CHAPTER 20

DHCP 機能および IP ソース ガードの設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチ上における、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 ポートベース アドレス割り当て機能の設定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、このリリースのコマンド 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。

DHCP 機能の概要

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 環境で広範囲に使用されています。この機能により、IP アドレス管理のオーバーヘッドを著しく軽減できます。また、DHCP により、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ので、制限のある IP アドレス スペースの節約に役立ちます。

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide*』*Release 12.2* の「*IP Addressing and Services*」の章の「*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、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間で転送するレイヤ 3 デバイスです。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間で透過的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、DHCP のセキュリティ機能で、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）を構築し、維持することで、ネットワーク セキュリティを提供します。この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.20-15）を参照してください。

DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールに似た機能を果たします。エンドユーザに接続する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する信頼できるインターフェイスとを区別するのに DHCP スヌーピングを使用します。

（注）　DHCP スヌーピングが正常に機能するために、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続する必要があります。

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で受信されたメッセージです。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場合、信頼できないメッセージは、カスタマーのスイッチなど、サービス プロバイダー ネットワークにないデバイスから送信されたものです。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送信元の可能性があるので、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 MAC（メディア アクセス制御）アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN（仮想 LAN）番号、およびスイッチ上のローカルにある信頼できないインターフェイスに対応するインターフェイス情報があります。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のデバイス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そのネットワークにはないデバイス上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、そのインターフェイスが属する VLAN で DHCP スヌーピングがイネーブルの場合、スイッチは送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスとを比較します。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。

- DHCPOFFER、DHCPACK、DHCPNAK、または DHCPLEASEQUERY パケットなどの、DHCP サーバからのパケットがネットワークまたはファイアウォールの外で受信された場合
- パケットが信頼できないインターフェイスで受信され、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 データベースにある 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するものの、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、メッセージが受信され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

DHCP スヌーピングをサポートする集約スイッチが DHCP Option 82 情報の挿入元のエッジ スイッチに接続されている場合、パケットが信頼できないインターフェイスに着信したときに、Option 82 情報が含まれるパケットは廃棄されます。DHCP スヌーピングがイネーブル化されているときに、パケットが信頼できないポートに着信した場合、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを取得せず、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ときに、**ip dhcp snooping information option allowed-trust** 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 スイッチから送信された Option 82 情報を含むパケットを受け入れます。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取得します。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上で Option 82 情報を含むパケットを受信する場合は、集約スイッチ上で、ダイナミック ARP 検査や IP ソース ガードなどの DHCP セキュリティ機能をイネーブルにできます。集約スイッチに接続されたエッジ スイッチのポートは、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。

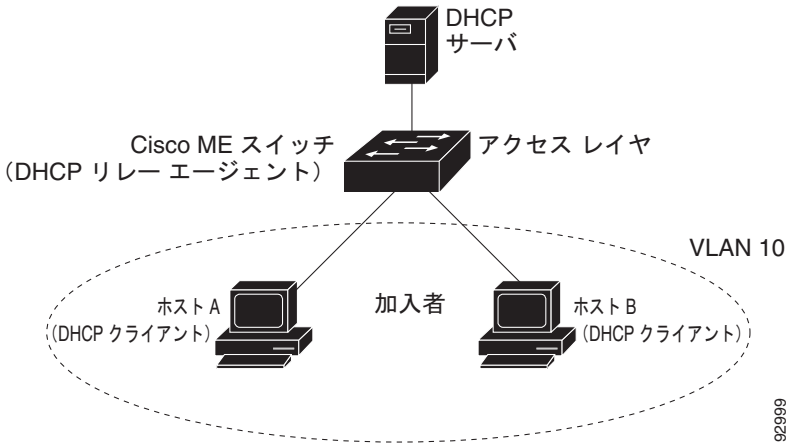
Option 82 データ挿入

住宅地のメトロポリタン イーサネット アクセス環境では、DHCP により、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。スイッチで DHCP Option 82 機能がイネーブルの場合は、（MAC アドレスの他に）ネットワークへの接続に使用されるスイッチ ポートにより、加入者デバイスを識別します。加入者 LAN の複数のホストは、アクセス スイッチ上の同一ポートに接続でき、一意に識別されます。

（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 20-1 は、中央集中型 DHCP サーバが、アクセス レイヤでスイッチに接続している加入者に IP アドレスの割り当てを行うメトロポリタン イーサネット ネットワークの例です。DHCP クライアントおよびこれに対応する DHCP サーバは、同じ IP ネットワークまたはサブネット上には存在しないため、DHCP リレー エージェント（Cisco ME スイッチ）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 メッセージを転送するように、ヘルパー アドレスを使用して設定されます。

図 20-1　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。

- ホスト（DHCP クライアント）は、DHCP 要求を生成して、ネットワーク上にブロードキャストします。
- スイッチが 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、回線 ID サブオプションは、パケットの受信ポートの識別子である **vlan-mod-port** です。リモート ID および回線 ID も設定できます。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.20-12）を参照してください。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- 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 サーバで、パケットを受信します。サーバが Option 82 対応の場合は、リモート ID、回線 ID、またはその両方を使用して、IP アドレスを割り当てて、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 アドレス数を制限するなど、ポリシーの実装を行います。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。スイッチでは、リモート ID あるいは回線 ID フィールドを調べて、自身が挿入した 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て、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、前述の一連のイベントが発生した場合、図 20-2 内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

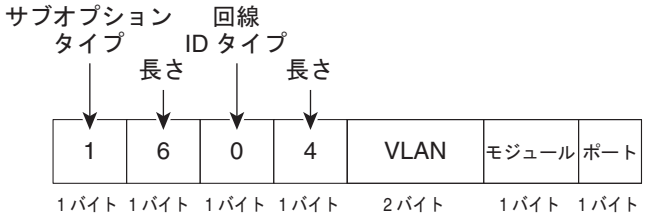
- リモート ID タイプ
- 回線 ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります たとえば 24 の 10/100 ポートおよび Small Form-factor Pluggable（SFP）モジュール スロットを含むスイッチでは、ポート 3 がファスト イーサネット 0/1 ポート、ポート 4 がファスト イーサネット 0/2 ポートのようになります。ポート 27 は SFP モジュール スロット 0/1 などのようになります。

図 20-2 に、デフォルトのサブオプション設定が使用されている場合の、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。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る場合にこれらのパケット形式を使用します。

図 20-2　　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

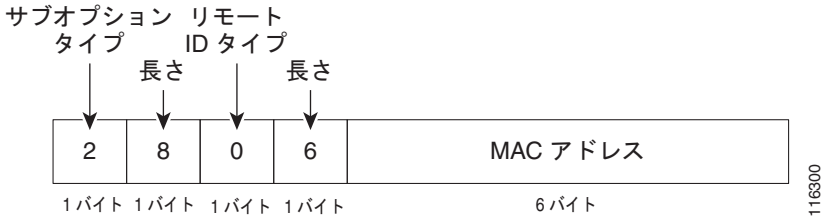


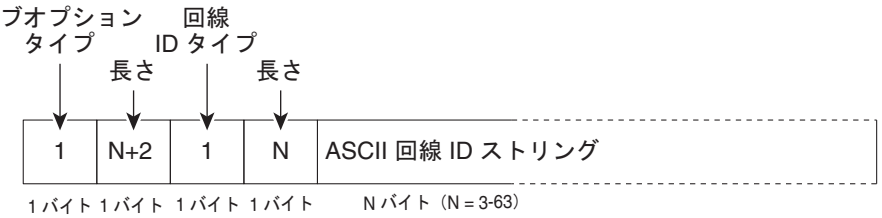
図 20-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングをグローバルにイネーブルにして、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力する場合に、これらのパケット形式を使用します。

パケット内の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。

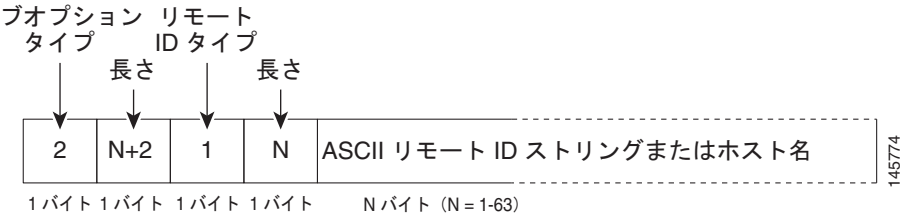
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 設定するストリング長に応じて、長さの値を変えられます。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 設定するストリング長に応じて、長さの値を変えられます。

図 20-3　　ユーザ設定のサブオプション 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 アドレスは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。各エントリの最後は、エントリに関連性のあるすべてのバイトが含まれる *checksum* 値です。各エントリは 72 バイトで、そのあとにスペースとチェックサム値が続きます。

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

リロードしたとき、スイッチは DHCP スヌーピング バインディング データベースを構築するため、バインディング ファイルを読み込みます。スイッチは、データベース変更時にファイルを更新することにより、ファイルの内容を維持します。

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

バインディングのあるファイルのフォーマットは次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

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

バインディング ファイルの例は次のとおりです。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 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 機能の設定

- 「DHCP リレー エージェントの設定」（P.20-10）
- 「パケット転送アドレスの指定」（P.20-10）
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.20-12）
- 「プライベート VLAN での DHCP スヌーピングのイネーブル化」（P.20-14）
- 「Cisco IOS DHCP サーバ データベースのイネーブル化」（P.20-14）
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」（P.20-14）

DHCP のデフォルト設定

表 20-1 に、DHCP のデフォルト設定を示します。

表 20-1　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]
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チェック	イネーブル（無効なメッセージは廃棄）[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た 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信するための DHCP スヌーピング オプション[3]	ディセーブル
DHCP スヌーピング制限レート	設定なし
DHCP スヌーピングの信頼	信頼されない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピング 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だけから、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル。設定が必要です。宛先が設定されている場合にだけ、この機能は有効です。

1. スイッチは、DHCP サーバとして設定された場合にだけ 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）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 スイッチから送信された 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

- スイッチでは、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 上でイネーブルになるまで、アクティブではありません。

- スイッチで DHCP スヌーピングをグローバルでイネーブルにする前に、DHCP サーバおよび DHCP リレー エージェントとして機能しているデバイスが設定されていて、イネーブルであることを確認してください。
- 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と、スヌーピングがディセーブルになるまで、次の Cisco IOS コマンドを使用できません。次のコマンドを入力すると、スイッチはエラー メッセージを返し、設定は適用されません。
  - **ip dhcp relay information check** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information policy** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trust-all** グローバル コンフィギュレーション コマンド
  - **ip dhcp relay information trusted** インターフェイス コンフィギュレーション コマンド
- スイッチに DHCP スヌーピング オプション情報を設定する前に、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できる IP アドレスを指定する、またはデバイスに DHCP オプションを設定する必要があります。
- スイッチ上に多数の回線 ID を設定する場合は、NVRAM（不揮発性 RAM）またはフラッシュ メモリに対して長い文字列が与える影響について考慮してください。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できる IP アドレスを指定する、デバイスに DHCP オプションを設定する、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あるものの、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、**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 に設定します。
- 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、**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 に設定します。
- 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際は、次の注意事項に従ってください。
  - NVRAM およびフラッシュ メモリのストレージ容量に制限があるので、バインディング ファイルは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存することを推奨します。
  - ネットワーク ベース URL（TFTP や FTP（ファイル転送プロトコル）など）の場合、スイッチが設定した URL のバインディング ファイルにバインディングを書き込む前に、その URL で空のファイルを作成しておく必要があります。先にサーバで空のファイルを作成する必要があるかどうかを判断するには、TFTP サーバのマニュアルを参照してください。一部の TFTP サーバはこの方法では設定できません。
  - データベースのリース時間を正確にするには、Network Time Protocol（NTP）をイネーブルにして、設定することを推奨します。詳細については、「NTP の設定」（P.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、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力することにより、DHCP スヌーピングの統計情報を表示できます。また、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力することにより、スヌーピングの統計情報カウンタをクリアできます。

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

DHCP サーバの設定

スイッチは、DHCP サーバとして機能させることもできます。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になっていますが、設定が行われていません。このため、これらの機能は動作しません。

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

DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 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）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 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」の章の「*Configuring DHCP*」を参照してください。

- リレー エージェント情報のチェック（確認）
- 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り、スイッチでメトロ IP アクセス イメージが稼動している場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的な規則は、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで

使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにできます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface vlan** *vlan-id*	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address subnet-mask*	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 4	**ip helper-address** *address*	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにできます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface range** *port-range* または **interface** *interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no shutdown**	必要な場合に、インターフェイスをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interfaces（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 8	**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 9	**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 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP パケット転送アドレスを削除するには、**no ip helper-address** *address* インターフェイス コンフィギュレーション コマンドを使用します。

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp snooping**	DHCP スヌーピングをグローバル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 サーバへの 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 は次のように設定できます。 • 最大 63 の ASCII 文字（スペースなし）の文字列 • スイッチの設定済みのホスト名 **（注）** ホスト名が 63 文字以上の場合は、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、スイッチの MAC アドレスです。
ステップ 6	**ip dhcp snooping information option allowed-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に、エッジ スイッチから送信された Option 82 情報を含む着信 DHCP スヌーピング パケットをスイッチが受信できるようにします。 デフォルトはディセーブルです。 **（注）** このコマンドを入力する必要があるのは、信頼できるデバイスに接続された集約スイッチだけです。
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	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。

	コマンド	目的
ステップ 9	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id string** [**override**] *ASCII-string*	（任意）指定され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。 1 ～ 4094 の範囲の VLAN ID を使用して、VLAN およびポートの識別子を指定します。デフォルトの回線 ID は、ポートの識別子で、**vlan-mod-port** フォーマットです。 回線 ID は、3 ～ 63 の ASCII 文字（スペースなし）の文字列になるよう設定できます。 （任意）加入者情報を定義するうえで、TLV 形式で挿入された回線 ID サブオプションが不要な場合は、キーワード **override** を使用します。
ステップ 10	**ip dhcp snooping trust**	（任意）インターフェイスを trusted または untrusted と設定します。信頼され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、キーワード **no** を使用します。デフォルトでは、信頼されません。
ステップ 11	**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）** 信頼されないレート制限を毎秒 100 パケット以下にすることを推奨します。信頼できるインターフェイスでレート制限を設定した場合、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、レート制限値を上げる必要があります。
ステップ 12	**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 13	**ip dhcp snooping verify mac-address**	（任意）信頼できないポートで受信された DHCP パケット内の送信元 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内のクライアント 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 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show running-config**	設定を確認します。
ステップ 16	**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 スイッチから送信された 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 allowed-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毎秒 100 パケットに設定する方法を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

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

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

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

show ip dhcp snooping 特権 EXEC コマンド出力には、プライマリおよびセカンダリ プライベート VLAN を含む、DHCP スヌーピングがイネーブルのすべての VLAN が表示されています。

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:**/*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:**/*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*	バインディング データベースが変更されたあとのデータベースの転送プロセスを停止する時間を指定します。 指定できる範囲は 0 ～ 86400 です。無制限を指定する場合、0 を使用します。デフォルトは 300 秒（5 分）です。

	コマンド	目的
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転送が遅延する期間を指定します。 指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。指定できる *vlan-id* の範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 秒です。 追加する各エントリにこのコマンドを入力します。 **（注）** 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 20-2 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 20-2　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、動的に設定されたバインディングだけを表示します。[1]
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。

1. 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、スイッチは手動で設定されたバインディングを削除しません。

DHCP サーバ ポートベース アドレス 割り当て

DHCP サーバ ポートベース アドレス割り当ては、DHCP が、付加されたデバイス クライアント ID またはクライアント ハードウェア 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 アドレスを維持できるようにする機能です。

イーサネット スイッチをネットワーク内に配置すると、それらのスイッチによって、直接接続されたデバイスに対する接続が提供されます。工場のような一部の環境では、あるデバイスに障害が発生した場合、交換デバイスが、既存のネットワーク内で即座に動作する必要があります。現在の DHCP 実装では、DHCP がその交換デバイスに対して同じ 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 IP アドレスは変わらないと見なされます。デバイスが交換された場合、DHCP クライアントが変わったとしても、アドレス割り当ては変わらないままである必要があります。

DHCP サーバ ポートベース アドレス割り当て機能を設定すると、ポート上で受信された DHCP メッセージ内でクライアント 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ていても、同じ IP アドレスがその同じ接続ポートに対して常に提供されるようになります。DHCP プロトコルでは、DHCP パケット内のクライアント ID オプションによって DHCP クライアントが認識されます。クライアント ID オプションを持っていないクライアントは、クライアント ハードウェア アドレスによって識別されます。この機能を設定すると、インターフェイスのポート名によって、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、つまりスイッチ ポートがクライアント ID になります。

どんな場合でも、同じポートに対してイーサネット ケーブルを接続することによって、同じ IP アドレスが DHCP を介して付加されたデバイスに割り当てられます。

DHCP サーバ ポートベース アドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけであり、サードパーティのサーバではサポートされていません。

DHCP サーバ ポートベース アドレス 割り当ての設定

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 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 アドレス割り当て設定のガイドライン

次に、DHCP ポートベース アドレス割り当て設定に関するガイドラインを示します。

- ポートごとに割り当てられる IP アドレスは 1 つだけです。
- **clear ip dhcp binding** グローバル コンフィギュレーション コマンドを使用しても、予約済みアドレス（事前割り当て）は消去できません。
- 事前割り当てアドレスは、通常のダイナミック IP アドレス割り当てからは自動的に除外されます。事前割り当てアドレスは、ホスト プール内では使用できませんが、DHCP アドレス プールごとに複数のアドレスを事前に割り当てることが可能です。

- DHCP プールから事前設定予約への割り当てを制限するには（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 DHCP 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 コマンドを入力します。

DHCP サーバ ポートベース アドレス 割り当てのイネーブル化

ポートベース アドレス割り当てをグローバルにイネーブルにし、インターフェイス上で加入者 ID をグローバルに生成するには、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 サーバを、加入者 ID がすべての着信 DHCP メッセージにおけるクライアント ID としてグローバルに使用され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 サーバを、加入者 ID がインターフェイス上のすべての着信 DHCP メッセージにおけるクライアント ID として使用され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）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後、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスを事前に割り当て、それらのアドレスをクライアントに関連付けます。DHCP プールから事前に設定された予約への割り当てを制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスを事前に割り当て、そのアドレスを、インターフェイス名によって識別されるクライアントに対して関連付けるには、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 ネットワーク番号およびサブネット マスクを指定します。
ステップ 4	**address** *ip-address* **client-id** *string* [**ascii**]	インターフェイス名によって特定される DHCP クライアントの IP アドレスを予約します。 *string*：ASCII 値または 16 進数値で指定できます。
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 アドレス予約を削除するには、**no address** *ip-address* **client-id** *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限なしに変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者 ID が自動的に生成されています。また、DHCP メッセージ内のクライアント ID フィールドは DHCP サーバによってすべて無視され、その代わりに、加入者 ID が使用されています。加入者 ID は、インターフェイスの短い名前と、IP アドレス 10.1.1.7 が事前に割り当てられたクライアントに基づいています。

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

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

DHCP サーバ ポートベース アドレス割り当て機能の設定の詳細については、Cisco.com の [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 で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 ポートベース アドレス 割り当ての表示

DHCP サーバ ポートベース アドレス割り当て情報を表示するには、表 20-3 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 20-3　DHCP ポートベース 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 サーバ上のアドレス バインディングを表示します。

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、ホストがネイバの IP アドレスを使用しようとする場合のトラフィック攻撃を回避できます。

DHCP スヌーピングが信頼できないインターフェイスでイネーブルの場合に IP ソース ガードをイネーブルにできます。IPSG がインターフェイスでイネーブルになったあと、スイッチは、DHCP スヌーピングで許可された DHCP パケットを除く、インターフェイスで受信されたすべての IP トラフィックをブロックします。ポート Access Control List（ACL; アクセス制御リスト）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、その他のトラフィックを拒否できます。

（注）　ポート ACL は同じインターフェイスに影響を与えるいずれのルータ 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。

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

ここでは、次の情報について説明します。

- 「送信元 IP アドレス フィルタリング」（P.20-20）
- 「送信元 IP および MAC アドレス フィルタリング」（P.20-21）
- 「スタティック ホスト用 IP ソース ガード」（P.20-21）

送信元 IP アドレス フィルタリング

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

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

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

送信元 IP および MAC アドレス フィルタリング

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

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

スイッチは、ポート セキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポート セキュリティ違反の発生時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 ホスト用 IP ソース ガード

（注） アップリンク ポートまたはトランク ポート上ではスタティック ホスト用 IP source guard（IPSG; IP ソース ガイド）は使用しないでください。

スタティック ホスト用 IPSG によって、IPSG 機能を非 DHCP およびスタティックな環境に拡張できます。旧 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したトラフィックはすべて破棄されます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。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がフィルタリングされます。旧バージョンの IPSG では、IPSG が動作するのに DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしに IPSG が動作します。スタティック ホスト用 IPSG では、IP デバイス トラッキング テーブルのエントリに基づいて、ポート ACL がインストールされます。スイッチでは、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 エントリが作成され、指定されたポートの有効なホストのリストが維持されます。指定されたポートにトラフィックを送信することを許可するホストの数も指定できます。これは、レイヤ 3 におけるポート セキュリティに相当します。

スタティック ホスト用 IPSG では、ダイナミック ホストもサポートされています。ダイナミック ホストによって、IP DHCP スヌーピング テーブル内に存在する DHCP 割り当て済み IP アドレスが受信されると、同じエントリが、IP デバイス トラッキング テーブルによって学習されます。**show ip device tracking all** EXEC コマンドを入力すると、IP デバイス トラッキング テーブルにエントリが ACTIVE として表示されます。

（注）　複数のネットワーク インターフェイスを持つ IP ホストの中には、一部の無効なパケットをネットワーク インターフェイスに送信可能なものもあります。無効なパケットには、ホストの別のネットワーク インターフェイスの IP アドレスまたは MAC アドレスが、送信元アドレスとして含まれています。無効なパケットが原因で、スタティック ホスト用 IPSG がそのホストに接続し、無効な IP アドレスまたは 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てしまう可能性があります。対応するオペレーティング システムとネットワーク インターフェイスのベンダーに相談して、ホストが無効なパケットを送信するのを防いでください。

スタティック ホスト用 IPSG では、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 バインディングが動的に取得されます。IP または MAC バインディングは、ARP および IP パケットによって、スタティック ホストから取得されます。これらのパケットは、デバイス トラッキング データベースに保存されます。指定されたポート上で動的に取得されるか、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、新しい IP アドレスを持つパケットはすべてハードウェアによって破棄されます。何らかの理由により移動または撤去されたホストを解決するために、スタティック ホスト用 IPSG では、IP デイバス トラッキングによって、学習された IP アドレス バインディングが動的にエージング アウトされます。この機能は、DHCP スヌーピングと共に使用できます。DHCP とスタティック ホストへ接続されているポート上で、複数のバインディングが確立されます。たとえば、バインディングが、デバイス トラッキング データベースと、DHCP スヌーピング バインディング データベースの両方に保存されます。

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、VLAN が所属するアクセス VLAN でイネーブルでなければなりません。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードがイネーブルで、DHCP スヌーピングがすべての VLAN でイネーブルの場合、送信元 IP アドレス フィルタがすべての VLAN に適用されます。

（注）　IP ソース ガードがイネーブルでトランク インターフェイス上の VLAN で DHCP スヌーピングがイネーブルまたはディセーブルの場合、スイッチが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 ガードを、送信元 IP および MAC アドレス フィルタリングによってイネーブルにする場合、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 をサポートできるようにする必要があります。IP ソース ガードが MAC アドレス フィルタリング上でイネーブルの場合、DHCP ホストの MAC アドレスは、ホストがリースを許可されるまで学習されません。パケットをサーバからホストに転送する場合、DHCP スヌーピングは、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 CAM（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。

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	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI と ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip verify source** または **ip verify source port-security**	IP ソース ガードと送信元 IP アドレス フィルタリングをイネーブルにします。 IP ソース ガードと送信元 IP および MAC アドレス フィルタリングをイネーブルにします。 （注）　**ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の 2 つの注意事項があります。 • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 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。

	コマンド	目的
ステップ 6	**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 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**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。
ステップ 9	**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 10	**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
gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet0/1
Switch(config)# end
```

スタティック ホスト用 IP ソース ガードの設定

レイヤ 2 アクセス ポート上におけるスタティック ホスト用 IP ソース ガードの設定

（注）　スタティック ホスト用 IPSG を動作させるには、**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 デバイス トラッキングをグローバルにイネーブルにしないか、あるいは、そのインターフェイス上で IP デバイス トラッキングの最大値を設定しないで、ポート上でこのコマンドだけを設定する場合、スタティック ホストを使用した IPSG によって、そのインターフェイスからのすべての IP トラフィックが拒否されます。この要件は、プライベート VLAN ホスト ポート上でのスタティック ホストを使用した 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 access 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。
ステップ 6	**ip verify source tracking port-security**	MAC アドレス フィルタリングを使用してスタティック ホスト用 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ときは、次の 2 つの注意事項があります。 • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュア アドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 7	**ip device tracking maximum** *number*	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の数の最大限度を確立します。指定できる範囲は 1 ～ 10 です。最大数は 10 です。 （注）　**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	**switchport port-security**	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 9	**switchport port-security maximum** *value*	（任意）このポートの MAC アドレスの最大値を確立します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show ip verify source** *interface* interface-id	設定を確認し、スタティック ホスト用 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 インターフェイス上における指定されたホストの IP と MAC バインディングを表示することによって、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、インターフェイス上の、スタティック ホストを使用した 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、ポート上の、スタティック ホストを使用して 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 ポート上で IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、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 gigabitethernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/3      ip trk       active       40.1.1.24                           10
Gi0/3      ip trk       active       40.1.1.20                           10
Gi0/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポート上で IP-MAC フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、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、このインターフェイス上のバインディングの数が最大値に達した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
```

次の例では、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 エントリを表示しています。CLI では、すべてのアクティブおよび非アクティブなエントリが表示されます。ホストがインターフェイス上で学習されると、その新しいエントリが ACTIVE としてマークされます。同じホストがそのインターフェイスから切断され、異なるインターフェイスに接続されると、そのホストが検知されると同時に新しい IP または MAC バインディング エントリが ACTIVE として表示されます。以前のインターフェイス上の、このホストの古いエントリは、INACTIVE としてマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet0/2     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet0/1     INACTIVE
```

次の例では、すべてのインターフェイスの、すべてのアクティブな IP または MAC バインディング エントリを表示しています。

```
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
```

次の例では、すべてのインターフェイスの、すべての非アクティブな IP または MAC バインディング エントリを表示しています。このホストは、最初に GigabitEthernet 0/1 上で学習されてから、次に GigabitEthernet 0/2 に移動されました。GigabitEthernet 0/1 上で学習された IP または MAC バインディング エントリは、INACTIVE としてマークされています。

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

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    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
```

次の例では、すべてのインターフェイスの、すべての IP デバイス トラッキング ホスト エントリの数を表示しています。

```
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 ポート上におけるスタティック ホスト用 IP ソース ガードの設定

（注） スタティック ホスト用 IPSG を動作させるには、**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 デバイス トラッキングをグローバルにイネーブルにしないか、あるいは、そのインターフェイス上で IP デバイス トラッキングの最大値を設定しないで、ポート上でこのコマンドだけを設定する場合、スタティック ホストを使用した IPSG によって、そのインターフェイスからのすべての IP トラフィックが拒否されます。この要件は、レイヤ 2 アクセス ポート上でのスタティック ホストを使用した IPSG にも適用されます。

レイヤ 2 アクセス ポート上で、IP フィルタを使用してスタティック ホスト用 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 ポート上でプライマリ 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 ポート上で独立 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。

	コマンド	目的
ステップ 9	**private-vlan association 201**	独立プライベート VLAN ポート上で、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）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 デバイス トラッキング テーブルがポート上で許可するスタティック IP の最大数を確立します。 最大数は 10 です。 （注）　スタティック ホスト用 IPSG を動作させるには、**ip device tracking maximum** *number* インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	**ip verify source tracking [port-security]**	このポート上で MAC アドレス フィルタリングを使用してスタティック ホストの IPSG をアクティブ化します。
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 ポート上で IP フィルタを使用してスタティック ホスト用 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 gigabitethernet0/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet0/3        ACTIVE
```

```
40.1.1.20       0000.0000.0305  200  FastEthernet0/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet0/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet0/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet0/3        ACTIVE
```

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合、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、テーブル内に表示されています。

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

出力には、プライマリおよびセカンダリの両方の VLAN 上に 5 つの有効な IP-MAC バインディングが存在していることが表示されます。

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 20-4 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 20-4　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 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。