



## DHCP 機能の設定

この章では、Catalyst 3550 スイッチで DHCP スヌーピングと 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、このリリースに対応する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。

この章の内容は、次のとおりです。

- 「DHCP 機能の概要」(P.18-1)
- 「DHCP 機能の設定」(P.18-8)
- 「DHCP 情報の表示」(P.18-18)

## DHCP 機能の概要

DHCP は、中央のサーバからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって 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 では、ネットワークに接続されたホストだけが IP アドレスを使用し、IP アドレスを永続的にホストに割り当てる必要がなくなるため、限られた IP アドレス空間を節約できます。

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.18-2)
- 「DHCP リレー エージェント」(P.18-2)
- 「DHCP スヌーピング」(P.18-2)
- 「Option 82 データ挿入」(P.18-3)
- 「Cisco IOS DHCP サーバ データベース」(P.18-7)
- 「DHCP スヌーピング バインディング データベース」(P.18-7)

DHCP クライアントに関する詳細については、『*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上の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、それらのアドレスを管理します。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、クライアントとサーバの間で 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、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは DHCP メッセージを受信し、新しい DHCP メッセージを生成して出力インターフェイスで送信します。

## DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース (DHCP スヌーピング バインディング テーブルとも呼ばれる) の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用すると、エンド ユーザに接続された信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続された、信頼できるインターフェイスとを差別化できます。



(注)

DHCP スヌーピングを正しく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経由でスイッチに接続する必要があります。

非信頼メッセージとは、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 ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、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 アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が格納されています。このデータベースには、信頼できるインターフェイスに相互接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信頼できないインターフェイスとなります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、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ドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、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側から着信した。
- パケットが信頼できないインターフェイスに着信し、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が一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング テーブルに含まれているが、バインディング テーブル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。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、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。

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スイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

Cisco IOS Release 12.1(22)EA3 よりも前のソフトウェア リリースまたは Cisco IOS Release 12.2(25)SEA 以降では、エッジスイッチにより Option 82 情報が挿入された場合、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ため、集約スイッチ上で DHCP スヌーピングを設定できません。また、スタティック バインディングや ARP アクセス コントロール リスト (ACL) を使用しない場合、スイッチ上で IP 送信元ガードやダイナミック アドレス解決プロトコル (ARP) インспекションも設定できません。

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認識します。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。集約スイッチ上のエッジスイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

## Option 82 データ挿入

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

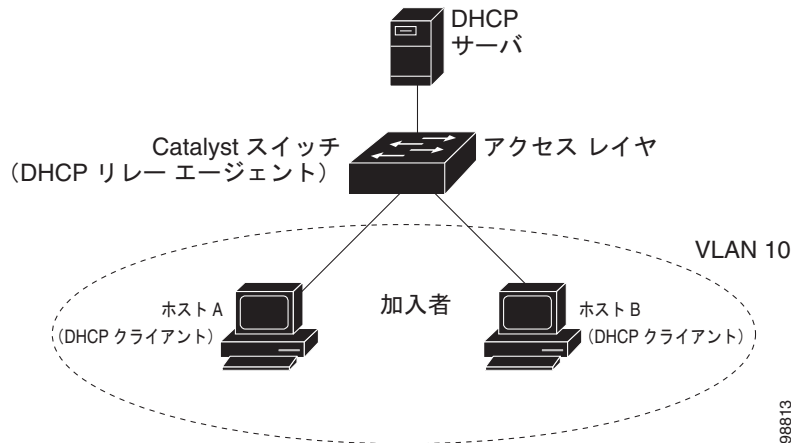


(注)

Cisco IOS Release 12.1(19)EA1 以降では、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 がある場合にサポートされます。スイッチは DHCP がディセーブルの場合にも、DHCP Option 82 機能をサポートします。

図 18-1 に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てる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 クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、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り、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 18-1 メトロポリタンイーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに 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)、およびパケットを受信したポートの識別子である **vlan-mod-port** または **snmp-ifindex** が含まれます (回線 ID サブオプション)。
- 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は、スイッチは DHCP パケット内にこの IP アドレスを追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するポリシーなどです。次に DHCP サーバは、DHCP 応答内にオプション 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。クライアントとサーバが同じサブネット上にある場合は、サーバはこの応答をブロードキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済み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から、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。

上記の一連のイベントが発生する間、図 18-2 に示す次のフィールドの値は変更されません。

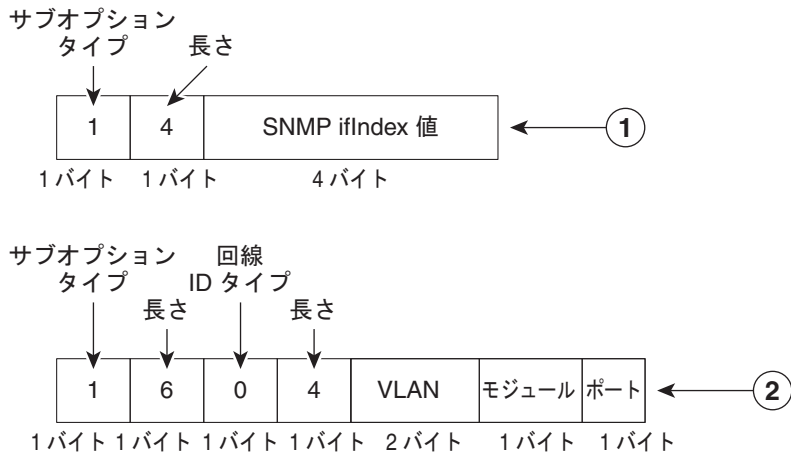
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ

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

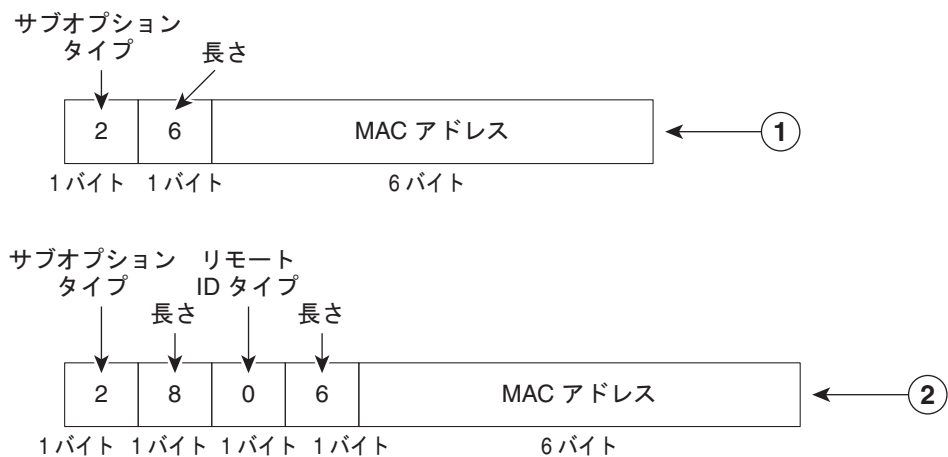
DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力し、SNMP ifIndex 形式を設定しない場合、回線 ID サブオプションのポート フィールドのポート番号は、0 から始まります。たとえば、Catalyst 3550-24 スイッチでは、ポート 0 が Fast Ethernet 0/1 ポート、ポート 1 が Fast Ethernet 0/2 ポート、ポート 2 が Fast Ethernet 0/3 ポートなどようになります。Port 24 はギガビット インターフェイス コンバータ (GBIC) ベースのギガビット モジュール スロット 0/1 に、ポート 25 は 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 18-2 は、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 サブオプションの場合、モジュール フィールドは常にゼロになります。

図 18-2 サブオプションのパケット形式  
回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット



116301

- |   |  |
|---|--|
| 1 | DHCP スヌーピングがグローバルにイネーブルで、 <b>ip dhcp relay information option</b> グローバル コンフィギュレーション コマンドを入力し、 <b>ip dhcp snooping information option format snmp-ifindex</b> 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、スイッチでは、これらの形式が使用されます。 |
| 2 | DHCP スヌーピングがグローバルにイネーブルで、 <b>ip dhcp snooping information option</b> 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 ifIndex 形式を設定しない場合、スイッチでは、これらの形式が使用されます。  |

## 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、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 アドレスを手動で割り当てること、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のが可能です。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 スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ (バインディング) は、IP アドレス、それに関連付けられた MAC アドレス、リース期間 (16 進形式)、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。各エントリの最後にある *checksum* 値は、ファイルの最初からエントリの末尾までのバイト数です。各エントリは、まず 72 バイトのデータがあり、その後 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、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 スヌーピングだけがイネーブルである場合は、スイッチの接続は切断されませんが、DHCP スヌーピングが DHCP スプーフィング攻撃を防止できない場合があります。

データベース エージェントは、設定された場所のファイルにバインディングを保存します。リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。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。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。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。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内 (書き込み遅延および中断タイムアウトの値によって設定される) に更新されない場合、更新は停止します。

次に、バインディングのあるファイルのフォーマットを示します。

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

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

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ているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スwitchがエントリを読み取り、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一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- 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 スヌーピングにおける信頼できるインターフェイスである。

## DHCP 機能の設定

ここでは、スイッチで DHCP スヌーピングと Option 82 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](#)」 (P.18-9)
- 「[DHCP スヌーピング設定時の注意事項](#)」 (P.18-9)
- 「[旧版のソフトウェア リリースからのアップグレード](#)」 (P.18-10)
- 「[DHCP サーバの設定](#)」 (P.18-11)
- 「[DHCP リレー エージェントのみのイネーブル化](#)」 (P.18-11)
- 「[DHCP リレー エージェントと Option 82 のイネーブル化](#)」 (P.18-11)
- 「[リレー エージェント情報 Option 82 の確認](#)」 (P.18-12)



- 「再転送ポリシーの設定」 (P.18-12)
- 「パケット転送アドレスの指定」 (P.18-13)
- 「DHCP スヌープングおよび Option 82 のイネーブル化」 (P.18-14)
- 「プライベート VLAN での DHCP スヌープングのイネーブル化」 (P.18-16)
- 「Cisco IOS DHCP サーバ データベースのイネーブル化」 (P.18-16)
- 「DHCP スヌープング 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.18-17)

## DHCP のデフォルト設定

表 18-1 に、DHCP のデフォルト設定を示します。

表 18-1 DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	IOS ソフトウェアではイネーブル、設定が必要。 <sup>1</sup>
DHCP リレー エージェント	イネーブル <sup>2</sup>
DHCP パケット転送アドレス	未設定
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)。 <sup>2</sup>
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換。 <sup>2</sup>
DHCP スヌープングをグローバルにイネーブル	ディセーブル
DHCP スヌープング情報オプション	イネーブル
信頼できない入カインターフェイスでパケットを受信するための DHCP スヌープング オプション <sup>3</sup>	ディセーブル
DHCP スヌープング レート制限	未設定
DHCP スヌープング信頼状態	信頼できない
DHCP スヌープング VLAN	ディセーブル
DHCP スヌープングの 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	IOS ソフトウェアではイネーブル、設定が必要。 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だけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌープング バインディング データベース エージェント	IOS ソフトウェアではイネーブル、設定が必要。 この機能は宛先が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り 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に限り 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によって Option 82 が挿入された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 スヌープング設定時の注意事項

ここでは、DHCP の設定時の注意事項を説明します。

- DHCP スヌーピングは、スイッチ上で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 で DHCP スヌーピングがイネーブルになるまでアクティブになりません。
- スイッチ上で 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 サーバや 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、イネーブルになっていることを確認してください。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにすると、スヌーピングをディセーブルにするまで Cisco IOS コマンドは使用できません。次のコマンドを入力しても、スイッチからはエラー メッセージが返され、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
- スイッチで 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設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- スイッチで 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設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップ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である場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- 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は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- 信頼できないデバイスが接続されたアグリゲーション 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 Option 82 情報をスプーフィングする可能性があります。

## 旧版のソフトウェア リリースからのアップグレード

Cisco IOS Release 12.1(19)EA1 では、旧リリースから Option 82 サブスクライバ ID の実装が変更されています。新しい Option 82 形式は、異なる回線 ID およびリモート ID サブオプション、**vlan-mod-port** を使用します。以前のバージョンは、**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。

スイッチで Option 82 が設定され、Cisco IOS Release 12.1(19)EA1 以降にアップグレードした場合、Option 82 の設定は影響を受けません。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した場合は、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。スイッチの DHCP スヌーピングをグローバルにディセーブルにすると、以前の Option 82 の設定が再びイネーブルになります。

下位互換性を確保するには、DHCP スヌーピングをイネーブルにする場合に、**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、(選択した形式の) Option 82 情報は、スヌーピングされた VLAN だけに挿入されます。

DHCP スヌーピングをイネーブルにしないで Option 82 の以前のバージョンを使用する手順については、「[DHCP リレー エージェントと Option 82 のイネーブル化](#)」(P.18-11) を参照してください。

## DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。デフォルトでは、Cisco IOS DHCP サーバおよび DHCP リレー エージェント機能はスイッチ上でイネーブルにされていますが、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 エージェントのみのイネーブル化

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	<b>configure terminal</b>	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	<b>service dhcp</b>	スイッチ上で DHCP サーバおよび 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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ4	<b>show running-config</b>	入力内容を確認します。
ステップ5	<b>copy running-config startup-config</b>	(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 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。

## DHCP リレー エージェントと Option 82 のイネーブル化

Cisco IOS Release 12.1(19)EA1 では、旧リリースから Option 82 サブスクリバ ID の実装が変更されています。DHCP スヌーピングを使用する場合のリレー エージェントと Option 82 の設定の詳細については、「[旧版のソフトウェア リリースからのアップグレード](#)」(P.18-10) を参照してください。

スイッチ上で DHCP リレー エージェントと Option 82 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	<b>configure terminal</b>	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	<b>service dhcp</b>	スイッチ上で DHCP サーバおよび 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。

	コマンド	目的
ステップ 3	<b>ip dhcp relay information option</b>	スイッチで、DHCP サーバ宛てに転送される要求メッセージ内の 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になっています。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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 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。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 の確認

デフォルトでは、スイッチは DHCP サーバからの受信する DHCP 応答パケットの option-82 フィールドが有効であることを確認します。無効なメッセージを受信すると、そのメッセージは廃棄されます。有効なメッセージを受信すると、スイッチは Option 82 フィールドを削除し、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。ディセーブルの場合、スイッチは option-82 フィールドの有効性を検証せず、パケットからオプションを削除して転送します。(この機能は、DHCP スヌーピングがスイッチでイネーブルになっている場合は使用できません)。



(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、情報チェック機能がイネーブルな場合、スイッチは、無効であるためにパケットをドロップします。ただし、場合によっては、option-82 フィールドを使用してクライアントを設定することがあります。この状況では、情報チェック機能をディセーブルにして、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する必要があります。ip dhcp relay information policy グローバル コンフィギュレーション コマンドを使用して、既存の Option 82 情報を含むパケットを受信した場合にスイッチが実行する処理を設定できます。詳細については、「再転送ポリシーの設定」(P.18-12)を参照してください。(この機能は、DHCP スヌーピングがスイッチでイネーブルになっている場合は使用できません)。

## 再転送ポリシーの設定

デフォルトでは、スイッチの再転送ポリシーは、DHCP クライアントから受信したパケットの既存のリレー情報を、スイッチの DHCP リレー情報に入れ替えることです。ご使用のネットワークでデフォルトの動作が適切でない場合、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変更できます。(この機能は、DHCP スヌーピングがスイッチでイネーブルになっている場合は使用できません)。



(注)

再転送ポリシーの動作が正しいことを確認するには、no ip dhcp relay information check グローバル コンフィギュレーション コマンドを使用して、リレー エージェント情報チェックがディセーブルであることを確認します。

特権 EXEC モードから、再転送ポリシーのアクションを変更するには、次の手順に従います。

	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 relay information policy {drop   keep   replace}</code>	再転送ポリシーを設定します。デフォルトの動作は、スイッチの DHCP リレー情報で既存の情報を入れ替える（上書きする）ことです。 <ul style="list-style-type: none"> <li>Option 82 情報も存在する場合、既存のリレー情報を含むメッセージを廃棄する場合は、<b>drop</b> キーワードを使用します。</li> <li>既存のリレー情報を保持する場合は、<b>keep</b> キーワードを使用します。</li> </ul>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	入力内容を確認します。
ステップ5	<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。

デフォルトの再転送ポリシーに戻すには、`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、クライアントとサーバが同じ物理サブネット上に存在しない場合に、それらのクライアントとサーバの間で DHCP パケットを転送するデバイスです。リレー エージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、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ます。これとは対照的に、リレー エージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して他のインターフェイスから送信します。

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。一般的なルールは、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 アドレスにすることができます。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。この手順は任意です。

	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 vlan vlan-id</code>	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	<code>ip address ip-address subnet-mask</code>	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	<code>ip helper-address address</code>	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 アドレスにすることができます。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。

	コマンド	目的
ステップ 5	<b>exit</b>	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	<b>interface range port-range</b>  または <b>interface interface-id</b>	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、インターフェイス範囲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	<b>switchport mode access</b>	ポートの VLAN メンバシップ モードを定義します。
ステップ 8	<b>switchport access vlan vlan-id</b>	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 9	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	<b>show running-config</b>	入力内容を確認します。
ステップ 11	<b>copy running-config startup-config</b>	(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。

次の例に、DHCP サーバ、リレー エージェント、および DHCP リレー情報 (Option 82) の挿入と削除をイネーブルにする方法を示します。これは、VLAN ID 10 のスイッチ仮想インターフェイスを作成し、そのインターフェイスに IP アドレスを割り当て、30.0.0.2 (DHCP サーバのアドレス) の DHCP パケット転送アドレスを指定します。DHCP クライアントに接続する 2 個のインターフェイス (Gigabit Ethernet 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ます (図 18-1 (P.18-4) 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	<b>configure terminal</b>	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	<b>ip dhcp snooping</b>	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	目的
ステップ 3	<code>ip dhcp snooping vlan <i>vlan-range</i></code>	1 つの 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 の範囲を入力することができます。これらはスペースで区切ります。
ステップ 4	<code>ip dhcp snooping information option</code>	スイッチで、DHCP サーバ宛てに転送される要求メッセージ内の 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。  デフォルトではイネーブルになっています。
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 オプションに異なる形式を選択するには、 <code>ip dhcp snooping information option format snmp-ifindex</code> を指定します。詳細については、「旧版のソフトウェア リリースからのアップグレード」(P.18-10) 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。
ステップ 6	<code>ip dhcp snooping information option allow-untrusted</code>	(任意) スwitch がエッジ スwitch に接続された集約スウィッチである場合、スウィッチがエッジ スwitch によって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを受け入れるようにします。  デフォルトではディセーブルになっています。  (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ウィッチだけです。
ステップ 7	<code>interface <i>interface-id</i></code>	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	<code>ip dhcp snooping trust</code>	(任意) インターフェイスを <code>trusted</code> または <code>untrusted</code> のいずれかに設定します。 <code>untrusted</code> クライアントからのメッセージをインターフェイスが受信できるようにするには、 <code>no</code> キーワードを使用します。デフォルトは <code>untrusted</code> です。
ステップ 9	<code>ip dhcp snooping limit rate <i>rate</i></code>	(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 ~ 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。  (注) 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。 <code>trusted</code> インターフェイスにレート制限を設定する場合、ポートが DHCP スヌーピングをイネーブルにした複数の VLAN に割り当てられているトランク ポートであれば、レート制限を増やさなければならない可能性があります。
ステップ 10	<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 11	<code>ip dhcp snooping verify mac-address</code>	(任意) 信頼できないポート上で受信した DHCP パケットにある送信元 MAC アドレスが、パケット内のクライアントのハードウェア アドレスと一致するかどうかを確認するように、スイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 13	<b>show running-config</b>	入力内容を確認します。
ステップ 14	<b>copy running-config startup-config</b>	(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。1 つの VLAN または VLAN の範囲で 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-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 スイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットをドロップ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および VLAN 10 でイネーブルにし、ファストイーサネットポート 0/1 のレート制限を 1 秒あたり 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 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

DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。DHCP スヌーピング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	<b>configure terminal</b>	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	<b>ip dhcp snooping database</b> { <b>flash:/filename</b>   <b>ftp://user:password@host/filename</b>   <b>http://[[username:password]@]</b> { <b>hostname</b>   <b>host-ip</b> }[/ <b>directory</b> ]} <b>/image-name.tar</b>   <b>rcp://user@host/filename</b> }	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 ファイルの URL を指定します。 <ul style="list-style-type: none"> <li>• <b>flash:/filename</b></li> <li>• <b>ftp://user:password@host/filename</b></li> <li>• <b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>• <b>rcp://user@host/filename</b></li> <li>• <b>tftp://host/filename</b></li> </ul>
ステップ 3	<b>ip dhcp snooping database timeout</b> <i>seconds</i>	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。0 を設定すると、待ち時間が無限になります。デフォルトは 300 秒 (5 分) です。
ステップ 4	<b>ip dhcp snooping database write-delay</b> <i>seconds</i>	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ~ 86400 秒です。デフォルトは 300 秒 (5 分) です。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>ip dhcp snooping binding mac-address</b> <b>vlan vlan-id ip-address interface</b> <i>interface-id expiry seconds</i>	(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。 <i>vlan-id</i> の範囲は 1 ~ 4904 です。 <i>seconds</i> の範囲は 1 ~ 4294967295 です。  このコマンドは、追加するエントリごとに入力します。  (注) このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 7	<b>show ip dhcp snooping database</b> [ <b>detail</b> ]	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	<b>copy running-config startup-config</b>	(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** 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。タイムアウトまたは遅延時間の値を再セットするには、**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** 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** 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 情報の表示

DHCP スヌーピング情報を表示するには、表 18-2 の特権 EXEC コマンドを 1 つ以上使用します。

表 18-2 DHCP 情報を表示するためのコマンド

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 データベース内の動的に設定されたバインディングのみを表示します。 <sup>1</sup>
<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の DHCP option-82 フィールドの挿入および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。

## 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、ホストがネイバーの IP アドレスを使用しようとしたときに発生するトラフィック攻撃を回避できます。

IP ソース ガードは、信頼できないインターフェイス上で DHCP スヌーピングがイネーブルにされている場合に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 アクセス コントロール リスト (ACL) は、この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 テーブルに送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他のトラフィックはすべて拒否します。

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にされている場合だけ、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。

## 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。スイッチは、送信元 IP 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に、IP トラフィックを転送します。

DHCP スヌーピング バインディングまたはスタティック IP 送信元バインディングがインターフェイスで追加、変更、削除された場合、スイッチは IP 送信元バインディングの変更に基づいてポート ACL を修正し、修正したポート ACL をインターフェイスに再適用します。

(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) 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と、スイッチはインターフェイス上のすべての IP トラフィックを拒否するポート ACL を作成して適用します。IP ソース ガードをディセーブルにした場合、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

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 アドレスと 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だけ、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 パケット、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、スイッチはこのパケットを転送します。DHCP パケットを除き、その他の種類のパケットはすべて、スイッチによりドロップされます。

スイッチは、送信元 MAC アドレスのフィルタリングにポートセキュリティを使用します。ポートセキュリティ違反が発生した場合、インターフェイスはシャットダウンします。

## IP ソース ガードの設定

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

- 「デフォルトの IP ソース ガード設定」(P.18-19)
- 「IP ソース ガード設定時の注意事項」(P.18-19)
- 「IP ソース ガードのイネーブル化」(P.18-20)
- 「IP ソース ガード情報の表示」(P.18-21)

## デフォルトの IP ソース ガード設定

IP ソース ガードは、デフォルトで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 ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding mac-address vlan vlan-id ip-address interface interface-id** グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。  

```
Static IP source binding can only be configured on switch port.
```
- IP ソース ガードと送信元 IP フィルタリングが 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 でイネーブルでなければなりません。

## IP ソース ガードの設定

- 複数の VLAN を持つトランク 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、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。



(注) IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- 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、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に IP ソース ガードを設定した場合、ポート セキュリティはサポートされません。
- EtherChannels では、IP ソース ガード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、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越えた場合、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	<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>	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	<code>ip verify source</code> または <code>ip verify source port-security</code>	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。  送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。  (注) <code>ip verify source port-security</code> 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場合は、次の 2 つの注意事項があります。 <ul style="list-style-type: none"> <li>DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てるできません。</li> <li>DHCP パケットの MAC アドレスが、セキュアアドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュアアドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。</li> </ul>
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。 スタティック バインディングごとにこのコマンドを入力します。

	コマンド	目的
ステップ6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ7	<b>show ip verify source</b> [ <b>interface interface-id</b> ]	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	<b>show ip source binding</b> [ <i>ip-address</i> ] [ <i>mac-address</i> ] [ <b>dhcp-snooping</b>   <b>static</b> ] [ <b>interface interface-id</b> ] [ <b>vlan vlan-id</b> ]	スイッチ、特定の VLAN、または特定のインターフェイス上に IP ソース バインディングを表示します。
ステップ9	<b>copy running-config startup-config</b>	(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 フィルタリングによる IP ソース ガードをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP 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、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 18-3 の特権 EXEC コマンドを 1 つ以上使用します。

表 18-3 IP ソース ガード情報を表示するためのコマンド

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

