセス ポートに設定します。
ステップ 5	**switchport access vlan** *vlan-id*	このポートの VLAN を設定します。

	コマンド	目的
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングによるスタティック 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する場合は、次の 2 つの点に注意してください。 • DHCP サーバは Option 82 をサポートしている必要があります。そうでない場合は、クライアントに 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す。DHCP クライアントの MAC アドレスは、スイッチが非 DHCP データ トラフィックを受信するときにだけ、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 装置追跡テーブルで許可される、ポート上のスタティック IP 数の上限を設定します。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 アドレスの上限を設定します。
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 の許可 ACL を表示します。
ステップ 12	**show ip device track all [active | inactive] count**	スイッチ インターフェイス上の指定されたホストの IP と MAC のバインディングを表示して、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**:アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します。

次に、インターフェイスでスタティック ホストの IPSG を停止する例を示します。

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

次に、ポートでスタティック ホストの IPSG をイネーブルにする例を示します。

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

次に、レイヤ 2 アクセス ポートで IP フィルタによる IPSG イネーブルにし、インターフェイス Gi0/3 上の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface 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 ポートで IP-MAC フィルタによる IPSG イネーブルにし、インターフェイス Gi0/3 上の有効な IP-MAC バインディングを確認して、このインターフェイス上のバインディング数が上限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 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の IP または MAC バインディング エントリをすべて表示する例を示します。CLI には、アクティブなエントリと非アクティブなエントリがすべて表示されます。インターフェイスでホストが学習されると、新しいエントリはアクティブとマークされます。同じホストがそのインターフェイスから切断され、別のインターフェイスに接続された場合、新しい IP または MAC バインディングは、ホストが検出されるとすぐにアクティブと表示されます。前のインターフェイス上のこのホストの古いエントリは、非アクティブとマークされます。

```
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のアクティブな IP または MAC バインディング エントリをすべて表示する例を示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    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非アクティブな IP または MAC バインディング エントリをすべて表示する例を示します。ホストは、最初に GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 に移動されます。GigabitEthernet 0/1 で学習された IP または MAC アドレスは、非アクティブとマークされます。

```
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の IP 装置追跡のホスト エントリの合計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。IP 装置追跡のグローバルなイネーブル化またはインターフェイス上での IP 装置の上限の設定を行わずに、ポートでこのコマンドの設定だけを行った場合、スタティック ホストの IPSG は、そのインターフェイスからの IP トラフィックをすべて拒否します。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 IP フィルタによるスタティック 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 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 ポート上の 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 に関連付けます。
ステップ 14	**ip device tracking maximum** *number*	IP 装置追跡テーブルで許可される、ポート上のスタティック IP 数の上限を設定します。 最大数は 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]**	このポートで MAC アドレス フィルタリングによるスタティック ホストの IPSG をアクティブにします。
ステップ 16	**end**	インターフェイス コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 17	**show ip device tracking all**	設定を確認します。
ステップ 18	**show ip verify source interface** *interface-id*	IP ソース ガードの設定を確認します。スタティック ホストの IPSG の許可 ACL を表示します。

次に、プライベート VLAN ホスト ポートで IP フィルタによるスタティック 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 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
```

この出力は、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 に関連付けられます。したがって、この例では、プライマリ VLAN ID 200 が表に表示されます。

```
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
```

この出力は、プライマリ VLAN とセカンダリ VLAN の両方に 5 つの有効な IP-MAC 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

表 26-3　IP ソース ガード情報を表示するためのコマンド

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 エントリを表示します。
show ip source binding	スイッチ上の IP 送信元バインディングを表示します。
show ip verify source	スイッチ上の 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、接続されている装置のクライアント ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポート上で同じ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内に配置されている場合、それらのスイッチは、直接接続されている装置への接続を提供します。一部の環境（作業現場など）では、装置に障害が発生した場合、既存ネットワーク内の交換装置がただちに稼動する必要があります。現在の DHCP 実装では、DHCP が交換装置に同じ IP アドレスを提供する保証はありません。制御やモニタなどに使用されるソフトウェアでは、安定した IP アドレスが各装置に関連付けられていることが前提となります。装置を交換したときには、DHCP クライアントが変更された場合でも、安定したアドレスが割り当てられる必要があります。

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、ポートで受信した 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、常に同じ IP アドレスが同じ接続ポートに提供されることが保証されます。DHCP プロトコルでは、DHCP パケット内のクライアント ID オプションで DHCP クライアントが識別されます。クライアント ID オプションを挿入しないクライアントは、クライアント ハードウェア アドレスで識別されます。この機能を設定した場合は、インターフェイスのポート名がクライアント ID やハードウェア アドレスよりも優先され、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 になります。

どの場合でも、イーサネット ケーブルを同じポートに接続することで、同じ IP アドレスが DHCP を介して接続装置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 でだけサポートされ、サードパーティ製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.26-26）
- 「ポートベースのアドレス割り当て設定時の注意事項」（P.26-27）
- 「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.26-27）

ポートベースのアドレス割り当てのデフォルト設定

デフォルトでは、DHCP サーバのポートベースのアドレス割り当てはディセーブルに設定されています。

ポートベースのアドレス割り当て設定時の注意事項

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を説明します。

- 1 つのポートに割り当てることができる IP アドレスは 1 つだけです。
- 予約済み（事前割り当て済み）のアドレスは、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドで消去できません。
- 事前割り当て済みのアドレスは、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。事前割り当て済みのアドレスはホスト プールで使用できませんが、各 DHCP アドレス プールには複数のアドレスを事前に割り当てることができます。
- DHCP プールからの割り当てを、予約済みアドレスに制限する（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ない）には、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

DHCP サーバのポートベース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にイネーブルにし、インターフェイス上で加入者 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**	DHCP サーバがすべての着信 DHCP メッセージで加入者 ID をクライアント ID としてグローバルに使用するように設定します。
ステップ 3	**ip dhcp subscriber-id interface-name**	インターフェイスの短い名前に基づいて加入者 ID を自動的に生成します。 特定のインターフェイス上で設定された加入者 ID は、このコマンドよりも優先されます。
ステップ 4	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip dhcp server use subscriber-id client-id**	DHCP サーバがインターフェイス上のすべての着信 DHCP メッセージで加入者 ID をクライアント ID として使用するように設定します。
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）設定をコンフィギュレーション ファイルに保存します。

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

IP アドレスの事前割り当てを行って、そのアドレスをインターフェイス名で識別されるクライアントに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp pool** *poolname*	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名は、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で識別される 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 進数値を指定できます。
ステップ 5	**reserved-only**	（任意）DHCP アドレス プール内の予約済みアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip dhcp pool**	DHCP プールの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。インターフェイス上で加入者 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。

IP アドレスの予約を DHCP プールから削除するには、**no address** *ip-address* **client-id** *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限なしに変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。

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、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短い名前とクライアントの事前割り当て済み 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>
```

次の例は、事前割り当て済みのアドレスが DHCP プールで正しく予約されたことを示しています。

```
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詳細については、Cisco.com ページで [Search] フィールドに *Cisco IOS IP Addressing Services* と入力して、Cisco IOS ソフトウェア マニュアルにアクセスしてください。マニュアルは次の URL からも入手できます。
http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバのポートベース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 26-4 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 26-4　DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

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。