



DHCP 機能の設定

この章では、Catalyst 3550 スイッチで Dynamic Host Configuration Protocol (DHCP) スヌーピングおよび Option 82 データ挿入機能を設定する方法について説明します。



(注)

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

この章で説明する内容は、次のとおりです。

- [DHCP 機能の概要 \(p.19-2\)](#)
- [DHCP 機能の設定 \(p.19-9\)](#)
- [DHCP 情報の表示 \(p.19-19\)](#)

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 環境で広く使用されています。DHCP を使用すると IP アドレス管理のオーバーヘッドが大幅に軽減されます。DHCP を使用すると、IP アドレスをホストに永続的に割り当てる必要がなくなり、IP アドレスを必要とするのはネットワークに接続されているホストだけになるので、DHCP は限られた IP アドレス空間の節約に役立ちます。

スイッチは、次の DHCP 機能をサポートします。

- DHCP サーバ (p.19-2)
- DHCP リレー エージェント (p.19-2)
- DHCP スヌーピング (p.19-2)
- Option 82 データ挿入 (p.19-4)
- Cisco IOS DHCP サーバ データベース (p.19-7)
- DHCP スヌーピング バインディング データベース (p.19-7)

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の指定アドレス プールから、IP アドレスを DHCP クライアントに割り当てて、クライアントを管理します。DHCP サーバは、DHCP クライアントに要求された設定パラメータを、自身のデータベースから渡すことができない場合は、ネットワーク管理者によって定義されている 1 つまたは複数のセカンダリ DHCP サーバに、その要求を転送できます。

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 / サーバ間にある DHCP パケットを転送するレイヤ 3 のデバイスです。クライアントおよびサーバが同一の物理サブネットにない場合、リレー エージェントは、クライアントとサーバ間で要求と応答を転送します。リレー エージェントの転送は、通常のレイヤ 2 転送とは異なります。レイヤ 2 転送では、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交換されますが、リレー エージェントは DHCP メッセージを受信してから、新しい DHCP メッセージを生成して、出力インターフェイスに送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼されない 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 (別名 DHCP スヌーピング バインディング テーブル) を構築および維持することで、ネットワーク セキュリティを提供する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼されないホストと DHCP サーバの間のファイアウォールと同様の機能を果たします。DHCP スヌーピングを使用すると、エンドユーザに接続した信頼されないインターフェイスと、DHCP サーバまたは別のスイッチに接続した信頼されるインターフェイスを区別できます。



(注) DHCP スヌーピングを適切に機能させるには、すべての DHCP サーバが信頼され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。

信頼されないメッセージとは、ネットワークまたはファイアウォールの外から受信されたメッセージのことです。DHCP スヌーピングをサービス プロバイダー環境で使用した場合、信頼されないメッセージはカスタマー スイッチのようにサービス プロバイダー ネットワーク外部のデバイスから送信されたことを意味します。不明なデバイスからのメッセージは、トラフィック攻撃の原因になる可能性があるため信頼されません。

DHCP スヌーピングのバインディング 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、リース期間、バインディング タイプ、VLAN (仮想 LAN) 番号、および信頼されないローカル スイッチのインターフェイスに対応したインターフェイス情報が含まれています。信頼されるインターフェイスと相互接続されているホストに関する情報は含まれていません。

サービス プロバイダー ネットワーク内で、信頼されるインターフェイスは、同じネットワーク内のデバイスにあるポートと接続されていることを意味します。信頼されないインターフェイスは、ネットワーク内で信頼されないインターフェイスと接続しているか、またはネットワーク外にあるデバイスのインターフェイスと接続していることとなります。

スイッチが信頼されないインターフェイスでパケットを受信して、そのインターフェイスが DHCP スヌーピングがイネーブルの VLAN に属している場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスがそのデフォルトと一致した場合、スイッチはパケットを転送します。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、次の状況のいずれかが発生した場合、DHCP パケットを廃棄します。

- DHCP サーバからのパケット (DHCP OFFER、DHCP ACK、DHCP NAK、または DHCP REQUEST など) をネットワークまたはファイアウォール外から受信する。
- 信頼されないインターフェイスでパケットが受信され、さらに送信元 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。
- スイッチは、DHCP スヌーピング バインディング テーブルの MAC アドレスを含む DHCP RELEASE または DHCP DECLINE ブロードキャスト メッセージを受信したが、バインディング テーブル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。
- リレー エージェントの IP アドレスが 0.0.0.0 でないものを含む DHCP パケットを DHCP リレー エージェントが転送する、または信頼されないポートに Option 82 情報を含むパケットをリレー エージェントが転送する。

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、パケットが信頼されないインターフェイス上で受信されると、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されるポートで受信された場合、集約スイッチは接続したデバイスの DHCP スヌーピング バインディングを学習しないので完全な 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 12.1(22)EA3 より前の、または Cisco IOS Release 12.2(25)SEA 以降のソフトウェア 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、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ので、DHCP スヌーピングを集約スイッチに設定できません。スタティック バインディングまたは Address Resolution Protocol (ARP; アドレス解決プロトコル) Access Control List (ACL; アクセス制御リスト) を使用していない場合、IP ソース ガードおよびダイナミック ARP 検査もスイッチに設定できません。

Cisco IOS Release 12.1(22)EA3 および Cisco IOS Release 12.2(25)SEA 以降では、集約スイッチが信頼されないインターフェイスを通じてエッジ スイッチに接続でき、`ip dhcp snooping information option allow-untrusted` グローバル コンフィギュレーション コマンドを入力した場合に、集約スイッチは Option 82 情報を持ったパケットをエッジ スイッチから受け付けます。集約スイッチは、信頼されないスイッチ インターフェイスを通じ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

る信頼され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するエッジスイッチのポートは、信頼され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 によって多数の加入者の IP アドレス割り当てを中央管理できます。スイッチで DHCP Option 82 機能をイネーブルにすると、(MAC アドレスのほかに)ネットワークへの接続に使用されているスイッチポートで加入者のデバイスを識別できます。加入者 LAN 上の複数のホストをアクセススイッチの同じポートに接続し、個別に識別できます。

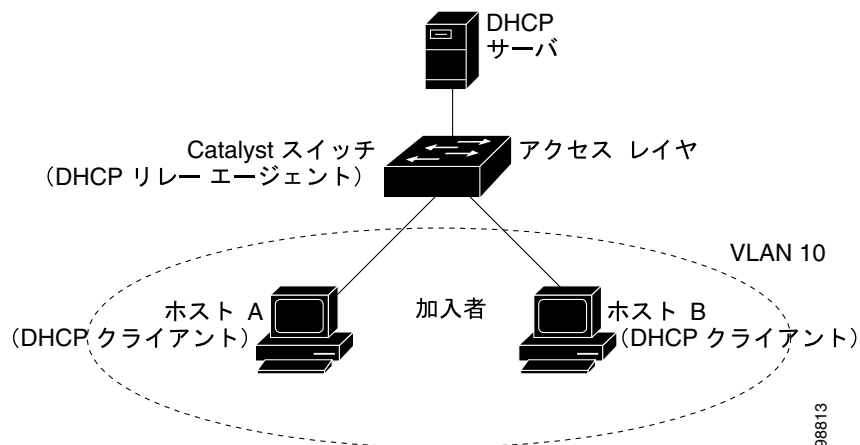


(注)

Cisco IOS Release 12.1(19)EA1 以降では、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のデバイスが割り当てられている VLAN に存在する場合のみ、DHCP Option 82 機能がサポートされます。また、スイッチは、DHCP がディセーブルのときに DHCP Option 82 機能もサポートします。

図 19-1 に示すメトロポリタンイーサネットネットワークの例では、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されている加入者に IP アドレスを割り当てています。DHCP クライアントとこれらのクライアントに関連付けられている 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ないので、DHCP リレー エージェント (Catalyst スイッチ) にヘルパーアドレスを設定することによって、ブロードキャスト転送、およびクライアント / サーバ間での DHCP メッセージの伝送を可能にしています。

図 19-1 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 スヌーピング情報の Option 82 機能をイネーブルにすると、次の順でイベントが発生します。

- ホスト (DHCP クライアント) が DHCP 要求を作成して、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、Option 82 情報をパケットに追加します。デフォルトで、Option 82 情報には、スイッチ MAC アドレス (リモート ID サブオプション)、および `vlan-mod-port` または `snmp-ifindex` のポート ID が含まれます。このポートからパケットは受信

されます（回線 ID サブオプション）。Cisco IOS Release 12.2(25)SEE から、リモート ID と回線 ID を設定できます。これらのサブオプションを設定する詳細については、「[DHCP スヌーピングおよび Option 82 のイネーブル化](#)」（p.19-15）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 DHCP パケットに IP アドレスを追加します。
- スwitchは Option 82 フィールドが含まれる DHCP 要求を DHCP サーバに転送します。
- DHCP サーバがパケットを受信します。サーバが Option 82 対応の場合、そのサーバはリモート 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るとともに、単一のリモート ID または回線 ID に割り当て可能な IP アドレス値制限などのポリシーを適用できます。さらに DHCP サーバは DHCP 応答内に Option 82 フィールドをエコーします。
- 要求がスイッチによって DHCP サーバへリレーされた場合、DHCP サーバはスイッチへの応答をユニキャストします。クライアントおよびサーバが同じサブネットに存在する場合、サーバは応答をブロードキャストします。スイッチは、リモート ID および（可能であれば）回線 ID フィールドを調べて、本来 Option 82 データが挿入されていたかを確認します。スイッチは Option 82 フィールドを削除してから、そのパケットを DHCP クライアント（DHCP 要求の送信元）に接続されているスイッチ ポートに転送します。

デフォルトのサブオプション設定では、説明した一連のイベントが発生した場合、[図 19-2](#) の例 1 と 2 にある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

[図 19-2](#) の例 3 では、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ています。このスイッチは、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 コマンドと `ip dhcp snooping vlan information option format-type circuit-id string` インターフェイス コンフィギュレーション コマンドを入力した場合にこれらのパケット形式を使用します。

リモート ID および回線 ID サブオプションを設定する際に、パケット内にある次のフィールドの値は、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 タイプが 1 です。
 - 設定した文字列の長さに応じて長さの値が変化します。
- リモート ID サブオプション フィールド
 - リモート ID タイプが 1 です。

設定した文字列の長さに応じて長さの値が変化します。

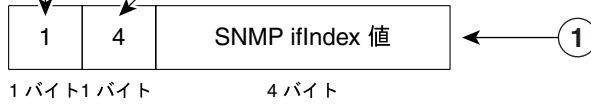
DHCP スヌーピングがグローバルにイネーブルのときに、`ip dhcp snooping information option` グローバル コンフィギュレーション コマンドを入力し、SNMP（簡易ネットワーク管理プロトコル）ifIndex フォーマットを設定しない場合、回線 ID サブオプションのポート フィールドのポート番号は 0 から始まります。たとえば、Catalyst 3550-24 スwitchでは、ポート 0 は FastEthernet 0/1 ポートで、ポート 1 が FastEthernet 0/2 ポート、ポート 2 が FastEthernet 0/3 ポートと続きます。ポート 24 は GBIC（ギガビット インターフェイス コンバータ）ベースのギガビット モジュール スロット 0/1 で、ポート 25 が GBIC ベースのギガビット モジュール スロット 0/2 になります。

図 19-2 に、デフォルトとユーザ設定のリモート ID サブオプションおよび回線 ID サブオプションの packets 形式を示します。回線 ID サブオプションでは、モジュール フィールドは常に 0 です。

図 19-2 サブオプションの packets 形式

回線 ID サブオプション フレーム形式

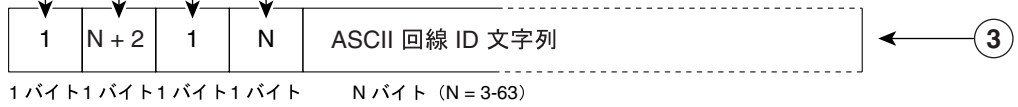
サブオプション
タイプ 長さ



サブオプション 回線 ID
タイプ 長さ タイプ 長さ

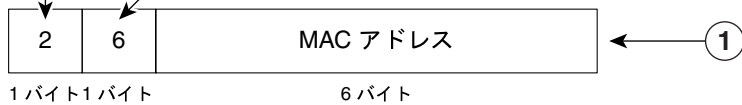


サブオプション 回線 ID
タイプ 長さ タイプ 長さ

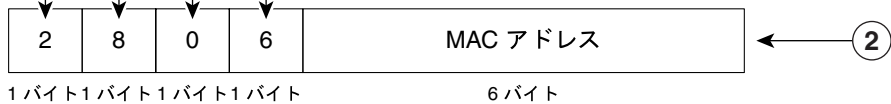


リモート ID サブオプション フレーム形式

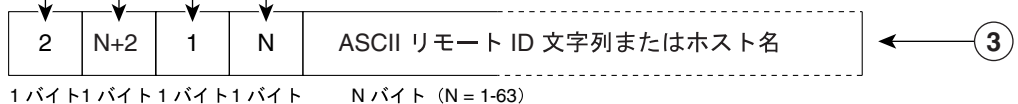
サブオプション
タイプ 長さ



サブオプション リモート ID
タイプ 長さ タイプ 長さ



サブオプション リモート ID
タイプ 長さ タイプ 長さ



145775

1	DHCP スヌーピングがグローバルにイネーブルで、 <code>ip dhcp relay information option</code> 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、さらに <code>ip dhcp snooping information option format snmp-ifindex</code> 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、スイッチはこの形式を使用します。
2	DHCP スヌーピングがグローバルにイネーブルで、 <code>ip dhcp snooping information option</code> 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、さらに SNMP ifIndex フォーマットが設定されていない場合、スイッチはこの形式を使用します。
3	DHCP スヌーピングがグローバルにイネーブルで、 <code>ip dhcp snooping information option format remote-id</code> 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、さらに <code>ip dhcp snooping vlan information option format-type circuit-id string</code> インターフェイス コンフィギュレーション コマンドが入力された場合、スイッチはこの形式を使用します。

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 アドレスの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され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。各エントリの最後には、ファイルの始まりからの全バイトとエントリに関連する全バイトが含まれ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時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、ダイナミック ARP または IP ソース ガードがイネーブル、DHCP スヌーピング バインディング データベースにダイナミック バインディングがある場合、スイッチはその接続を切断します。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、スイッチはその接続を切断しませんが、DHCP スヌーピングが DHCP スプーフィング攻撃を防げないことがあります。

リロード時、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。データベースの変更時にスイッチは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り、バインディングを消失した場合にはただちにデータベース内のエントリを更新します。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、設定変更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) 指定の時間更新されない場合、更新は停止します。

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 行目の *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、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witch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、スイッチで DHCP スヌーピングおよび Option 82 を設定する手順について説明します。

- DHCP のデフォルト設定 (p.19-9)
- DHCP スヌーピング設定時の注意事項 (p.19-10)
- 旧ソフトウェアリリースからのアップグレード (p.19-11)
- DHCP サーバの設定 (p.19-11)
- DHCP リレー エージェントのみのイネーブル化 (p.19-11)
- DHCP リレー エージェントおよび Option 82 のイネーブル化 (p.19-12)
- リレー エージェント情報 Option 82 の検証 (p.19-12)
- 再転送ポリシーの設定 (p.19-13)
- パケット転送アドレスの指定 (p.19-14)
- DHCP スヌーピングおよび Option 82 のイネーブル化 (p.19-15)
- プライベート VLAN での DHCP スヌーピングのイネーブル化 (p.19-17)
- Cisco IOS DHCP サーバ データベースのイネーブル化 (p.19-17)
- 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.19-18)

DHCP のデフォルト設定

表 19-1 に、DHCP のデフォルト設定を示します。

表 19-1 DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアでイネーブル。設定が必要です。 ¹
DHCP リレー エージェント	イネーブル ²
DHCP パケット転送アドレス	設定なし
リレー エージェント情報の確認	イネーブル(無効なメッセージは廃棄されます) ³
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報の置換 ²
DHCP スヌーピングのグローバルなイネーブル化	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
信頼されない入力インターフェイスでパケットを受信する 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 スヌーピング信頼状態	信頼できない
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

表 19-1 DHCP のデフォルト設定 (続き)

機能	デフォルト設定
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアでイネーブル。設定が必要です。 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。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアでイネーブル。設定が必要です。 この機能は宛先が設定されている場合にのみ、動作します。

1. スwitch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witch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witch仮想インターフェイス) で設定されている場合のみ、DHCP パケットをリレーします。
3. スwitchがエッジ スwitchから Option 82 情報を持ったパケットを受信する集約スウィッチである場合に、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。

- DHCP スヌーピングをスイッチでグローバルにイネーブルにする必要があります。
- VLAN で DHCP スヌーピングがイネーブルになるまで、DHCP スヌーピングはアクティブになりません。
- スwitchでグローバルに DHCP スヌーピングをイネーブルにする前に、DHCP サーバとして動作しているデバイスと、DHCP リレー エージェントが設定されてイネーブルの状態にあることを確認してください。
- DHCP スヌーピングをスイッチで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 コマンドは利用できません。これらのコマンドを入力した場合、スイッチがエラー メッセージを戻して、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 option` 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witchに DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能しているデバイスの設定を行う必要があります。たとえば、DHCP サーバが割り当てまたは省略できる 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witchに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能しているデバイスの設定を行う必要があります。たとえば、DHCP サーバが割り当てまたは省略できる 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、もしくは DHCP データベース エージェントを設定する必要があります。
- DHCP リレー エージェントがイネーブルで DHCP スヌーピングがディセーブルの場合、DHCP Option 82 データ挿入機能はサポートされません。
- スwitch 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性のある設定にしてください。

- 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性のない設定にしてください。
- `ip dhcp snooping information option allow-untrusted` コマンドを信頼され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、信頼されないデバイスが Option 82 情報をスプーフィングする場合があります。

旧ソフトウェア リリースからのアップグレード

Cisco IOS Release 12.1(19)EA1 では、Option 82 加入者識別 に関する実装が旧リリースから変更されました。新しい Option 82 形式では、異なる回線 ID およびリモート ID サブオプションの `vlan-mod-port` を使用します。旧バージョンでは、`snmp-ifindex` 回線 ID およびリモート ID サブオプションを使用します。

スイッチに Option 82 が設定され、Cisco IOS Release 12.1(19)EA1 以降にアップグレードする場合、Option 82 の設定に影響はありません。ただし、`ip dhcp snooping` グローバル コンフィギュレーション コマンドを使用してスイッチで DHCP スヌーピングをグローバルにイネーブルにするときは、以前の Option 82 の設定は中断され、新しい Option 82 形式が適用されます。スイッチで DHCP スヌーピングをグローバルにディセーブルにするとき、以前の Option 82 の設定が再びイネーブルになります。

下位互換性を保つには、DHCP スヌーピングをイネーブルにするときに `ip dhcp snooping information option format snmp-ifindex` 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、以前の Option 82 形式を選択できます。DHCP スヌーピングをグローバルにイネーブルにすると、(選択済み形式の) Option 82 情報だけがスヌーピングされた VLAN に挿入されます。

DHCP スヌーピングをイネーブルにしないで Option 82 の旧バージョンを使用するには、「[DHCP リレー エージェントおよび Option 82 のイネーブル化](#)」(p.19-12) を参照してください。

Cisco IOS Release 12.2(25)SEE から、リモート ID と回線 ID サブオプションに ASCII 文字を設定できます。これらのサブオプションを設定する詳細については、「[DHCP スヌーピングおよび Option 82 のイネーブル化](#)」(p.19-15) を参照してください。

DHCP サーバの設定

スイッチは DHCP サーバとして動作させることができます。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、スイッチでイネーブルになっていません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。

DHCP サーバとしてスイッチを設定する手順については、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP addressing and Services」にある「Configuring DHCP」を参照してください。

DHCP リレー エージェントのみのイネーブル化

スイッチで DHCP リレー エージェントをイネーブルにするには、イネーブル 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	<code>configure terminal</code>	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	<code>service dhcp</code>	スイッチで 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、イネーブルに設定されています。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
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。

DHCP リレー エージェントおよび Option 82 のイネーブル化

Cisco IOS Release 12.1(19)EA1 では、Option 82 加入者識別に関する実装が旧リリースから変更されました。DHCP スヌーピングを使用するときのリレー エージェントおよび Option 82 の設定に関する詳細については、「旧ソフトウェア リリースからのアップグレード」(p.19-11)を参照してください。

スイッチで DHCP リレー エージェントおよび Option 82 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行います。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service dhcp	スイッチで DHCP サーバおよびリレー エージェントをイネーブルにします。デフォルトでは、イネーブルに設定されています。
ステップ 3	ip dhcp relay information option	DHCP サーバへの DHCP 要求メッセージ転送時の、DHCP リレー情報 (Option 82 フィールド) の挿入および削除をイネーブルにします。 デフォルトでは、この機能はディセーブルです。
ステップ 4	end	イネーブル EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	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。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 relay 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。

リレー エージェント情報 Option 82 の検証

デフォルトでは、スイッチは DHCP サーバから受信した DHCP 応答パケットの Option 82 フィールドが有効であるかどうかを確認します。無効なメッセージを受信した場合、スイッチはそのメッセージを廃棄します。有効なメッセージを受信した場合、スイッチは Option 82 フィールドを削除してから、そのパケットを転送します。

この機能をディセーブルにするには、no ip dhcp relay information check グローバル コンフィギュレーション コマンドを使用します。この機能をディセーブルにした場合、スイッチは Option 82 フィールドの有効性は検証しませんが、パケットからこのオプションを削除して転送します (スイッチで DHCP スヌーピングがイネーブルのときは、この機能は利用できません)。



(注) スイッチが DHCP クライアントから Option 82 フィールドを含むパケットを受信し、スイッチでこの情報の確認機能がイネーブルになっている場合、クライアント側からのこのような情報は無効であるため、スイッチはそのパケットを廃棄します。ただし場合によっては、クライアント側に Option 82 フィールドが設定されていることもあります。このような場合は、スイッチがパケットから Option 82 フィールドを削除しないように、スイッチの情報確認機能をディセーブルにしなければなりません。ip dhcp relay information policy グローバル コンフィギュレーション コマンドを使用すると、既存の Option 82 情報を含むパケットを受信した場合のスイッチの動作を設定できます。詳細については、「再転送ポリシーの設定」(p.19-13) を参照してください。(スイッチで DHCP スヌーピングがイネーブルのときは、この機能は利用できません)

再転送ポリシーの設定

デフォルトの再転送ポリシーでは、スイッチは DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。このデフォルトのスイッチ動作がご使用のネットワーク構成に適さない場合は、ip dhcp relay information policy {drop | keep | replace} 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、設定を変更できます(スイッチで DHCP スヌーピングがイネーブルのときは、この機能は利用できません)。



(注) 再転送ポリシーを正常に機能させるためには、no ip dhcp relay information check グローバル コンフィギュレーション コマンドを使用して、リレー エージェント情報の確認機能をディセーブルにする必要があります。

再転送ポリシーの動作を変更するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	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 relay information policy {drop keep replace}	再転送ポリシーを設定します。デフォルトでは、既存の情報がスイッチの DHCP リレー情報に置き換えられます(上書きされます)。 <ul style="list-style-type: none"> 既存のリレー情報に Option 82 情報も含まれている場合に、そのメッセージをスイッチが廃棄するように指定するには、drop キーワードを使用します。 既存のリレー情報をスイッチが保持するように指定する場合は、keep キーワードを使用します。
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。

再転送ポリシーをデフォルト設定に戻すには、no ip dhcp relay information policy グローバル コンフィギュレーション コマンドを使用します。

パケット転送アドレスの指定

DHCP リレー エージェントは、同じ物理サブネット上にないクライアントとサーバ間の DHCP パケットを転送する任意のデバイスです。リレー エージェントの転送は、IP ルータによる通常の転送とは異なります。IP ルータの転送では、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交換されますが、リレー エージェントは DHCP メッセージを受信してから、新しい DHCP メッセージを作成して、別のインターフェイスに送信します。

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存在する場合は、**ip helper-address address** インターフェイス コンフィギュレーション コマンドをスイッチに設定する必要があります。通常は、クライアントに最も近いレイヤ 3 インターフェイスにこのコマンドを設定します。**ip helper-address** コマンドには、特定の DHCP サーバの IP アドレスを使用できます。また、宛先のネットワーク セグメントにほかの DHCP サーバがある場合は、ネットワーク アドレスを使用することもできます。ネットワーク アドレスを使用すると、任意の DHCP サーバが要求に応答できるようになります。

パケット転送アドレスを指定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	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 SVI 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 アドレスと 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 アドレスには、特定の DHCP サーバのアドレスを使用できます。また、宛先のネットワーク セグメントにほかの DHCP サーバがある場合はネットワーク アドレスを使用することもできます。ネットワーク アドレスを使用すると、ほかのサーバが DHCP 要求に応答できるようになります。 複数のサーバがある場合は、各サーバに 1 つずつヘルパー アドレスを設定することもできます。
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	switchport mode access	そのポートの VLAN メンバーシップ モードを決定します。
ステップ 8	switchport access vlan vlan-id	ステップ 2 で設定した同じ 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。

次に、DHCP サーバ、リレー エージェント、DHCP リレー情報 (Option 82) の挿入および削除をイネーブルにする例を示します。この例では、VLAN ID 10 のスイッチ仮想インターフェイスを作成し、これに IP アドレスを割り当てて、30.0.0.2 の DHCP パケット転送アドレス (DHCP サーバアドレス) を指定しています。DHCP クライアントに接続されている 2 つのインターフェイス (GigabitEthernet 0/1 および 0/2) は VLAN 10 のスタティック アクセスポートとして設定されています (図 19-1 [p.19-4] を参照)。




```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# service dhcp
Switch(config)# ip dhcp relay information option
Switch(config)# interface vlan 10
Switch(config-if)# ip address 10.0.0.1 255.0.0.0
Switch(config-if)# ip helper-address 30.0.0.2
Switch(config-if)# exit
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチで DHCP スヌーピングをイネーブルにするには、イネーブル 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	<code>configure terminal</code>	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	<code>ip dhcp snooping</code>	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	<code>ip dhcp snooping vlan <i>vlan-range</i></code>	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 は、VLAN ID 番号を特定して VLAN ID を単一で入力したり、カンマ区切りで一連の VLAN ID を入力したり、ハイフン区切りで VLAN ID の範囲を入力したり、スペース区切りで開始と終了の VLAN ID を入力して VLAN ID の範囲を入力したりできます。
ステップ 4	<code>ip dhcp snooping information option</code>	DHCP サーバへの DHCP 要求メッセージ転送時の、DHCP リレー情報 (Option 82 フィールド) の挿入および削除をイネーブルにします。デフォルトはイネーブルです。
ステップ 5	<code>ip dhcp snooping information option format snmp-ifindex</code>	(任意) Option 82 機能の回線 ID およびリモート ID サブオプションの代替フォーマットを選択するには、 <code>ip dhcp snooping information option format snmp-ifindex</code> を指定します。詳細については、「旧ソフトウェア リリースからのアップグレード」(p.19-11) を参照してください。 デフォルト設定は、 <code>no ip dhcp snooping information option format snmp-ifindex</code> です。

■ DHCP 機能の設定

コマンド	目的
ステップ 6 ip dhcp snooping information option format remote-id [string ASCII-string hostname]	<p>(任意) リモート ID サブオプションを指定します。</p> <p>次のようにリモート ID を設定できます。</p> <ul style="list-style-type: none"> 最大 63 の ASCII 文字列 (スペースなし) スイッチの設定済みホスト名 <p> (注) ホスト名が 64 文字以上の場合、リモート ID 設定では 63 文字までに切り捨てられます。</p> <p>デフォルトのリモート ID はスイッチ MAC アドレスです。</p>
ステップ 7 ip dhcp snooping information option allow-untrusted	<p>(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。</p> <p>デフォルトはディセーブルです。</p> <p> (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のみ、このコマンドを入力する必要があります。</p>
ステップ 8 interface interface-id	<p>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。</p>
ステップ 9 ip dhcp snooping vlan vlan information option format-type circuit-id string ASCII-string	<p>(任意) 指定したインターフェイスで回線 ID サブオプションを指定します。</p> <p>1 ~ 4049 の範囲の VLAN ID を使用して VLAN およびポート ID を指定します。</p> <p>3 ~ 63 の ASCII 文字列 (スペースなし) で回線 ID を設定できます。</p> <p>デフォルトの回線 ID はポート ID で、フォーマットは vlan-mod-port です。</p>
ステップ 10 ip dhcp snooping trust	<p>(任意) インターフェイスを信頼される状態または信頼されない状態として設定します。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インターフェイスを設定するには、no キーワードを使用できます。デフォルトは信頼されない状態です。</p>
ステップ 11 ip dhcp snooping limit rate rate	<p>(任意) インターフェイスが 1 秒間に受信できる DHCP パケット数を設定します。指定できる範囲は 1 ~ 4294967294 です。デフォルトでは、レート制限は設定されていません。</p> <p> (注) 100 パケット / 秒以下の信頼されないレート制限を推奨します。信頼されるインターフェイスにレート制限を設定した場合に、DHCP スヌーピングがイネーブルの複数の VLAN にトランク ポートを割り当てると、レート制限の強化が必要となることがあります。</p>
ステップ 12 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>

	コマンド	目的
ステップ 13	<code>ip dhcp snooping verify mac-address</code>	(任意) 信頼され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するように、スイッチを設定します。デフォルトは、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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 15	<code>show running-config</code>	設定を確認します。
ステップ 16	<code>copy running-config startup-config</code>	(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 範囲の 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-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。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 allow-untrusted` グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 で DHCP スヌーピングをグローバルにイネーブルにし、ポート FastEthernet 0/1 でレート制限を 100 パケット / 秒に設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface fastethernet0/1
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 の両方に伝播されます。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 で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	目的
ステップ 1	<code>configure terminal</code>	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	<code>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}</code>	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。 <ul style="list-style-type: none"> <code>flash:/filename</code> <code>ftp://user:password@host/filename</code> <code>http://[[username:password]@]{hostname host-ip}/{/directory} /image-name.tar</code> <code>rcp://user@host/filename</code> <code>tftp://host/filename</code>
ステップ 3	<code>ip dhcp snooping database timeout seconds</code>	停止するまでにデータベースの転送を終了するのに待機する時間を秒数で指定します。 指定できる範囲は 0 ~ 86400 です。0 を設定すると時間は無限になります。デフォルト値は 300 秒 (5 分) です。
ステップ 4	<code>ip dhcp snooping database write-delay seconds</code>	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。デフォルト値は 300 秒 (5 分) です。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</code>	(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。 <code>vlan-id</code> に指定できる範囲は 1 ~ 4904 です。 <code>seconds</code> 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) スイッチをテストまたはデバッグする場合にこのコマンドを使用します。
ステップ 7	<code>show ip dhcp snooping database [detail]</code>	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	<code>copy running-config startup-config</code>	(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対してこのコマンドを入力します。

DHCP 情報の表示

DHCP スヌーピング情報を表示するには、表 19-2 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 19-2 DHCP 情報表示用のコマンド

コマンド	目的
<code>show ip dhcp snooping</code>	スイッチの DHCP スヌーピング設定を表示します。
<code>show ip dhcp snooping binding</code>	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に設定されたバインディングのみを表示します。 ¹
<code>show ip dhcp snooping database</code>	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。
<code>show running-config</code>	すべてのインターフェイスでの DHCP Option 82 フィールドの挿入と削除のステータスを表示します。

1. DHCP スヌーピングがイネーブルの状態、インターフェイスがダウンステートに変わった場合、スイッチは手動設定し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、非ルーテッド レイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能です。IP ソース ガードを使用して、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 パケット以外の、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 ACL 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 バインディングを変更してポート ACL を変更し、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のみ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 パケット以外の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に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 (p.19-21)
- IP ソース ガード設定時の注意事項 (p.19-21)
- IP ソース ガードのイネーブル化 (p.19-22)
- IP ソース ガード情報の表示 (p.19-23)

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

- 非ルーテッドポートでのみスタティック 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属するアクセス VLAN 上でイネーブルにする必要があります。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードをイネーブルにして、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 スヌーピングを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 セキュリティは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、この機能をイネーブルにできます。
- Ternary CAM (TCAM) エントリ数が使用可能な最大数を超えた場合、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>ip verify source</code> または <code>ip verify source port-security</code>	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) <code>ip verify source port-security</code> 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 セキュリティ両方をイネーブルにする場合、次の注意事項があります。 <ul style="list-style-type: none"> • DHCP サーバは Option 82 をサポートする必要があります。サポートしない場合、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。スイッチが非 DHCP データトラフィックを受信した場合にのみ、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	<code>exit</code>	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	<code>ip source binding mac-address vlan vlan-id ip-address interface interface-id</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show ip verify source [interface interface-id]</code>	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	<code>show ip source binding [ip-address] [mac-address] [dhcp-snooping static] [interface interface-id] [vlan vlan-id]</code>	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	<code>copy running-config startup-config</code>	(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 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 フィルタリングのある 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 19-3 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 19-3 IP ソース ガード情報の表示用コマンド

コマンド	目的
<code>show ip source binding</code>	スイッチの IP ソース バインディングを表示します。
<code>show ip verify source</code>	スイッチの IP ソース ガード設定を表示します。

