CHAPTER 38

DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Dynamic Host Configuration Protocol（DHCP）スヌーピングと IP ソース ガード、およびスタティック ホストの IPSG を設定する手順について説明します。設定上の注意事項、設定手順、および設定例も示します。

この章の主な内容は、次のとおりです。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

Catalyst 4500 のコマンド リファレンスに掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

DHCP スヌーピングについて

DHCP スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング テーブルを構築およびメンテナンスすることで安全性を持たせる DHCP セキュリティ機能です。信頼でき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外部からの受信メッセージのうち、ネットワーク内でトラフィック攻撃を引き起こす可能性のあるメッセージです。

DHCP スヌーピング バインディング テーブルには、MAC 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 番号、およびスイッチの信頼できないローカル インターフェイスに対応するインターフェイス情報が格納されます。信頼できるインターフェイスに相互接続するホストに関する

情報は収められていません。信頼できないインターフェイスとは、ネットワークまたはファイアウォール外部からのメッセージを受信するように設定されたインターフェイスです。信頼できるインターフェイスとは、ネットワーク内からのメッセージのみを受信するように設定されたインターフェイスです。

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のように機能します。また、DHCP スヌーピングは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 サーバまたは別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差異化する方法を提供します。

（注）　VLAN 上で DHCP スヌーピングをイネーブルにするには、スイッチ上で DHCP スヌーピングをイネーブルにする必要があります。

DHCP スヌーピングはスイッチと VLAN に対して設定できます。スイッチ上で DHCP スヌーピングをイネーブルにする場合、インターフェイスはレイヤ 2 ブリッジとして動作し、レイヤ 2 VLAN に送信される DHCP メッセージを代行受信および保護します。VLAN 上で DHCP スヌーピングをイネーブルにする場合、スイッチは VLAN ドメイン内のレイヤ 2 ブリッジとして動作します。

次の内容について説明します。

信頼送信元と信頼できない送信元

DHCP スヌーピング機能は、トラフィックの送信元が信頼できるかまたは信頼できないかを判別します。信頼できない送信元は、トラフィック攻撃または他の敵対的アクションを起こすことがあります。これらの攻撃を回避するために、DHCP スヌーピング機能は、信頼できない送信元からのメッセージおよびレート制限トラフィックをフィルタします。

エンタープライズ ネットワークでは、管理制御下のデバイスは信頼できる送信元です。これらのデバイスには、使用ネットワークのスイッチ、ルータ、およびサーバが含まれます。ファイアウォール外またはネットワーク外のデバイスは、信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダー環境では、サービス プロバイダー ネットワーク内にないデバイス（顧客のスイッチなど）は、信頼できない送信元です。ホスト ポートは、信頼できない送信元です。

Catalyst 4500 シリーズ スイッチでは、接続しているインターフェイスの信頼状態を設定して、送信元が信頼できることを示します。

すべてのインターフェイスのデフォルトは、信頼できない状態です。DHCP サーバ インターフェイスは、信頼できる送信元として設定する必要があります。また、ネットワーク内のデバイス（スイッチまたはルータなど）に接続している場合、他のインターフェイスも信頼できる送信元として設定できます。通常は、ホスト ポート インターフェイスは信頼できる送信元としては設定しません。

（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。これは、信頼できない DHCP メッセージが、信頼できるインターフェイスにしか転送されないためです。

DHCP スヌーピング データベース エージェントの概要

スイッチのリロード時にバインディングが失われないようにするには、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。このエージェントがないと、DHCP スヌーピングによって確立されたバインディングがスイッチのリロード時に失われます。接続も同様に失われます。

データベース エージェントのメカニズムでは、設定されたロケーションのファイルにバインディングを格納します。リロード時に、スイッチはファイルを読み取り、バインディングのデータベースを作成します。スイッチは、データベースが変更されるとファイルを書き込み、ファイルを最新の状態に保ちます。

バインディングを含むファイルの形式は、次のようになります。

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

ファイルの各エントリは、ファイルが読み取られるたびにエントリの確認に使用されるチェックサムでタグ付けされています。最初の行の <initial-checksum> エントリは、以前の書き込みに関連付けられたエントリと最新の書き込みに関連付けられたエントリを区別するのに役立ちます。

次に、バインディング ファイルの例を示します。

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1                                   e5e1e733
1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1                                   4b3486ec
1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1                                  f0e02872
1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1                                  ac41adf9
1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1                                     34b3273e
END
```

各エントリには、IP アドレス、VLAN、MAC アドレス、リース期間（16 進法）、およびバインディングに関連付けられたインターフェイスが含まれます。各エントリの最後には、ファイルの開始からエントリに関連付けられたすべてのバイトの合計を計上するチェックサムがあります。各エントリは、72 バイトのデータで構成され、スペースおよびチェックサムがあとに続きます。

起動時に、算出されたチェックサムが格納されたチェックサムに合致すると、スイッチはファイルからエントリを読み取り、バインディングを DHCP スヌーピング データベースに追加します。算出されたチェックサムが格納されたチェックサムに合致しない場合、ファイルから読み取られたエントリが無視され、失敗したエントリに続くすべてのエントリも無視されます。また、スイッチは、リース時間が期限切れになったファイルのすべてのエントリを無視します（この状況があり得るのは、リース時間が期限切れを示している場合があるためです）。また、エントリ内で参照されているインターフェイスが、すでにシステム内に存在しない場合、または、ルータ ポートや DHCP スヌーピング信頼インターフェイスの場合も、ファイルからのエントリが無視されます。

スイッチが新しいバインディングを学習した場合、または一部のバインディングを失った場合、スイッチはスヌーピング データベースから修正した一連のエントリをファイルに書き込みます。書き込みでは、実際の書き込みが行われるまで、バッチに対して設定可能な遅延時間内で、可能な限り多くの変更を行うことができます。各転送に関連付けられるのは、完了しない場合に、その後転送が中断されるタイムアウトです。これらのタイマーは、書き込み遅延および中断タイムアウトと呼ばれます。

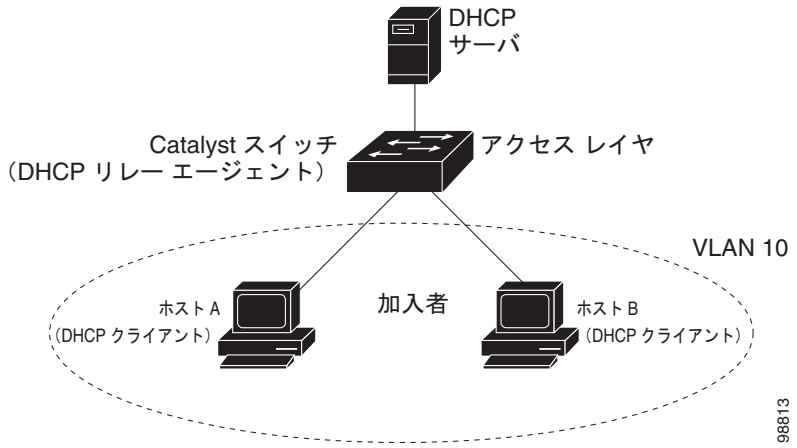
オプション 82 データ挿入

居住、メトロポリタン イーサネット アクセス環境では、DHCP が多数のサブスクライバの IP アドレス割り当てを集中的に管理できます。DHCP オプション 82 機能がスイッチでイネーブルのとき、サブスクライバ デバイスは、（MAC アドレスのほかに）ネットワークへの接続に使用しているスイッチ ポートによって識別されます。サブスクライバ LAN の複数ホストは、アクセス スイッチにある同じポートに接続でき、一意に識別されます。

（注）　DHCP オプション 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サブスクライバ デバイスが割り当てられている VLAN 上にある場合にのみサポートされます。

図 38-1 に、アクセス レイヤでスイッチに接続しているサブスクライバに IP アドレスを集中 DHCP サーバが割り当てる、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 クライアントとその関連 DHCP サーバが同じ IP ネットワークまたはサブネット上にないため、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で DHCP メッセージを転送するようにヘルパー アドレスで設定されています。

図 38-1　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



スイッチでの DHCP スヌーピング情報オプション 82 をイネーブルにすると、次のイベントが順に発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、ネットワーク上で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、オプション 82 情報をパケットに追加します。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスで、回線 ID サブオプションは、パケットが受信されるポートの識別子 **vlan-mod-port** です。Cisco IOS Release 12.2(40)SG 以降では、リモート ID および回線 ID を設定できます。これらのサブオプションの設定手順については、「DHCP スヌーピングとオプション 82 のイネーブル化」（P.38-11）を参照してください。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

- DHCP サーバがパケットを受信します。サーバがオプション 82 対応である場合、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、単一リモート ID または回線 ID に割り当て可能な多数の IP アドレスを制限するようなポリシーを実装できます。また、DHCP サーバは、DHCP 応答に含まれるオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID および場合によっては回線 ID フィールドを検査して、元からオプション 82 データが挿入されたのかどうかを確認します。スイッチはオプション 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続しているスイッチ ポートにパケットを転送します。

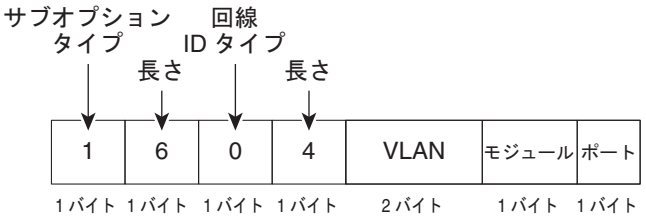
デフォルトのサブオプション設定では、説明したイベントが順に発生すると、図 38-2 にあるフィールドの値は変更されません。

- 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

図 38-2 に、デフォルトのサブオプション設定が使用されたときの、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションの場合、モジュール番号はスイッチ モジュール番号に対応します。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** グローバル コンフィギュレーション コマンドを開始すると、スイッチはパケット形式を使用します。

図 38-2　サブオプション パケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

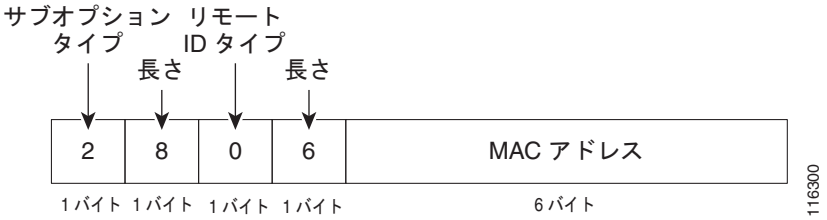


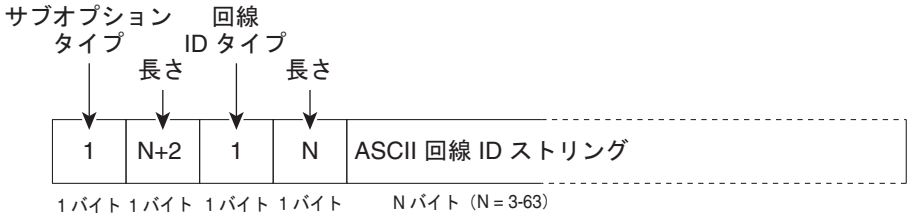
図 38-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット形式を示します。DHCP スヌーピングがグローバルにイネーブルで、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド**および ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが開始されると、スイッチはこれらのパケット形式を使用します。

パケット内のこれらのフィールドの値は、リモート ID および回線 ID サブオプションを設定すると、デフォルト値から変更されます。

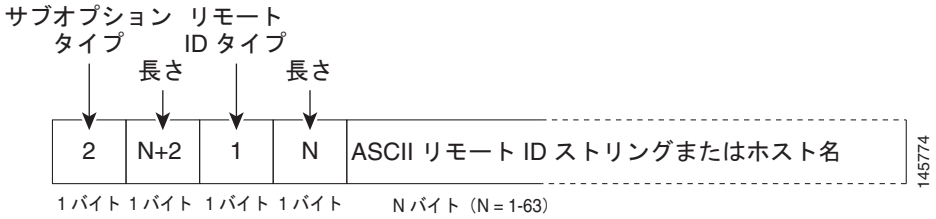
- 回線 ID サブオプション フィールド
  - 回線 ID タイプは 1 です。
  - 長さの値は変数で、設定した文字列の長さによって変わります。
- リモート ID サブオプション フィールド
  - リモート ID タイプは 1 です。
  - 長さの値は変数で、設定した文字列の長さによって変わります。

図 38-3　ユーザ設定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（ユーザ設定のストリング）



リモート ID サブオプション フレーム フォーマット（ユーザ設定のストリング）



DHCP スヌーピングの設定

スイッチ上で DHCP スヌーピングを設定する場合、信頼できるインターフェイスと信頼できないインターフェイスを区別できるようにスイッチを設定します。VLAN 上で DHCP スヌーピングを使用する前に、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。他の DHCP 機能から切り離して DHCP スヌーピングをイネーブルにできます。

ここでは、DHCP スヌーピングを設定する手順について説明します。

（注）　DHCP サーバの設定については、次の URL の『*Cisco IOS IP and IP Routing Configuration Guide*』の「Configuring DHCP」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html

DHCP スヌーピングのデフォルト設定

DHCP スヌーピングは、デフォルトでディセーブルに設定されています。表 38-1 に DHCP スヌーピングの各オプションのデフォルト設定値を示します。

表 38-1　DHCP スヌーピングのデフォルト設定値

オプション	デフォルト値/ステート
dhcp snooping	ディセーブル
dhcp snooping information option	イネーブル
dhcp snooping information option allow-untrusted	ディセーブル
dhcp snooping limit rate	infinite（レート制限のディセーブルと同じように機能）
dhcp snooping trust	untrusted（信頼性がない）
dhcp snooping vlan	ディセーブル

デフォルト設定値を変更する場合は、「DHCP スヌーピングのイネーブル化」を参照してください。

DHCP スヌーピングのイネーブル化

（注） DHCP スヌーピングがグローバルにイネーブルに設定されている場合、ポートが設定されるまで DHCP 要求がドロップされます。そのため、作成時ではなく、メンテナンス ウィンドウの間に、この機能を設定する必要がある場合があります。

DHCP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# 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。 DHCP スヌーピングをディセーブルにするには、**no** キーワードを使用します。
ステップ 2	`Switch(config)# ip dhcp snooping vlan` *number* `[`*number*`] | vlan {`*vlan range*`}]`	VLAN または VLAN 範囲上の DHCP スヌーピングをイネーブルにします。
ステップ 3	`Switch(config)# errdisable recovery {cause dhcp-rate-limit | interval` *interval*`}`	（任意）指定したエラー ディセーブル理由から回復するために必要な時間を設定します。
ステップ 4	`Switch(config)# errdisable detect cause dhcp-rate-limit {action shutdown vlan}`	（任意）VLAN 単位でエラー ディセーブル検出をイネーブルにします。 **（注）** このコマンドは、デフォルトでイネーブルに設定されており、違反が発生するとインターフェイスがシャットダウンされます。

	コマンド	目的
ステップ 5	`Switch(config-if)# ip dhcp snooping trust`	インターフェイスの信頼性を trusted または untrusted に設定します。 untrusted 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、**no** キーワードを使用します。
ステップ 6	`Switch(config-if)# ip dhcp snooping limit rate` *rate*	インターフェイスが受信できる 1 秒あたりの DHCP パケット数（pps）を設定します。[1]
ステップ 7	`Switch(config)# end`	コンフィギュレーション モードを終了します。
ステップ 8	`Switch# show ip dhcp snooping`	設定を確認します。

1. 信頼できないインターフェイスのレート制限を 101 pps 以上に設定しないことを推奨します。信頼できない各クライアントの推奨レート制限は、15 pps です。通常、レート制限は信頼できないインターフェイスに適用されます。信頼できるインターフェイスのレート制限を設定する場合は、スイッチ上のすべての DHCP トラフィックが信頼できるインターフェイスによって集約されることを考慮して、レート制限をより高い値に調整する必要があります。ネットワーク構成に応じてこのしきい値を調整する必要があります。CPU が、DHCP パケットを平均速度 1001 pps 以上で受信しないようにしてください。

DHCP スヌーピングは、単一の VLAN または複数の VLAN に設定できます。単一の VLAN を設定するには、VLAN 番号を 1 つ入力します。VLAN の範囲を設定するには、最初と最後の VLAN 番号、またはダッシュと VLAN 範囲を入力します。

DoS 攻撃を防ぐために、着信 DHCP パケット数がレート制限されます。着信 DHCP パケットのレートが設定された制限を超える場合は、ポートが errdisable ステートに置かれます。ポートのシャットダウンを防ぐには、違反の発生時に、**errdisable detect cause dhcp-rate-limit action shutdown vlan** 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、ポート上で問題になっている VLAN のみをシャットダウンします。

errdisable recovery cause dhcp-rate-limit グローバル コンフィギュレーション コマンドを設定すると、セキュア ポートが errdisable ステートの場合に実行してこのステートを自動的に解除できます。また、**shutdown** および **no shutdown** のインターフェイス コンフィギュレーション コマンドを入力すると、手動で再びイネーブルにできます。ポートが VLAN 単位で errdisable モードの場合、**clear errdisable interface** ***name*** **vlan** ***range*** コマンドを使用すると、ポート上の VLAN を再度イネーブルにすることもできます。

次に、VLAN 500 ～ 555 の DHCP スヌーピング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)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
500,555
DHCP snooping is operational on following VLANs:
500,555
DHCP snooping is configured on the following L3 Interfaces:
```

```
Insertion of option 82 is enabled
    circuit-id default format: vlan-mod-port
    remote-id: switch123 (string)
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled DHCP
snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
 ------------------------     -------     -----------------
FastEthernet5/1              yes         100
  Custom circuit-ids:
    VLAN 555: customer-555
FastEthernet2/1              no          unlimited
  Custom circuit-ids:
    VLAN 500: customer-500

Switch#
```

次の設定では、ルーティングが別の Catalyst スイッチ（たとえば、Catalyst 6500 シリーズ スイッチ）で定義された場合の DHCP スヌーピング設定手順について説明しています。

```
// Trust the uplink gigabit Ethernet trunk port

interface range GigabitEthernet 1/1 - 2
switchport mode trunk
switchport trunk encapsulation dot1q
ip dhcp snooping trust

!

interface VLAN 14
ip address 10.33.234.1 255.255.254.0
ip helper-address 10.5.1.2
```

（注） アップリンク ギガビット インターフェイスでトランキングがイネーブルであり、Catalyst 6500 シリーズ スイッチに上記ルーティング設定が定義されている場合は、Option 82 を追加する（Catalyst 4500 シリーズ スイッチ上の）ダウンストリーム DHCP スヌーピングとの「信頼」関係を設定する必要があります。Catalyst 6500 シリーズ スイッチでこの作業を実行するには、**ip dhcp relay information trusted** VLAN コンフィギュレーション コマンドを使用します。

集約スイッチ上での DHCP スヌーピングの設定

集約スイッチ上で DHCP スヌーピングをイネーブルにするには、信頼できないスヌーピング ポートとしてダウンストリーム スイッチに接続するインターフェイスを設定します。ダウンストリーム スイッチ（または集約スイッチと DHCP クライアント間のパスにある DSLAM などのデバイス）が、DHCP パケットに DHCP Option 82 情報を追加すると、信頼できないスヌーピング ポート上に着信した DHCP パケットはドロップされます。**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドが設定された集約スイッチは、任意の信頼できないスヌーピング ポートからの Option 82 情報を持つ DHCP 要求を受け入れることができます。

DHCP スヌーピングとオプション 82 のイネーブル化

スイッチで DHCP スヌーピングとオプション 82 をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	`Switch(config)# ip dhcp snooping vlan` *vlan-range*	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ～ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力できます。これらはスペースで区切ります。
ステップ 4	`Switch(config)# ip dhcp snooping information option`	スイッチが、転送された DHCP 要求メッセージにある DHCP リレー情報（オプション 82 フィールド）を DHCP サーバに挿入したり削除したりできるようにイネーブルにします。これは、デフォルト設定です。
ステップ 5	`Switch(config)# ip dhcp snooping information option format remote-id [string` *ASCII-string* `| hostname]`	（任意）リモート ID サブオプションを設定します。 次になるようにリモート ID を設定できます。 • 63 文字までの ASCII 文字（スペースなし）の文字列 • スイッチの設定済みホスト名 a. ホスト名が 63 文字以上の場合、リモート ID 設定では 63 文字に切り捨てられます。 デフォルトのリモート ID は、スイッチの MAC アドレスです。
ステップ 6	`Switch(config)# 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た集約スイッチである場合、エッジ スイッチからのオプション 82 情報付き着信 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。 デフォルト設定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ている集約スイッチにのみ入力します。
ステップ 7	`Switch(config)# interface` *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	`Switch(config-if)# ip dhcp snooping vlan` *vlan* `information option format-type circuit-id string` *ASCII-string*	（任意）指定したインターフェイスの回線 ID サブオプションを設定します。 1 ～ 4094 の範囲内の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、形式は **vlan-mod-port** です。 回線 ID が 3 ～ 63 文字の ASCII 文字（スペースなし）の文字列になるように設定できます。
ステップ 9	`Switch(config-if)# ip dhcp snooping trust`	（任意）インターフェイスの信頼性を trusted または untrusted に設定します。untrusted 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、**no** キーワードを使用します。デフォルト設定は信頼できない状態です。

	コマンド	目的
ステップ 10	`Switch(config-if)# ip dhcp snooping limit rate rate`	（任意）インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ～ 2048 です。デフォルトでは、レート制限は設定されていません。 （注）　信頼できないレート制限は、最高で毎秒 100 パケットを推奨します。信頼できるインターフェイスの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になっている複数の VLAN に割り当てられたトランク ポートであると、レート制限を増やす必要があります。
ステップ 11	`Switch(config-if)# 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 12	`Switch(config)# ip dhcp snooping verify mac-address`	（任意）信頼できないポートで受信される 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 ハードウェア アドレスに一致するかどうかを、スイッチが確認するように設定します。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 アドレスに一致することを確認します。
ステップ 13	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 14	`Switch# show running-config`	入力を確認します。
ステップ 15	`Switch# 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。オプション 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。集約スイッチがエッジ スイッチからのオプション 82 情報付き着信 DHCP スヌーピング パケットをドロップするように設定するには、**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および VLAN 10 でイネーブルにし、ポートで毎秒 100 パケットのレート制限を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
```

PVLAN 上での DHCP スヌーピングのイネーブル化

DHCP スヌーピングを Private VLAN（PVLAN）でイネーブルにして、同一 VLAN 内のレイヤ 2 ポートを 分離できます。DHCP スヌーピングがイネーブル（ディセーブル）の場合、設定はプライマリ VLAN および関連付けられたセカンダリ VLAN の両方に伝播します。この設定変更をセカンダリ VLAN に反映させずに、プライマリ VLAN の DHCP スヌーピングをイネーブル（ディセーブル）にすることはできません。

セカンダリ VLAN で DHCP スヌーピングを設定することは可能ですが、関連付けられたプライマリ VLAN で DHCP スヌーピングを設定しないと有効になりません。関連付けられた プライマリ VLAN が設定されている場合、対応するプライマリ VLAN によってセカンダリ VLAN の DHCP スヌーピング モードが有効になります セカンダリ VLAN で DHCP スヌーピングを手動で設定すると、スイッチで次の警告メッセージが発行されます。

```
DHCP Snooping configuration may not take effect on secondary vlan XXX
```

show ip dhcp snooping コマンドは、DHCP スヌーピングが イネーブルのすべての VLAN（プライマリおよびセカンダリの両方）を表示します。

PVLAN 上での DHCP スヌーピングのイネーブル化

DHCP スヌーピング、IPSG、および DAI は、補助または音声の VLAN を含む個々の VLAN 上でイネーブルおよびディセーブルにできるレイヤ 2 ベースのセキュリティ機能です。これは、Cisco IP 電話機能を適切に動作させるためには、音声 VLAN で DHCP スヌーピングをイネーブルにする必要があることを意味します。

イーサネット チャネル グループでの DHCP スヌーピングの設定

DHCP スヌーピングを設定する場合、物理インターフェイス設定に対して **ip dhcp snooping trust** を追加することによって、信頼できるインターフェイスとして DHCP パケットを送信するトランク インターフェイスを設定する必要があります。.ただし、イーサネット チャネル グループ上で DHCP パケットを送信する場合は、次のように、論理ポートチャネル インターフェイス上で **ip dhcp snooping trust** を設定する必要があります。

```
Switch# show run int port-channel50
Building configuration...

Current configuration : 150 bytes
!
interface Port-channel50
 switchport
 switchport trunk native vlan 4092
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
end

Switch#
```

DHCP スヌーピング データベース エージェントのイネーブル化

データベース エージェントを設定するには、次の作業を 1 つまたは複数行います。

コマンド	目的
Switch(config)# **ip dhcp snooping database { *url* | write-delay *seconds* | timeout *seconds* }** Switch(config)# **no ip dhcp snooping database [write-delay | timeout]**	（必須）データベース エージェント（またはファイル）の URL および関連付けられたタイムアウト値を設定します。
Switch# **show ip dhcp snooping database [detail]**	（任意）データベース エージェントの現在の動作ステートおよび転送に関連付けられた統計情報を表示します。
Switch# **clear ip dhcp snooping database statistics**	（任意）データベース エージェントに関連付けられた統計情報をクリアします。
Switch# **renew ip dhcp snooping database [validation none] [*url*]**	（任意）所定の URL のファイルからの読み取りエントリを要求します。
Switch# **ip dhcp snooping binding *mac-addr* vlan *vlan ipaddr* interface *ifname* expiry *lease-in-seconds*** Switch# **no ip dhcp snooping binding *mac-addr* vlan *vlan ipaddr* interface *ifname***	（任意）スヌーピング データベースのバインディングを追加または削除します。

（注）　NVRAM（不揮発性 RAM）およびブートフラッシュの保存容量は限られているので、TFTP またはネットワークベースのファイルを使用してください。フラッシュにデータベース ファイルを保存する場合は、エージェントによって新しく更新されると新しいファイルが作成されます（フラッシュがすぐにいっぱいになります）。さらに、フラッシュで使用するファイルシステムの性質上、ファイル数が多いとアクセスが遅くなります。TFTP からアクセス可能なリモート ロケーションにファイルが格納されている場合、RPR/SSO スタンバイ スーパーバイザ エンジンはスイッチオーバーが発生したときにバインディング リストを引き継ぐことができます。

（注）　ネットワークベースの URL（TFTP および FTP（ファイル転送プロトコル）など）では、スイッチが最初に一連のバインディングを書き込む前に、設定された URL に空のファイルを作成することが必要です。

着信 DHCP パケットのレート制限

スイッチの CPU によって DHCP 違反チェックが実行されます。したがって、DoS 攻撃を防ぐために着信 DHCP パケット数がレート制限されています。

着信 DHCP パケットのレートが設定された制限を超える場合は、ポートが errdisable ステートに置かれます。ユーザが介入するか、または errdisable 回復をイネーブルにして、指定されたタイムアウト時間の経過後自動的にこのステートから回復するまで、ポートはこの状態のままです。

（注）　インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip dhcp snooping limit rate** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスがデフォルトのレート制限に戻ります。

ポートのシャットダウンを防ぐには、違反の発生時に、**errdisable detect cause dhcp-rate-limit action shutdown vlan** 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、ポート上で問題になっている VLAN のみをシャットダウンします。

着信 DHCP パケットのレートを制限するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# errdisable detect cause dhcp-rate-limit [action shutdown vlan]`	VLAN 単位でエラー ディセーブル検出をイネーブルにします。
ステップ 3	`Switch(config)# interface interface-id`	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	`Switch(config-if)# [no] ip dhcp snooping limit rate`	インターフェイス上の着信 DHCP 要求および DHCP 応答のレートを制限します。 デフォルト レートはディセーブルです。
ステップ 5	`Switch(config-if)# 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	`Switch(config)# errdisable recovery {cause dhcp-rate-limit | interval interval}`	（任意）DHCP の errdisable ステートからのエラー回復をイネーブルにします。 デフォルトでは、回復はディセーブルで、回復間隔は 300 秒です。 **interval** *interval* には、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 7	`Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show interfaces status`	設定を確認します。
ステップ 9	`Switch# show errdisable recovery`	設定を確認します。
ステップ 10	`Switch# 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。

デフォルトのレート制限設定に戻すには、**no ip dhcp-rate-limit** 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 検査のエラー回復をディセーブルにするには、**no errdisable recovery cause dhcp-rate-limit** 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、着信パケット数の上限（100 pps）を設定し、バースト間隔（1 秒）を指定する例を示します。

```
SwitchB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)# interface g3/31
SwitchB(config-if)# ip dhcp-rate-limit rate 100 burst interval 1
SwitchB(config-if)# exit
SwitchB(config)# errdisable recovery cause dhcp-rate-limit
SwitchB(config)# exit
SwitchB# show interfaces status

Port    Name               Status     Vlan       Duplex Speed Type
```

```
Te1/1                     connected  1          full   10G   10GBase-LR
Te1/2                     connected  vl-err-dis full   10G   10GBase-LR
SwitchB# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

SwitchB#
1w2d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 101 packets received in 739 milliseconds on Gi3/31.
1w2d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/31, putting Gi3/31 in
err-disable state
SwitchB# show clock
*02:21:43.556 UTC Fri Feb 4 2005
SwitchB#
SwitchB# show interface g3/31 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi3/31                       err-disabled 100          auto   auto 10/100/1000-TX
SwitchB#
SwitchB#
1w2d: %PM-4-ERR_RECOVER: Attempting to recover from arp-inspection err-disable state on
Gi3/31
SwitchB# show interface g3/31 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi3/31                       connected    100        a-full  a-100 10/100/1000-TX
SwitchB# show clock
*02:27:40.336 UTC Fri Feb 4 2005
SwitchB#
```

データベース エージェントの設定例

次に、前述のコマンドを使用する例を示します。

例 1：データベース エージェントのイネーブル化

次に、DHCP スヌーピング データベース エージェントを設定して、所定のロケーションにバインディングを格納し、設定および動作ステートを表示する例を示します。

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
```

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0

Switch#
```

出力の最初の 3 行は、設定された URL および関連付けられたタイマー設定値を表示します。次の 3 行は、動作ステートおよび書き込み遅延時間および中断タイマーの残りの時間を表示します。

出力に表示される統計情報のうち、Startup Failures は起動時のファイル読み込みまたは作成に失敗した試行回数を示します。

（注） ロケーションはネットワークに基づいているため、TFTP サーバに一時ファイルを作成する必要があります。TFTP サーバ デーモンが参照できるようにディレクトリ「directory」に 0 バイトのファイル「file」を作成して、標準的な UNIX ワークステーション上に一時ファイルを作成できます。UNIX ワークステーションのサーバ実装の一部では、ファイルへの書き込みに対して完全な（777）許可がファイルに必要です。

DHCP スヌーピング バインディングは、MAC アドレスおよび VLAN の組み合わせに適合しています。したがって、スイッチがすでにバインディングを所有する、所定の MAC アドレスと VLAN の組み合わせのエントリがリモート ファイルにある場合、ファイルが読み取られるときにリモート ファイルからのエントリは無視されます。この状態をバインディング コリジョンといいます。

エントリに指定されたリースが読み取られた時間によって期限切れになった可能性があるので、ファイルのエントリが無効になる可能性があります。Expired leases カウンタは、この状態によって無視されたバインディング数を示します。Invalid interfaces カウンタは読み取りの際に、エントリで指定されたインターフェイスがシステムに存在しない場合、またはインターフェイスが存在する場合は、それがルータ、または DHCP スヌーピングで信頼されたインターフェイスのどちらかであるために無視されたバインディング数を示します。Unsupported vlans は、指定された VLAN がシステムによってサポートされないために無視されたエントリ数を示します。Parse failures カウンタは、スイッチがファイルのエントリの意味を解釈できなかった場合に無視されたエントリ数を示します。

スイッチは、このような無視されたバインディングに対して 2 組のカウンタを維持します。1 つは、このような状態の少なくとも 1 つによって無視されたバインディングを、少なくとも 1 つ持つ読み取りのカウンタを提供します。このようなカウンタは「Last ignored bindings counters」として表示されます。Total ignored bindings counters は、スイッチが起動されて以降のすべての読み取りで無視されたバインディングの総数を表します。この 2 組のカウンタは、**clear** コマンドによってクリアされます。したがって、総数カウンタは、最後にクリアが行われてから無視されたバインディング数を示す場合があります。

例 2：TFTP ファイルからのバインディング エントリの読み取り

手動で TFTP ファイルのエントリを読み取るには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# **show ip dhcp snooping database**	DHCP スヌーピング データベース エージェントの統計情報を表示します。
ステップ 2	Switch# **renew ip dhcp snoop data** *url*	所定の URL からファイルを読み取るようにスイッチに指示します。
ステップ 3	Switch# **show ip dhcp snoop data**	読み取りステータスを表示します。
ステップ 4	Switch# **show ip dhcp snoop bind**	バインディングが正常に読み取られたことを確認します。

次に、手動で tftp://10.1.1.1/directory/file からエントリを読み取る例を示します。

```
Switch# showb ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Switch#
Switch# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.

Switch#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Switch#
Switch# show ip dhcp snoop data
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
```

```
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        1   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Switch#
Switch# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:05   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:02   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:04   1.1.1.1          49810       dhcp-snooping  1536  GigabitEthernet1/1
00:01:00:01:00:03   1.1.1.1          49810       dhcp-snooping  1024  GigabitEthernet1/1
00:01:00:01:00:01   1.1.1.1          49810       dhcp-snooping  1     GigabitEthernet1/1
Switch#
Switch# clear ip dhcp snoop bind
Switch# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Switch#
```

例 3：DHCP スヌーピング データベースへの情報の追加

手動で DHCP スヌーピング データベースにバインディングを追加するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# show ip dhcp snooping binding`	DHCP スヌーピング データベースを表示します。
ステップ 2	`Switch# ip dhcp snooping binding` *binding-id* `vlan` *vlan-id* `interface` *interface* `expiry` *lease-time*	ip dhcp snooping EXEC コマンドを使用してバインディングを追加します。
ステップ 3	`Switch# show ip dhcp snooping binding`	DHCP スヌーピング データベースを確認します。

次に、手動で DHCP スヌーピング データベースにバインディングを追加する例を示します。

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Switch#
Switch# ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gi1/1 expiry 1000

Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          992         dhcp-snooping  1     GigabitEthernet1/1
Switch#
```

DHCP スヌーピング情報の表示

スイッチ上のすべてのインターフェイスについて、DHCP スヌーピング バインディング テーブルおよび設定情報を表示できます。

バインディング テーブルの表示

各スイッチの DHCP スヌーピング バインディング テーブルには、信頼できないポートに関連したバインディング エントリが格納されています。テーブルには、trusted ポートに相互接続するホストに関する情報は収められていません。相互接続した各スイッチは、独自の DHCP スヌーピング バインディング テーブルを持つためです。

次に、スイッチの DHCP スヌーピング バインディング情報を表示する例を示します。

```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6943        dhcp-snooping  10    FastEthernet6/10
Switch#
```

表 38-2 で **show ip dhcp snooping binding** コマンド出力のフィールドを説明します。

表 38-2　show ip dhcp snooping binding コマンド出力

フィールド	説明
MAC Address	クライアント ハードウェアの MAC アドレス
IP Address	DHCP サーバに割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレス リース時間（秒）
Type	バインディング タイプ（DHCP スヌーピングによって学習されたダイナミック バインディングまたは静的に設定されたバインディング）
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続するインターフェイス

DHCP スヌーピング設定の表示

次に、スイッチの DHCP スヌーピング設定を表示する例を示します。

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 is enabled
Option82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface            Trusted        Rate limit (pps)
---------            -------        ----------------
FastEthernet2/1      yes            10
FastEthernet3/1      yes            none
GigabitEthernet1/1   no             20
Switch#
```

IP ソース ガードについて

この機能は、DHCP スヌーピングと同様、DHCP スヌーピングの信頼できないレイヤ 2 ポート上でイネーブルに設定されています。最初に、ポートのすべての IP トラフィックが、DHCP スヌーピング処理によってキャプチャされた DHCP パケットを除いてブロックされます。クライアントが DHCP サーバから有効な IP アドレスを受信する場合、またはユーザがスタティック IP 送信元バインディングを設定した場合に、Per-Port and VLAN Access Control List（PVACL）がポート上にインストールされます。この処理は、クライアント IP トラフィックをバインディングに設定された送信元 IP アドレスに制限するので、IP 送信元バインディングにない送信元 IP アドレスを持つ IP トラフィックが排除されます。このフィルタリングは、ホストがネイバー ホストの IP アドレスを名乗ってネットワークを攻撃することを制限します。

（注） DHCP スヌーピングがイネーブルにされた大量の VLAN のトランク ポート上で IP ソース ガードがイネーブルにされている場合、ACL ハードウェア リソースが不足し、代わりにパケットの一部がソフトウェアでスイッチングされる可能性があります。

（注） IP ソース ガードがイネーブルの場合、ACL ハードウェア プログラミングの代替方式を指定する場合があります。詳細については、「ACL によるネットワーク セキュリティの設定」の章の「TCAM プログラミングおよび ACL」を参照してください。

（注） インターフェイスがダウン ステートになっている場合は、TCAM が RACL ではなく、PACL に使用されます。

IP ソース ガードは、アクセスおよびトランクの両方を含むレイヤ 2 ポートだけをサポートしています。それぞれの信頼できないレイヤ 2 ポートには、2 つのレベルの IP トラフィック セキュリティ フィルタリングがあります。

- 送信元 IP アドレス フィルタ

  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。IP 送信元バインディング エントリに一致する送信元 IP アドレスを持つ IP トラフィックだけが許可されます。

  新しい IP 送信元エントリ バインディングがポートで作成または削除されると、IP 送信元アドレス フィルタが変更されます。IP 送信元バインディングの変更を反映するために、ポート PVACL がハードウェアで再計算および再適用されます。デフォルトでは、ポートに IP 送信元バインディングがない状態で IP フィルタがイネーブルにされている場合、すべての IP トラフィックを拒否するデフォルトの PVACL がポートにインストールされます。同様に、IP フィルタがディセーブルにされている場合、すべての IP 送信元フィルタ PVACL がインターフェイスから削除されます。

- 送信元 IP および MAC アドレス フィルタ

  IP トラフィックは送信元 IP アドレスと MAC アドレスに基づいてフィルタリングされます。IP 送信元バインディング エントリに一致する送信元 IP アドレスと MAC アドレスを持つ IP トラフィックだけが許可されます。

（注） IP ソース ガードが IP と MAC フィルタリング モードでイネーブルに設定されている場合、DHCP プロトコルが正常に動作するように、DHCP スヌーピング Option 82 がイネーブルに設定されている必要があります。Option 82 データがないと、スイッチは DHCP サーバ応答を転送するようにクライアント ホスト ポートを設置できません。そして、DHCP サーバ応答がドロップされ、クライアントは IP アドレスを取得できなくなります。

IP ソース ガードの設定

IP ソース ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# 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。 DHCP スヌーピングをディセーブルにするには、**no** キーワードを使用します。
ステップ 2	`Switch(config)# ip dhcp snooping vlan` *number* [*number*]	VLAN 上で DHCP スヌーピングをイネーブルにします。
ステップ 3	`Switch(config-if)# no ip dhcp snooping trust`	インターフェイスの信頼性を trusted または untrusted に設定します。 ネットワーク内部からのメッセージのみを受信するようにインターフェイスを設定する場合は、**no** キーワードを使用します。
ステップ 4	`Switch(config-if)# ip verify source vlan dhcp-snooping port-security`	ポート上の IP ソース ガード、送信元 IP、および送信元 MAC アドレス フィルタリングをイネーブルにします。
ステップ 5	`Switch(config-if)# switchport port-security limit rate invalid-source-mac N`	ポート上の学習済み送信元 MAC アドレスに対してセキュリティ レート制限をイネーブルにします。 （注）　この制限は、IP および MAC アドレスの両方をフィルタリングするように IP ソース ガードがイネーブルにされたポートにのみ適用されます。
ステップ 6	`Switch(config)# ip source binding` *mac-address* `Vlan` *vlan-id ip-address* `interface` *interface-name*	ポート上にスタティック IP バインディングを設定します。
ステップ 7	`Switch(config)# end`	コンフィギュレーション モードを終了します。
ステップ 8	`Switch# show ip verify source interface` *interface-name*	設定を確認します。

インターフェイス上のスタティック ホストを使用して IP ソース ガードを停止したい場合、インターフェイス コンフィギュレーション サブモードで次のコマンドを使用します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

インターフェイス コンフィギュレーション サブモードで「no ip device tracking」が使用されている場合は、実際に、このコマンドが解釈され、グローバル コンフィギュレーション モードで実行されるため、IP デバイス トラッキングがグローバルにディセーブルになります。「ip verify source tracking [port-security]」というコマンドが使用されるインターフェイスでは、IP デバイス トラッキングをグローバルにディセーブルにすると、スタティック ホストを使用した IP ソース ガードによって、このようなインターフェイスからのすべての IP トラフィックが拒否されます。

（注）　スタティック IP 送信元バインディングが設定できるのは、スイッチ ポート上だけです。レイヤ 3 ポート上で
ip source binding vlan interface コマンドを発行すると、「`Static IP source binding can only be configured on switch port`」というエラー メッセージが表示されます。

次に、VLAN 10 ～ 20 上でレイヤ 2 ポートごとの 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)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface fa6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa6/1      ip-mac       active       10.0.0.1                            10
Fa6/1      ip-mac       active       deny-all                            11-20
Switch#
```

この出力は、VLAN 10 に有効な DHCP バインディングが 1 つあることを示します。

PVLAN 上での IP ソース ガードの設定

PVLAN ポートでは、IP ソース ガードを有効にするためにプライマリ 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。プライマリ VLAN 上の IP ソース ガードは、自動的にセカンダリ VLAN に伝播されます。セカンダリ VLAN 上にスタティック IP 送信元バインディングを設定することはできますが、有効ではありません。手動でセカンダリ VLAN 上にスタティック IP 送信元バインディングを設定すると、次の意味の警告が表示されます。

警告　**IP 送信元フィルタは、IP 送信元バインディングが設定されたセカンダリ VLAN では有効にならない可能性があります。PVLAN 機能がイネーブルになっている場合は、プライマリ VLAN 上の IP 送信元フィルタがすべてのセカンダリ VLAN に自動的に伝播されます。**

IP ソース ガード情報の表示

スイッチ上のすべてのインターフェイスに関する IP ソース ガード PVACL 情報を表示するには、**show ip verify source** コマンドを使用します。

- 次に、VLAN 10 ～ 20 で DHCP スヌーピングがイネーブルにされていて、IP フィルタリングに対してインターフェイス fa6/1 が設定されていて、VLAN 10 に既存の IP アドレス バインディング 10.0.01 が存在する場合に表示される PVACL の例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
```

（注）　2 番めのエントリは、デフォルト PVACL（すべての IP トラフィックを拒否）が、有効な IP 送信元バインディングを持たず、スヌーピングがイネーブルにされた VLAN のポート上にインストールされていることを示します。

- 次に、trusted ポートに対して表示される PVACL の例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/2      ip           inactive-trust-port
```

- 次に、DHCP スヌーピングが設定されていない VLAN のポートに対して表示される PVACL の例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/3      ip           inactive-no-snooping-vlan
```

- 次に、複数のバインディングが IP/MAC フィルタリングに設定されているポートに対して表示される PVACL の例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip-mac       active       deny-all         deny-all        12-20
```

- 次に、ポート セキュリティが設定されておらず、IP/MAC フィルタリングが設定されているポートに対して表示される PVACL の例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/5      ip-mac       active       10.0.0.3         permit-all      10
fa6/5      ip-mac       active       deny-all         permit-all      11-20
```

（注） MAC フィルタで permit-all が表示されるのは、ポート セキュリティがイネーブルにされていないためです。MAC フィルタはポート/VLAN に適用できず、事実上ディセーブルの状態です。常にポート セキュリティを最初にイネーブルにしてください。

- 次に、IP 送信元フィルタ モードが設定されていないポートに **show ip verify source** コマンドを入力した場合に表示されるエラー メッセージの例を示します。

```
IP Source Guard is not configured on the interface fa6/6.
```

また、**show ip verify source** コマンドを使用して、IP ソース ガードがイネーブルにされたスイッチ上のすべてのインターフェイスを表示できます。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
fa6/2      ip           inactive-trust-port
fa6/3      ip           inactive-no-snooping-vlan
fa6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip-mac       active       deny-all         deny-all        12-20
fa6/5      ip-mac       active       10.0.0.3         permit-all      10
fa6/5      ip-mac       active       deny-all         permit-all      11-20
```

IP 送信元バインディング情報の表示

スイッチ上のすべてのインターフェイス上で設定された IP 送信元バインディングを表示するには、**show ip source binding** コマンドを使用します。

```
Switch# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6522        dhcp-snooping  10    FastEthernet6/10
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    FastEthernet6/10
Switch#
```

表 38-3 で **show ip source binding** コマンド出力のフィールドについて説明します。

表 38-3　show ip source binding コマンド出力

フィールド	説明
MAC Address	クライアント ハードウェアの MAC アドレス
IP Address	DHCP サーバに割り当てられたクライアント IP アドレス
Lease(sec)	IP アドレス リース時間（秒）
Type	バインディング タイプ（Command-Line Interface（CLI; コマンドライン インターフェイス）から設定されたスタティック バインディング、および DHCP スヌーピングによって学習されたダイナミック バインディング）
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続するインターフェイス