CHAPTER 21

DHCP 機能および IP ソース ガードの設定

この章では、Catalyst 3750 Metro スイッチに、Dynamic Host Configuration Protocol（DHCP）スヌーピング機能および Option 82 データ挿入機能を設定する手順について説明します。また、IP ソース ガード機能の設定方法も説明しています。

（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 IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』Release 12.2 の「DHCP Commands」の章を参照してください。

この章で説明する内容は、次のとおりです。

DHCP 機能の概要

DHCP は、中央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のみが IP アドレスを使用するので、制限された IP アドレス スペースの節約に役立ちます。

スイッチでは次の DHCP 機能をサポートしています。

- DHCP サーバ（p.21-2）
- DHCP リレー エージェント（p.21-2）
- DHCP スヌーピング（p.21-2）
- Option 82 データ挿入（p.21-4）
- Cisco IOS DHCP サーバ データベース（p.21-7）
- DHCP スヌーピング バインディング データベース（p.21-7）

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」にある「Configuring DHCP」を参照してください。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ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の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.21-16）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 サーバの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 スヌーピングを正常に機能させるためには、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部から受信したメッセージです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合、信頼できないメッセージは、カスタマー スイッチなど、サービス プロバイダーのネットワーク上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 MAC（メディア アクセス制御）アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN（仮想 LAN）番号、スイッチ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をネットワークまたはファイアウォールの外部から受信する場合
- 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しても、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、パケットが信頼できないインターフェイスで受信されるとスイッチは Option 82 情報を持ったパケットを廃棄します。DHCP スヌーピングがイネーブルで、パケットが信頼できるポートで受信された場合、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。

Option 82 情報が Cisco IOS Release 12.2(25)EY より前のソフトウェア リリースが動作するエッジ スイッチによって挿入されている場合は、DHCP スヌーピング バインディング データベースが正しく読み込まれないため、DHCP スヌーピングを集約スイッチに設定できません。また、スタティック バインディングまたは Address Resolution Protocols（ARP）Access Control List（ACL; アクセス制御リスト）を使用していない場合は、IP ソース ガードおよびダイナミックな ARP 検査をスイッチに設定できません。

Cisco IOS Release 12.2(25)EY 以降では、集約スイッチを信頼できないインターフェイスを介してエッジ スイッチに接続でき、**ip dhcp snooping information option 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 Option 82 情報を持ったパケットを受け付けます。集約スイッチは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 ARP または IP ソース ガードなどの DHCP セキュリティ機能は、ホストが接続されている信頼できない入力インターフェイスで Option

82 情報を持ったパケットをスイッチが受信している間でも、集約スイッチ上でイネーブルにできます。集約スイッチに接続されたエッジ 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。

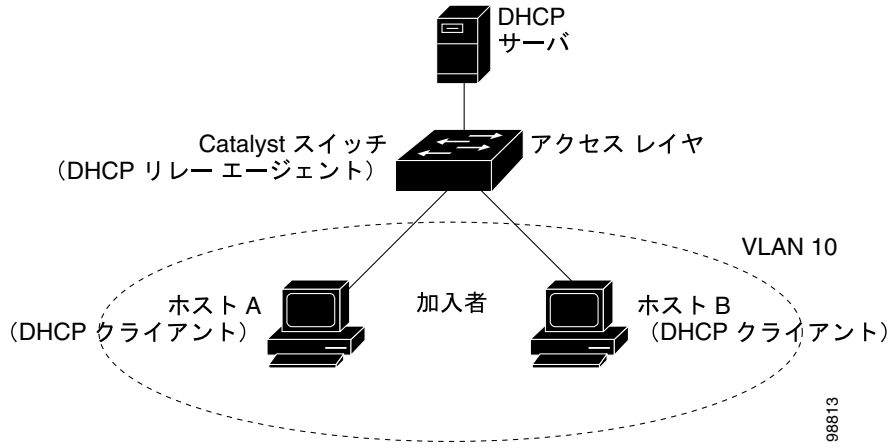
Option 82 データ挿入

住宅地のメトロポロタン 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 アドレスのほかに）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することができ、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 にある場合にのみサポートされます。

図 21-1 に、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 ネットワークの例を示します。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（Catalyst 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の間の DHCP メッセージを伝送するように、ヘルパー アドレスを使用して設定されます。

図 21-1　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 情報が追加されます。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションは、パケットの受信ポートの ID である **vlan-mod-port** です。Cisco IOS Release 12.2(25)SEE 以降では、リモート ID と回線 ID を設定することができます。これらのサブオプションの設定については、「DHCP スヌーピングおよび Option 82 のイネーブル化」（p.21-12）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、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバ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。さらに DHCP サーバは、DHCP 応答内に Option 82 フィールドをそのまま含めます。
- スイッチにより要求がサーバにリレーされた場合、DHCP サーバはこれに対する応答をスイッチにユニキャストします。スイッチでは、リモート ID あるいは回線 ID フィールドを調べて、自分が挿入した Option 82 データであることを確認します。スイッチは Option 82 フィールドを削除して、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は、前述の一連のイベントが発生したときに、図 21-2 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
  - 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、ポート番号が 3 から始まります。たとえば、スイッチでは、ポート 3 が Fast Ethernet 1/0/1 ポート、ポート 4 が Fast Ethernet 1/0/2 ポート、ポート 5 が Fast Ethernet 1/0/3 ポートなどのようになります。ポート 27 は Small Form-factor Pluggable（SFP）モジュール スロット 1/0/1、ポート 28 は SFP モジュール スロット 2/0/2 です。

図 21-2 に、リモート ID サブオプションおよび回線 ID サブオプションのデフォルト設定のパケット フォーマットを示します。回線 ID サブオプションの場合、モジュール番号がスタック内のスイッチ番号に対応します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合に、このパケット フォーマットを使用します。

図 21-2　デフォルトのサブオプション パケット フォーマット

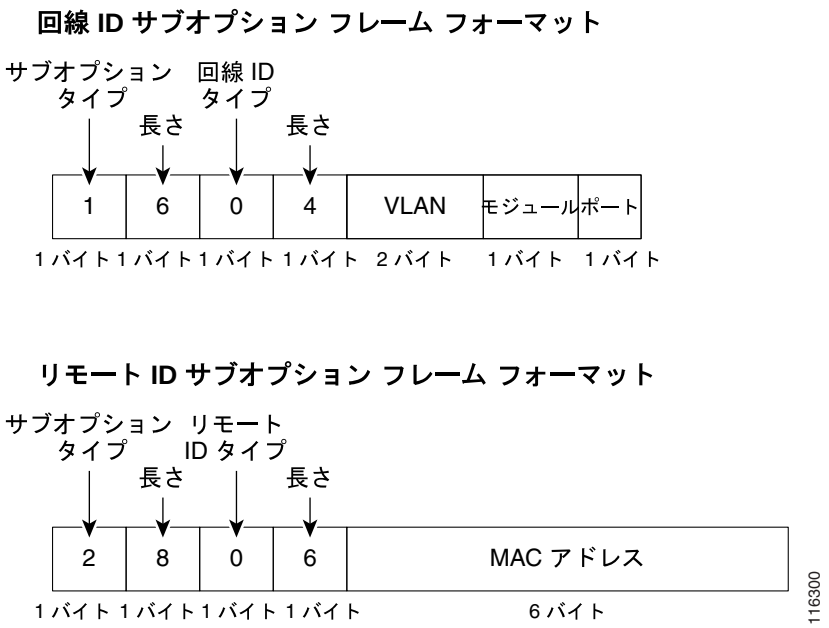


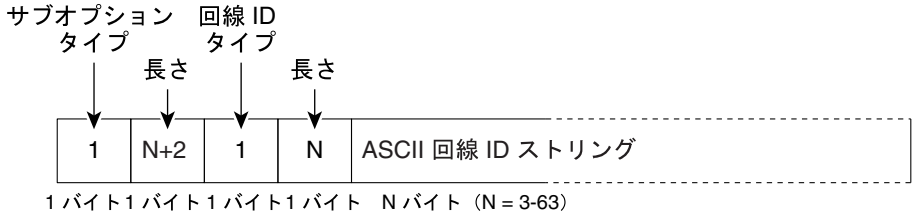
図 21-3 は、ユーザ設定済みのリモート ID サブオプションおよび回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチで次のパケット フォーマットが使用されます。

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。

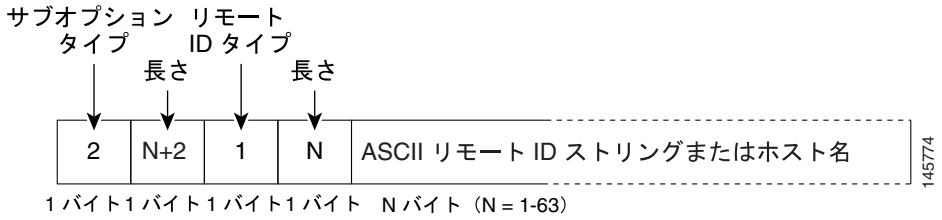
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定するストリングの長さにより変わります。

図 21-3　ユーザ設定済みのサブオプション パケット フォーマット

回線 ID サブオプション フレーム フォーマット（ユーザ設定済みストリングの場合）



リモート ID サブオプション フレーム フォーマット（ユーザ設定済みストリングの場合）



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*、ブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てることも、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。データベースには最大で 8192 のバインディングを保存できます。

各データベース エントリ（*binding*）には、IP アドレス、関連 MAC アドレス、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、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でファイルにバインディングを保存します。各エントリの末尾には、ファイルの先頭からのすべてのバイトを、エントリに関連付けられたすべてのバイトで確認するチェックサムがあります。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る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 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 スヌーピングのみ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場合があります。

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更新され、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したエントリと前のファイル更新に関連したエントリとを区別します。

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 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 スヌーピング信頼インターフェイスの場合。

DHCP 機能の設定

ここでは、スイッチに DHCP サーバ、DHCP リレー エージェント、DHCP スヌーピング、Option 82、Cisco IOS DHCP サーバ バインディング データベース、スイッチの DHCP スヌーピング データベースを設定する方法について説明します。

DHCP のデフォルト設定

表 21-1 に、DHCP のデフォルト設定を示します。

表 21-1　DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	イネーブル[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]
Cisco IOS DHCP サーバ バインディング データベース	イネーブル[3]
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け付ける DHCP スヌーピング オプション[4]	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
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[3]	イネーブル

1. スイッチは、DHCP サーバとして設定されている場合のみ 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 SVI 上に設定されている場合にのみ DHCP パケットをリレーします。
3. スイッチは、DHCP サーバとして設定されているデバイスからのみネットワーク アドレスおよび設定パラメータを取得します。
4. スイッチがエッジ スイッチから Option 82 情報を持ったパケットを受信する集約スイッチである場合に、この機能を使用します。

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に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おり、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** グローバル 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デバイスを必ず設定します。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。
- スイッチで多数の回線 ID を設定しているときは、長い文字列が NVRAM（不揮発性 RAM）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。回線 ID が他のデータとの組み合わせにより、NVRAM またはフラッシュ メモリの許容量を超えた場合は、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を必ず設定します。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、**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するように設定します。
- 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信頼できないポートに設定します。
- 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場合は、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 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の URL（TFTP や FTP など）の場合、この URL でスイッチがバインディング ファイルにバインディングを書き込めるようになるには、設定された 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。TFTP サーバには、この方法で設定することができないものがあります。
  - データベースのリース時間が正確であることを確実にするために、NTP をイネーブルにし、設定することを推奨します。詳細については、「NTP の設定」（p.6-4）を参照してください。
  - NTP が設定されている場合、スイッチは、スイッチのシステム クロックが NTP と同期しているときにのみ、バインディング変更をバインディング ファイルに書き込みます。
- **ip dhcp snooping information option allowed-untrusted** コマンドを、信頼できないデバイスが接続されている集約スイッチに入力しないでください。このコマンドを入力すると、信頼できないデバイスが Option 82 情報をスプーフィングする場合があります。

DHCP サーバの設定

スイッチは DHCP サーバとして機能します。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェント機能はスイッチ上でイネーブルですが、設定されていません。これらの機能は動作可能ではありません。

スイッチを DHCP サーバとして設定する手順については、『*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 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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service dhcp**	スイッチ上で DHCP サーバとリレー 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**	イネーブル EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCP サーバおよびリレー 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「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（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、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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
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*	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、スイッチ仮想インターフェイスを作成します。
ステップ 3	**ip address** *ip-address subnet-mask*	IP アドレスおよび 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。

	コマンド	説明
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と、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface range** *port-range* または **interface** *interface-id*	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。
ステップ 7	**switchport mode access**	ポートの VLAN メンバーシップ モードを定義します。
ステップ 8	**switchport access vlan** *vlan-id*	ステップ 2 で設定したものと同じ VLAN にポートを割り当てます。
ステップ 9	**end**	イネーブル EXEC モードに戻ります。
ステップ 10	**show running-config**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

DHCP スヌーピングおよび Option 82 のイネーブル化

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

	コマンド	説明
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 番号で識別された単独の VLAN ID、カンマで区切られた一連の VLAN ID、ハイフンで区切られた VLAN ID の範囲、またはスペースで区切られた開始および終了 VLAN ID を使用して区切られた VLAN ID 範囲を入力できます。
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。 デフォルトではイネーブルです。

	コマンド	説明
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（スペースを除く） • 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 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の場合、スイッチをイネーブルにして、エッジ スイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを受信します。 デフォルトはディセーブルです。 **（注）** 集約スイッチが信頼できるデバイスに接続されている場合にのみ、このコマンドを入力する必要があります。
ステップ 7	**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、設定するインターフェイスを指定します。
ステップ 8	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id 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 およびポートの ID を、1 ～ 4094 の範囲の VLAN ID を使用して指定します。 回線 ID は 3 ～ 63 文字の ASCII 文字列（スペースを除く）で設定することができます。 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。
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として設定します。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。デフォルトは untrusted です。
ステップ 10	**ip dhcp snooping limit rate** *rate*	（任意）インターフェイスが受信できる毎秒ごとの 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）** 信頼でき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 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。

	コマンド	説明
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 13	**end**	イネーブル EXEC モードに戻ります。
ステップ 14	**show running-config**	設定を確認します。
ステップ 15	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジ スイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを廃棄するよう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 100 パケット / 秒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 gigabitethernet1/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

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

DHCP スヌーピングがすでに プライマリ VLAN に設定されていて、DHCP スヌーピングをセカンダリ VLAN とは異なるように設定した場合、セカンダリ VLAN の設定は有効になりません。DHCP スヌーピングをプライマリ VLAN に設定する必要があります。DHCP スヌーピングがプライマリ VLAN に設定されておらず、VLAN 200 などのセカンダリ VLAN に DHCP スヌーピングを設定した場合、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 イネーブル 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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
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*}	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*	停止するまでに、データベース転送プロセスの終了を待つ時間を秒単位で指定します。 指定できる範囲は 0 ～ 86400 です。0 を設定すると、待ち時間が無限になります。デフォルト値は 300 秒（5 分）です。
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伝送が遅延する期間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルト値は 300 秒（5 分）です。
ステップ 5	**end**	イネーブル 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。 追加する各エントリに対してこのコマンドを入力します。 **（注）** このコマンドは、スイッチのテスト中やデバッグ中に使用します。
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クリアするには、**clear ip dhcp snooping database statistics** イネーブル 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** イネーブル 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* イネーブル 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 21-2 に示す、1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 21-2　DHCP 情報表示用のコマンド

コマンド	説明
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のみを表示します。[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 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、スイッチは手動設定されたバインディングを削除しません。

（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、スイッチはスタティックに設定されたバインディングを削除しません。

IP ソース ガードの概要

IP ソース ガードは、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した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。IP ソース ガード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 ソース バインディング テーブル内の送信元 IP アドレスの IP トラフィックのみを許可し、他のトラフィックをすべて拒否できます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP ソース 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、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のみ、IP ソース 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 ポートでのみサポートされます。IP ソース ガードを、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 フィルタリングとともに設定できます。

送信元 IP アドレス フィルタリング

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 ソース 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 ソース 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 ソース 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再び適用します。

IP ソース バインディング（DHCP スヌーピングでダイナミックに学習されたか手動で設定された）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 ソース 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。

送信元 IP および MAC アドレス フィルタリングがある IP ソース ガード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 ソース バインディングと一致する場合、スイッチはパケットを転送します。スイッチは、DHCP パケットを除く、他のすべてのタイプのパケットを廃棄します。

スイッチは、ポート セキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポート セキュリティ違反が発生する場合はインターフェイスをシャット ダウンできます。

IP ソース ガードの設定

ここでは、スイッチで IP ソース ガードを設定する方法について説明します。

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

IP ソース ガードの設定時の注意事項は次のとおりです。

- スタティック IP バインディングは非ルーテッド ポートでのみ設定できます。**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、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.
  ```

- 送信元 IP フィルタリングのある IP ソース ガードが VLAN でイネーブルの場合、DHCP スヌーピングは、インターフェイスが所属するアクセス 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 ガードをイネーブルにしていて、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 イネーブルまたはディセーブルにする場合、スイッチが適切にトラフィックをフィルタリングしない場合があります。

- 送信元 IP および MAC アドレス フィルタリングがある IP ソース ガードがイネーブルの場合、DHCP スヌーピングおよびポート セキュリティがインターフェイスでイネーブルでなければなりません。
- 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。
- IEEE 802.1x ポートベース認証がイネーブルである場合は、IP ソース ガード機能をイネーブルにすることができます。
- Ternary CAM（TCAM）エントリ数が使用可能な最大数を超えた場合は、CPU の使用量が増加します。

IP ソース ガードのイネーブル化

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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
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*	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、設定するインターフェイスを指定します。
ステップ 3	**ip verify source** または **ip verify source port-security**	送信元 IP アドレス フィルタリングがある IP ソース ガードをイネーブルにします。 IP ソース ガードと送信元 IP および MAC アドレス フィルタリングをイネーブルにします。 （注） **ip verify source port-security** インターフェイス コンフィギュレーション コマンドを使用して、IP ソース ガードとポート セキュリティの両方をイネーブルにしたときは、2 つの注意事項があります。 • DHCP サーバは 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のみ、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 ソース バインディングを追加します。 各スタティック バインディングに対してこのコマンドを入力します。
ステップ 6	**end**	イネーブル EXEC モードに戻ります。
ステップ 7	**show ip verify source** [**interface** *interface-id*]	すべてのインターフェイスまたは特定のインターフェイスに対して IP ソース ガード設定を表示します。
ステップ 8	**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**inteface** *interface-id*] [**vlan** *vlan-id*]	スイッチ、特定の VLAN、または特定のインターフェイス上の IP ソース バインディングを表示します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

送信元 IP アドレス フィルタリングがある 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 ソース バインディング エントリを削除するには、**no ip source global** コンフィギュレーション コマンドを使用します。

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Switch(config)# end
```

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 21-3 に示すイネーブル EXEC コマンドを 1 つまたは複数組み合わせて使用します。

表 21-3　IP ソース ガード情報の表示用コマンド

コマンド	説明
show ip source binding	スイッチの IP ソース 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。