CHAPTER 22

DHCP 機能および IP ソース ガードの設定

この章では、Catalyst 3750 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 ガード機能を設定する手順についても説明します。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（注） この章で使用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 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だけが 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。

ここでは、以下について説明します。

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」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の指定したアドレス プールから IP アドレスを DHCP クライアントに割り当てて、それを管理します。DHCP サーバが DHCP クライアントの要求するコンフィギュレーション パラメータをデータベースから提供できない場合、要求をネットワーク管理者が定義する 1 つまたは複数のセカンダリ DHCP サーバに転送できます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバ間で DHCP パケットを転送するレイヤ 3 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、両者間の要求および応答を転送します。リレー エージェントの転送は、IP データグラムがネットワーク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て新しい DHCP メッセージを生成し、これを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 メッセージのフィルタリングおよび 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）の構築および維持により、ネットワーク セキュリティを提供する DHCP のセキュリティ機能です。データベースの詳細については、「DHCP スヌーピング情報の表示」（p.22-16）を参照してください。

DHCP スヌーピングは、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。DHCP スヌーピングを使用すると、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方法も提供します。

（注）　DHCP スヌーピングを適切に機能させるには、すべての DHCP サーバ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 プロバイダーの環境で使用する場合、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外のデバイスから送信されます。不明なデバイスからのメッセージは、トラフィック攻撃の送信元である可能性があるので、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、バインド タイプ、VLAN（仮想 LAN）番号、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したインターフェイス情報が登録されています。このデータベースには、信頼されるインターフェイスと相互接続す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、信頼されるインターフェイスは同じネットワーク内にあるデバイス上のポートに接続されます。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や、ネットワーク外にあるデバイス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からパケットを受信し、そのインターフェイスが DHCP スヌーピングをイネーブルにしている VLAN に属している場合、スイッチは、送信元 MAC アドレスおよび DHCP クライアント ハードウェア アドレスを比較します。アドレスが一致する場合（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。

次のいずれかの状況が発生すると、スイッチは DHCP パケットを廃棄します。

- 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部から着信した場合
- 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 アドレスおよび DHCP クライアント ハードウェア アドレスが一致しない場合
- DHCP スヌーピング バインディング データベースに MAC アドレスのある DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージをスイッチが受信したが、バインディング データベースのインターフェイス情報が、メッセージを受信したインターフェイスと一致しない場合
- DHCP リレー エージェントが、リレー エージェント IP アドレス（0.0.0.0 以外）を含む DHCP パケットを転送したり、またはリレー エージェントが、Option 82 情報を含むパケットを信頼できないポートへ転送した場合

スイッチが DHCP スヌーピングをサポートする集約スイッチで、DHCP Option 82 情報を挿入しているエッジ スイッチに接続している場合、Option 82 情報を持つパケットが信頼できないインターフェイスで受信されたときにスイッチはその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る場合、集約スイッチは接続デバイスの 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。

Cisco IOS Release 12.2(25)SEA より以前のソフトウェア リリースで稼働するエッジ スイッチによって Option 82 情報が挿入された場合、DHCP スヌーピングを集約スイッチに設定できません。DHCP スヌーピング バインディング データベースが適切に構築されないからです。また、スタティック バインディングまたは Address Resolution Protocol（ARP）Access Control List（ACL; アクセス制御リスト）を使用しない場合、IP ソース ガードとダイナミック ARP 検査をスイッチに設定できません。

Cisco IOS Release 12.2(25)SEA 以降では、集約スイッチが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て **ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力した場合、集約スイッチはエッジ スイッチから Option 82 情報を持つ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ているホストのバインディングを学習します。ホストと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スイッチが Option 82 情報を持つパケットを受信している間も、ダイナミック ARP 検査や IP ソース ガードなどの DHCP セキュリティ機能は集約スイッチでイネーブルのままです。集約スイッチに接続されているエッジ スイッチ上のポートは、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。

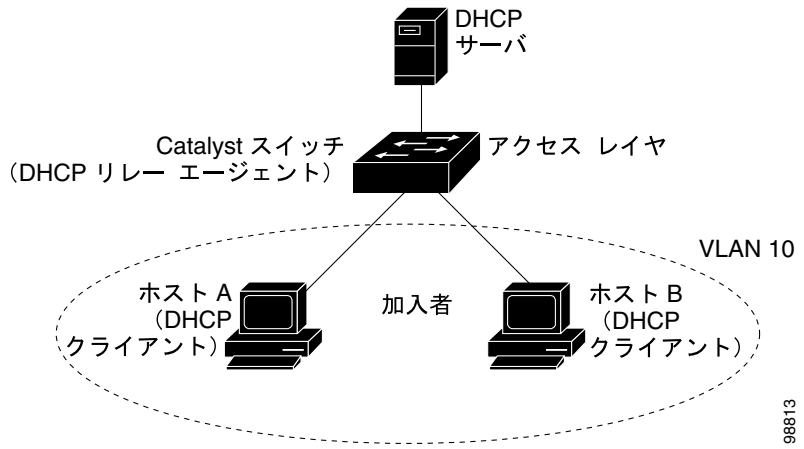
Option 82 データ挿入

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の場合に、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 でのみサポートされます。

図 22-1 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（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 22-1　メトロポリタン イーサネット ネットワークの DHCP リレー エージェント



スイッチで DHCP スヌーピング情報 Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- 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。Option 82 情報には、スイッチの MAC アドレス（リモート ID サブオプション）およびパケットの受信ポートの識別子である **vlan-mod-port**（回線 ID サブオプション）が含まれます。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケット内に追加します。
- スイッチは、Option 82 フィールドを含む 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。

前述のイベントが発生したとき、図 22-2 の次のフィールドの値は変化しません。

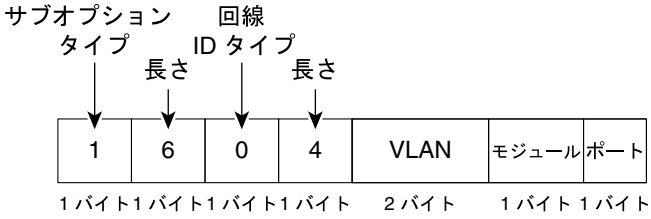
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 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 x/0/1 ポート、ポート 4 がファスト イーサネット x/0/2 ポートのようになります。x はスタック メンバー番号です。ポート 27 は SFP モジュール スロット x/0/1 のようになります。

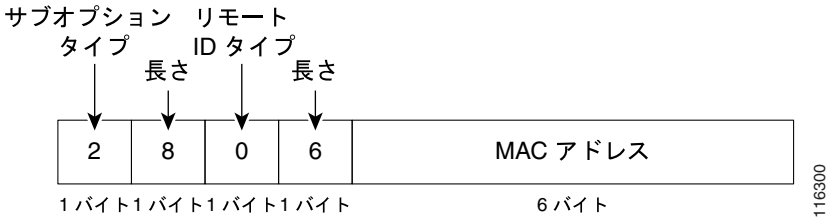
図 22-2 に、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションの場合、モジュール番号がスタック内のスイッチ番号に対応します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力される場合にこのパケット形式を使用します。

図 22-2　サブオプション パケット形式

回線 ID サブオプション フレーム形式



リモート ID サブオプション フレーム形式



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では、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。IP アドレス、*address bindings*、ブート ファイルなどのコンフィギュレーション パラメータが含まれています。

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 アドレスと 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できます。または 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ができます。手動または自動アドレス 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 8192 個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、対応する MAC アドレス、リース時間（16 進表記）、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で、バインディングをファイルに保存します。各エントリの末尾は、ファイルの先頭からエントリに関連する全バイトまでの総バイト チェックサムです。各エントリは、72 バイトのあとにスペース、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 スヌーピングのみ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 DHCP スプーフィング攻撃を防止できないことがあります。

リロードしたとき、スイッチは DHCP スヌーピング バインディング データベースを構築するため、バインディング ファイルを読み込みます。データベースが変更されると、スイッチはファイルを更新します。

スイッチが新しいバインディングを学習するかバインディングを失ったとき、スイッチはデータベース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。

次に、バインディングのあるファイル形式を示します。

```
<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、ファイルを読み込んだとき、スイッチがエントリを確認するのに使用するチェックサム値のタグが付いています。最初の行の *initial-checksum* エントリでは、最後のファイル更新に対応付けられたエントリと、前のファイル更新に対応付けられた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 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
```

スイッチが起動し、計算されたチェックサム値が保存されたチェックサム値と等しくなる場合、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込み、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すると、スイッチはエントリをすべて無視します。

- スイッチはエントリを読み込み、計算されたチェックサム値が保存されたチェックサム値と等しくなりません。エントリとそのあとのエントリが無視されます。
- エントリには、リース時間の期限があります（リース時間が満了したときにスイッチがバインディング エントリを削除しない場合）。
- エントリのインターフェイスはシステムにありません。
- インターフェイスは、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です。

DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに参加すると、スイッチはスタック マスターから DHCP スヌーピング設定を受信します。メンバーがスタックから脱退した場合は、スイッチに関連付けられたすべての DHCP スヌーピング アドレス バインディングが無効になります。

スタック マージが発生し、スタック マスターがもはやスタック マスターでなくなると、そのスタック マスター内のすべての DHCP スヌーピング バインディング（スタック マスターは除く）が失われます。スタック分割により、既存のスタック マスターは変更されませんが、分割されたスイッチに所属するバインディングは、無効になります。分割されたスタックの新しいマスターは、新たに着信する DHCP パケットの処理を開始します。スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

DHCP 機能の設定

ここでは、次の設定について説明します。

DHCP のデフォルト設定

表 22-1 に、DHCP のデフォルト設定を示します。

表 22-1　DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル。設定が必要[1]
DHCP リレー エージェント	イネーブル[2]
DHCP パケットの転送アドレス	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）[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上のパケットを受け入れる 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 アドレス確認	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[4]
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。宛先が設定されている場合のみ、この機能は有効

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 に設定されている場合のみ、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 スイッチの Option 82 情報を持つパケットを受信する集約スイッチに対してのみ使用します。
4. スイッチは DHCP サーバとして設定されたデバイスからのみ、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。

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す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 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 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が設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりすることのできる IP アドレスを指定するか、またはこれらのデバイスに DHCP オプションを設定する必要があります。
- スイッチに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりすることができる IP アドレスを指定する、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 DHCP スヌーピングがディセーブルの場合、DHCP Option 82 データ挿入機能が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、ポートを信頼できるように設定するには、**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、ポートを信頼できないものとして設定するには、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力します。
- DHCP スヌーピング バインディング データベースの設定時は、次の注意事項に従ってください。
  - NVRAM（不揮発性 RAM）とフラッシュ メモリのストレージ容量は制限されているので、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、スイッチが設定したバインディング ファイルにバインディングを書き込む前に、その URL で空のファイルを作成しておく必要があります。先にサーバで空のファイルを作成する必要があるかどうかを判断するには、TFTP サーバのマニュアルを参照してください。一部の TFTP サーバはこの方法では設定することができません。
  - データベースのリース時間を正確にするには、Network Time Protocol（NTP）をイネーブルにして、設定することを推奨します。詳細については、「NTP の設定」（p.7-5）を参照してください。
  - NTP が設定されており、スイッチ システム クロックが NTP と同期化している場合にのみ、スイッチはバインディング変更をバインディング ファイルに書き込みます。
- 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 **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した場合、信頼できないデバイスは Option 82 情報をスプーフィングする可能性があります。

DHCP サーバの設定

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

スイッチでの DHCP サーバの設定手順の詳細については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP addressing and Services」の章にある「Configuring DHCP」を参照してください。

DHCP サーバとスイッチ スタック

データベースをバインドする DHCP は、スタック マスターで管理されます。新しいスタック マスターが割り当てられる場合は、新しいマスターは保存されているバインド データベースを TFTP サーバからダウンロードします。スタック マスターに障害が生じると、保存されていないバインド データベースは失われます。失われたバインドに関連する IP アドレスは、解除されます。**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] グローバル コンフィギュレーション コマンドを使用して、自動バックアップを設定する必要があります。

スタック マージが発生すると、スタック メンバーとなるスタック マスターは、すべての DHCP リースのバインドを失います。スタックを分割すると、分割された新しいマスターは、既存の DHCP リースのバインドではなく、新しい DHCP サーバの動作をします。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

DHCP 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 サーバおよびリレー エージェントをイネーブルにします。デフォルトでは、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。

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

- 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 サーバと 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、**ip helper-address** *address* インターネット コンフィギュレーション コマンドでスイッチを設定する必要があります。一般的には、クライアントに一番近いレイヤ 3 インターフェイスでコマンドを設定します。**ip helper-address** コマンドで使用されるアドレスは、特定の DHCP サーバ IP アドレスを使用するか、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にネットワーク アドレスを使用できます。ネットワーク アドレスを使用すると、任意の DHCP サーバで要求を応答できます。

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*	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 アドレスを特定の DHCP サーバ アドレスにすることができます。また他の DHCP サーバが宛先ネットワーク セグメントにある場合にネットワーク アドレスを使用できます。ネットワーク アドレスを使用すると、他のサーバで DHCP 要求に応答できます。 複数のサーバがある場合、1 つのヘルパー アドレスを各サーバに設定できます。
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た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た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*	ポートをステップ 2 で設定された同じ VLAN に割り当てます。
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場合は、**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。

	コマンド	説明
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 番号で識別される単一 VLAN ID、カンマで分離された一連の VLAN ID、ハイフンで分離された VLAN ID の範囲、開始および終了 VLAN ID をスペースで分離した VLAN ID の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。これがデフォルト設定です。
ステップ 5	**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ている集約スイッチの場合、エッジ スイッチからの Option 82 情報を持つ着信 DHCP スヌーピング パケットを受け入れるようにスイッチをイネーブルにします。 デフォルトではディセーブルです。 **（注）** このコマンドは、信頼できるデバイスに接続された集約スイッチにのみ入力する必要があります。
ステップ 6	**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 7	**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、**no** キーワードを使用します。デフォルトでは untrusted です。
ステップ 8	**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。デフォルトの場合、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。信頼され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 スヌーピングがイネーブルである複数の VLAN に割り当てられたトランク ポートである場合、レート制限を増やす必要があります。
ステップ 9	**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 10	**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 11	**end**	イネーブル EXEC モードに戻ります。
ステップ 12	**show running-config**	設定を確認します。
ステップ 13	**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 情報を持つ着信 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、DHCP スヌーピングをグローバルに VLAN 10 でイネーブルにし、ポートのレート制限を毎秒 100 パケットに設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライベート VLAN で DHCP スヌーピングをイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN、および対応付けられたセカンダリ VLAN 両方に伝播されます。プライマリ VLAN で DHCP スヌーピングがイネーブルの場合、DHCP スヌーピングはセカンダリ VLAN で設定されます。

DHCP スヌーピングがすでにプライマリ VLAN で設定され、セカンダリ VLAN に別の設定で DHCP スヌーピングを設定する場合、セカンダリ VLAN の設定は有効になりません。プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピングがプライマリ VLAN で設定されていない場合、DHCP スヌーピングを VLAN 200 などのセカンダリ VLAN 上に設定する際に次のような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 コマンド出力では、DHCP スヌーピングがイネーブルであるプライマリおよびセカンダリ プライベート VLAN を含む、すべての VLAN を表示します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースのイネーブルおよび設定手順の詳細については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「Configuring DHCP」の章にある「DHCP Configuration Task List」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および設定するには、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**[*number*]**:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** | **rcp:**//*user@host*/*filename*}| **tftp:**//*host*/*filename*	次の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 ファイル用に URL を指定します。 • **flash**[*number*]**:**/*filename* （任意）スタック マスターのスタック メンバー番号を指定するには、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*image-name*.**tar** • **rcp:**//*user@host*/*filename* • **tftp:**//*host*/*filename*
ステップ 3	**ip dhcp snooping database timeout** *seconds*	データベース転送プロセスを停止するまでの待ち時間を秒単位で指定します。 デフォルト値は 300 秒です。範囲は 0 ～ 86400 です。値を 0 に指定すると、無期限に転送を続行します。
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、転送が遅延する時間を指定します。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）バインディング エントリを 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。*vlan id* の範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。 追加するエントリそれぞれに、このコマンドを入力します。 **（注）** スイッチのテストやデバッグを行うとき、このコマンドを使用します。
ステップ 7	**show ip dhcp snooping database** [**detail**]	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を止めるには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウト値または遅延値をリセットするには、**ip dhcp snooping database timeout** *seconds* または **ip dhcp snooping database write-delay** *seconds* グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報を消去するには、**clear ip dhcp snooping database statistics** 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 データベースからバインディング 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。削除するエントリそれぞれに、このコマンドを入力します。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 22-2 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 22-2　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	DHCP スヌーピング バインディング データベース（別名バインディング テーブル）内のダイナミックに設定されたバンディングのみを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip 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、DHCP スヌーピング バインディング データベースおよび手動で設定された IP ソース バインディングに基づきトラフィックをフィルタリングすることで、非ルーテッドのレイヤ 2 インターフェイス上で 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、ホストがネイバの IP アドレスを使用するときに発生するトラフィック攻撃を防げます。

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の場合、IP ソース ガードをイネーブルにできます。インターフェイスで IP ソース ガードがイネーブルになると、スイッチはインターフェイスで受信したすべての IP トラフィック（DHCP スヌーピングにより許可された DHCP パケットを除く）をブロックします。ポート ACL はインターフェイスに適用されます。ポート ACL は、IP ソース バインディング テーブル内の送信元 IP アドレスのある IP トラフィックのみを許可し、それ以外のトラフィックをすべて拒否します。

IP ソース バインディング テーブルには、DHCP スヌーピングによって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、対応付けられた MAC アドレス、対応付けられた VLAN 番号が含まれます。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、アクセスおよびトランク ポートを含めたレイヤ 2 ポートでのみサポートされます。IP ソース ガードに送信元 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 フィルタリングを設定できます。

ここでは、以下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.22-17）
- 送信元 IP および MAC アドレス フィルタリング（p.22-18）

送信元 IP アドレス フィルタリング

このオプションで IP ソース ガードがイネーブルの場合、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 テーブルのバインディングと一致する場合、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、インターフェイス上で追加、変更、または削除された場合、スイッチは IP ソース バインディングの変更を利用してポート ACL を変更し、再びポート ACL をインターフェイスに適用します。

IP ソース バインディング（DHCP スヌーピングによってダイナミックに学習、または手動で設定）が設定されていないインターフェイス上で、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 IP トラフィックをすべて拒否するポート ACL を作成および適用します。IP ソース ガードをディセーブルにする場合、スイッチはインターフェイスからポート ACL を削除します。

送信元 IP および MAC アドレス フィルタリング

このオプションで IP ソース ガードがイネーブルの場合、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。送信元 IP 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のみ、スイッチはトラフィックを転送します。

送信元 IP および MAC アドレス フィルタリングのある 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 アドレスと有効な IP ソース バインディングが一致する場合、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 タイプ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すると、インターフェイスは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、次の設定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

ここでは、IP ソース ガードの設定時の注意事項を説明します。

- 非ルーテッド ポートにのみ、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.
  ```

- 送信元 IP フィルタリングのある IP ソース ガードが、VLAN 上でイネーブルの場合、インターフェイスが属するアクセス VLAN 上で 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 のあるトランク インターフェイスで IP ソース ガードをイネーブルにし、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 上に適用されます。

（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場合、スイッチはトラフィックを正常にフィルタリングできないことがあります。

- 送信元 IP および MAC アドレス フィルタリングのある 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 セキュリティをインターフェイス上でイネーブルにする必要があります。
- プライベート VLAN が設定されているインターフェイス上で 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の場合に、この機能をイネーブルにできます。
- Ternary CAM（TCAM）エントリ数が利用可能な最大数を超えた場合、CPU の使用が増加します。

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*	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 フィルタリングのある 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 フィルタリングのある 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、セキュアな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だけ、DHCP クライアントの MAC アドレスはセキュア アドレスとして学習されます。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **inteface** *interface-id*	スタティック IP ソース バインディングを追加します。 このコマンドを各スタティック バインディングに入力します。
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*]	インターフェイスすべて、または特定のインターフェイスの 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 フィルタリングのある 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** 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 11 で送信元 IP および MAC フィルタリングのある 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 gigabitethernet1/0/1
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 22-3 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 22-3　IP ソース ガード情報の表示用のコマンド

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 ガードの設定を表示します。