CHAPTER 37

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。

この章で説明する主な内容は、次のとおりです。

- 「DHCP スヌーピングの概要」（P.37-1）
- 「スイッチ上での DHCP スヌーピングの設定」（P.37-7）
- 「DHCP スヌーピング情報の表示」（P.37-17）
- 「IP ソース ガードの概要」（P.37-18）
- 「スイッチ上での IP ソース ガードの設定」（P.37-19）
- 「IP 送信元バインディング情報の表示」（P.37-21）
- 「スタティック ホスト用 IP ソース ガードの設定」（P.37-22）

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

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

DHCP スヌーピングの概要

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 サーバの間でファイアウォールに似た役割を果たします。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。

- 「信頼できるソースおよび信頼できないソース」（P.37-2）
- 「DHCP スヌーピング データベース エージェントの概要」（P.37-3）
- 「Option 82 データ挿入」（P.37-4）

信頼できるソースおよび信頼できないソース

DHCP スヌーピング機能では、トラフィック ソースが信頼できるかできないかについて特定されます。信頼できない送信元の場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。このような攻撃を防ぐために、DHCP スヌーピング機能では、メッセージをフィルタ処理し、信頼できないソースからのトラフィックのレートを制限します。

企業ネットワークでは、管理担当者の管理下にあるデバイスは、信頼できるソースです。これらのデバイスには、ネットワークのスイッチ、ルータ、サーバが含まれます。ファイアウォールで保護されていないデバイスまたはネットワークの外側にあるデバイスは、信頼できないソースです。ホスト ポートは、一般的に、信頼できないソースとして扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー スイッチなど）。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の信頼状態は、信頼できない状態になります。DHCP サーバ インターフェイスは、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。ユーザのネットワーク内でデバイス（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（注）　DHCP スヌーピングが正常に機能するには、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続し、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だけ転送されるようにする必要があります。

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。

バインディングを保持するファイルの形式は、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
```

ファイル内の各エントリには、チェックサムを示すタグが付けられます。これは、ファイルが読み取られるたびに、エントリの検証に使用されます。1 行めの <initial-checksum> エントリは、最新の書き込みに関連する各エントリを、以前の書き込みに関連する各エントリから区別します。

次に、バインディング ファイルの例を示します。

```
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
```

各エントリは、IP アドレス、VLAN、MAC アドレス、リース期間（16 進数単位）、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を示します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、72 バイトのデータ、スペース、およびチェックサムの順で設定されます。

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。より多くの変更を蓄積してから、実際の書き込みを一括して行えるように、この書き込みの実行には遅延時間を設定できます。個々の転送には、未完了の転送が中断されるまでの時間を示すタイムアウトが関連付けられます。このようなタイマーを、書き込み遅延および中断タイムアウトと呼びます。

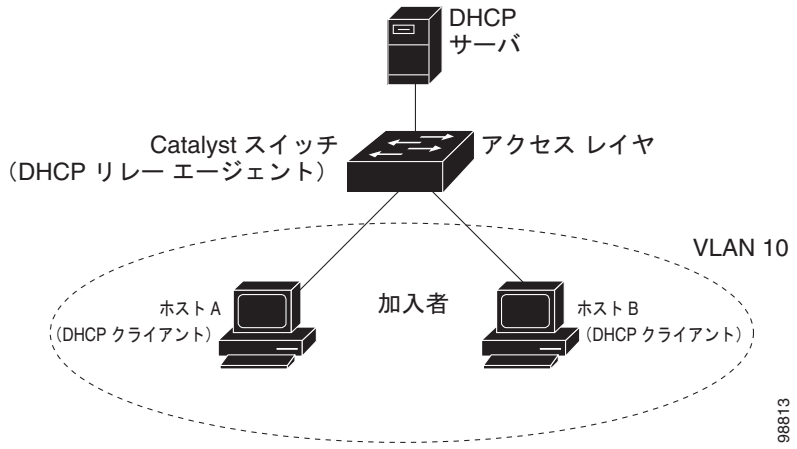
Option 82 データ挿入

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。サブスクライバ 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）　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あり、この機能を使用する加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 37-1 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 37-1　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。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。サブオプションの設定の詳細については、「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.37-10）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、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート 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ようなポリシーを実装したりできます。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。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。

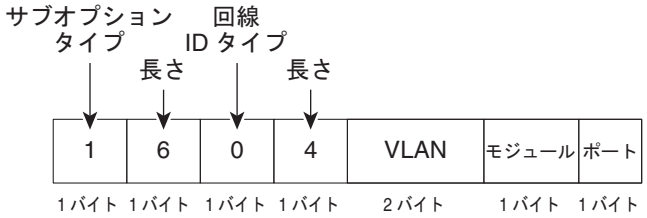
デフォルトのサブオプション設定では、説明したイベントが順に発生すると、図 37-2 にあるフィールドの値は変更されません。

- 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 37-2 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 37-2　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

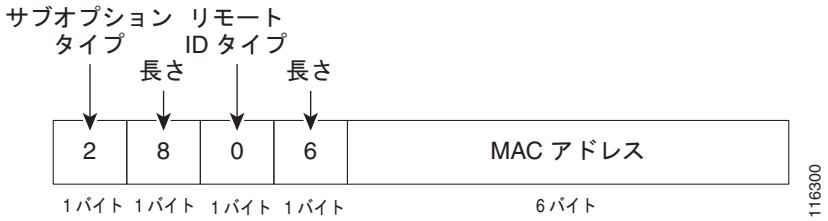


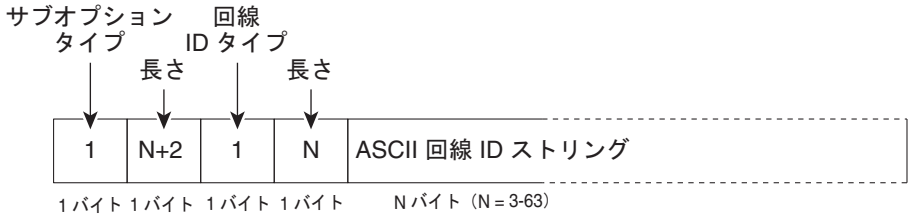
図 37-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力されると、スイッチにより、パケット フォーマットが使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

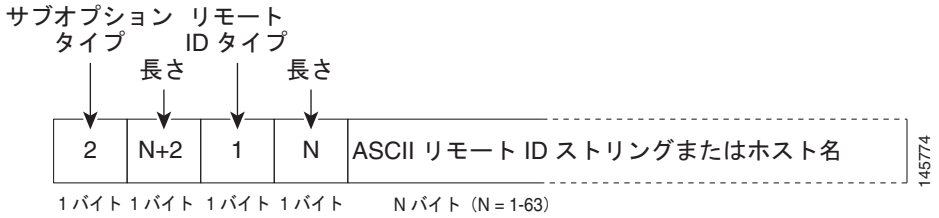
- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 37-3　ユーザ設定の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）



スイッチ上での 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 で DHCP スヌーピングを使用するには、事前に DHCP スヌーピングをグローバルにイネーブルにしておく必要があります。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。

DHCP スヌーピングをイネーブルにしたあと、すべての DHCP リレー情報オプション コンフィギュレーション コマンドはディセーブルになります。次のコマンドがあります。

- **ip dhcp relay information check**
- **ip dhcp relay information policy**
- **ip dhcp relay information trusted**
- **ip dhcp relay information trust-all**

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。

- 「DHCP スヌーピングのデフォルト設定」（P.37-8）
- 「DHCP スヌーピングのイネーブル化」（P.37-8）
- 「集約スイッチ上での DHCP スヌーピングの設定」（P.37-10）
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.37-10）
- 「プライベート VLAN 上での DHCP スヌーピングのイネーブル化」（P.37-12）
- 「PVLAN 上での DHCP スヌーピングのイネーブル化」（P.37-12）
- 「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」（P.37-13）
- 「データベース エージェントの設定例」（P.37-13）

（注）　DHCP サーバの設定の詳細については、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 37-1 は、各 DHCP スヌーピング オプションのデフォルトの設定値をすべて示します。

表 37-1　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 / 状態
DHCP スヌーピング	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
DHCP スヌーピング情報オプション allow-untrusted	ディセーブル
DHCP スヌーピング レート制限	infinite（レート制限のディセーブルと同じように機能）
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

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化します。 **no** キーワードを使用して DHCP スヌーピングをディセーブルにできます。
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。

	コマンド	目的
ステップ 3	`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 4	`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 5	`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 6	`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、信頼できるインターフェイスはスイッチのすべての DHCP トラフィックを収束するため、レート制限を高い値に調整する必要があることに注意してください。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。1 つの VLAN で設定するには、1 つの VLAN 番号を入力します。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。

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 スヌーピングおよび Option 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化します。
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	`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。これがデフォルト設定です。

	コマンド	目的
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。 次のようにリモート ID を設定できます。 • 63 文字までの ASCII 文字列（スペースなし） • スイッチに設定されたホスト名 **（注）** ホスト名が 64 文字以上の場合、リモート ID 設定で 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 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。 デフォルト設定では無効になっています。 **（注）** このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
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、**vlan-mod-port** の形式です。 回線 ID は 3 ～ 63 の ASCII 文字列（スペースなし）を設定できます。
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 untrusted です。
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。trusted 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 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のクライアント ハードウェア アドレスと一致することを確認します。
ステップ 13	`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。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-range* グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジ スイッチによって 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、ポートのレート制限を 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 gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN 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 コマンドを実行すると、DHCP スヌーピングがイネーブルにされたすべての VLAN（プライマリおよびセカンダリの両方）が表示されます。

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 フォン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。

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、および関連する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状態、および転送に関連する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する統計情報を消去します。
Switch# **renew ip dhcp snooping database [validation none] [***url***]**	（任意）指定の URL にあるファイルから、エントリの読み取りを要求します。
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 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。

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、指定の場所にバインディングを保存するように DHCP スヌーピング データベース エージェントを設定し、この設定内容と動作状態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、動作状態のほか、書き込み遅延時間および中断タイマーが経過するまでに残された時間を表します。

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 アドレスと VLAN の組み合わせに重点を置いています。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。このような状態を、バインディング コリジョンと呼びます。

ファイル内のエントリに示されたリース期間が、ファイルの読み取り時にすでに経過している場合は、このエントリは無効になります。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いずれ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。サポートされない VLAN は、エントリの示す VLAN がシステム上でサポートされない場合に無視されたエントリの数を示します。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、上記の条件が 1 つ以上該当するために無視された 1 つ以上のバインディングを持つ、個々の読み取りに対するカウンタです。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のために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

TFTP ファイルからエントリを手動で読み取るには、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**	読み取りのステータスを表示します。
ステップ 4	Switch# **show ip dhcp snoop bind**	バインディングの読み取りが適切に行われたかどうかを確認します。

次に、tftp://10.1.1.1/directory/file からエントリを手動で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

DHCP スヌーピング データベースにバインディングを手動で追加するには、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、DHCP スヌーピング データベースにバインディングを手動で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 37-2 では、**show ip dhcp snooping binding** コマンドの出力結果における各フィールドについて説明します。

表 37-2　show ip dhcp snooping binding コマンドの出力結果

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 サーバから割り当てられたクライアント IP アドレス
Lease (seconds)	IP アドレスのリース期間
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 ホストに接続され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 ガードの概要

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、ポート単位 VLAN アクセス コントロール リスト（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、「Configuring Network Security with ACLs」の章の「TCAM Programming and ACLs」を参照してください。

（注） インターフェイスがダウン ステートの場合、TCAM リソースは消費されません。

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。

スイッチ上での 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化します。 **no** キーワードを使用して DHCP スヌーピングをディセーブルにできます。
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。 ネットワーク内からのメッセージだけ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、このコマンドは変換され、実際にグローバル コンフィギュレーション モードで実行されて、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]」というコマンドを使用するすべてのインターフェイスでは、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ると、スタティック ホストを使用する IP ソース ガードが、これらのインターフェイスからのすべての IP トラフィックを拒否するようになります。

（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。プライベート VLAN 機能がイネーブルにされている場合、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に設定された 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 37-3 では、**show ip source binding** コマンドの出力結果における各フィールドについて説明します。

表 37-3　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 サーバから割り当てられたクライアント IP アドレス
Lease (seconds)	IP アドレスのリース期間
Type	バインディング タイプ（CLI 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 ホストに接続されるインターフェイス

スタティック ホスト用 IP ソース ガードの設定

（注） Supervisor Engine 6-E は、この機能をサポートして*いません*。

（注） スタティック ホストの IPSG は、アップリンク ポートでは使用しないでください。

スタティック ホストの IP ソース ガード（IPSG）は、IPSG 機能を非 DHCP およびスタティック環境に拡張します。既存の IP ソース ガード（IPSG）機能は、DHCP スヌーピング機能により作成されたエントリを使用して、スイッチに接続されたホストを検証します。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。基本的に、DHCP 環境は IPSG が機能するための前提条件になります。スタティック ホストの IPSG 機能は、DHCP に対する IPSG の依存性を削除します。スイッチは、ARP 要求または他の IP パケットに基づいてスタティック エントリを作成し、このエントリを使用して指定ポートの有効なホストのリストを保持します。さらに、ユーザは、指定ポートにトラフィックを送信できるホスト数を指定できます。これは、レイヤ 3 でのポート セキュリティに相当します。

（注） 複数ネットワーク インターフェイスを持つ一部の IP ホストは、一部の無効パケットをネットワーク インターフェイスに投入することがあります。これらの無効パケットには、送信元アドレスとしてのホストの別のネットワーク インターフェイスの IP/MAC アドレスを含みます。これにより、ホストに接続しているスイッチにあるスタティック ホストの IPSG が、無効な IP/MAC アドレス バインディングを学習し、有効なバインディングを拒否します。無効パケットの投入を回避するには、対応する OS またはそのホストのネットワーク デバイスのベンダーに相談する必要があります。

スタティック ホストの IPSG は、最初に ACL ベースのスヌーピング メカニズムを介して動的に IP MAC バインディングを学習します。IP/MAC バインディングは、ARP および IP パケットを経由してスタティック ホストから学習され、デバイス トラッキング データベースを使用して保存されます。指定ポートで動的に学習された、または静的に設定された IP アドレスの数が最大限度に達すると、新しい IP アドレスを持つパケットはハードウェアでドロップされます。何らかの理由で移動されたまたは

消去されたホストを扱うために、スタティック ホストの IPSG 機能は IP デバイス トラッキング機能を強化し、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングと同時に使用できます。複数バインディングが、DHCP とスタティック ホストの両方に接続されているポート上で確立されます（つまり、バインディングは、デバイス トラッキング データベースだけでなく、DHCP スヌーピング バインディング データベースにも保存されます）。

次の内容について説明します。

- 「レイヤ 2 アクセス ポート上のスタティック ホストの IPSG」（P.37-23）
- 「PVLAN ホスト ポート上のスタティック ホストの IPSG」（P.37-26）

レイヤ 2 アクセス ポート上のスタティック ホストの IPSG

レイヤ 2 アクセス ポート上でスタティック ホストの IPSG を設定できます。

レイヤ 2 アクセス ポート上で IP フィルタを使用してスタティック ホストの IPSG 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 device tracking`	IP ホスト テーブルをオンにします。
ステップ 2	`Switch(config)# interface fastEthernet <a/b>`	IP 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	`Switch(config-if)# switchport mode access`	アクセスとしてポートを設定します。
ステップ 4	`Switch(config-if)# switchport access vlan <n>`	このポートに VLAN を設定します。
ステップ 5	`Switch(config-if)# ip device tracking maximum <n>`	このポート上でバインディングの最大限度を確立します。 最大限度は 10 です。
ステップ 6	`Switch(config-if)# switchport port-security`	（任意）このポートのポート セキュリティをアクティブにします。
ステップ 7	`Switch(config-if)# switchport port-security maximum <n>`	（任意）このポートの MAC アドレスの最大数を確立します。
ステップ 8	`Switch(config-if)# ip verify source tracking [port-security]`	このポート上でスタティック ホストの IPSG をアクティブにします。
ステップ 9	`Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	`Switch# show ip verify source interface-name`	設定を確認します。
ステップ 11	`Switch# show ip device track all [active | inactive] count`	スイッチ インターフェイス上の指定ホストの IP/MAC バインディングを表示して、設定を確認します。 • **all active**：アクティブな IP/MAC バインディング エントリだけを表示します。 • **all inactive**：非アクティブな IP/MAC バインディング エントリだけを表示します。 • **all**：アクティブおよび非アクティブの IP/MAC バインディング エントリを表示します。

インターフェイス上でスタティック ホストの IPSG を停止するには、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"
```

ポート上でスタティック ホストの IPSG をイネーブルにするには、次のコマンドを実行します。

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ****set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on the port
```

注意　IP デバイス トラッキングをグローバルにイネーブルにせずに、またはそのインターフェイス上の IP デバイス トラッキングの最大値を設定せずに、ポートで **ip verify source tracking [port-security]** インターフェイス コンフィギュレーション コマンドだけを設定した場合、スタティック ホストの IPSG は、そのインターフェイスからのすべての IP トラフィックを拒否します。

（注）　上記の問題は、PVLAN ホスト ポート上のスタティック ホストの IPSG にも適用されます。

次に、レイヤ 2 アクセス ポートでの IP フィルタを使用したスタティック ホストの IPSG をイネーブルにし、インターフェイス Fa4/3 上で 3 つの有効 IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip trk       active       40.1.1.24                           10
Fa4/3      ip trk       active       40.1.1.20                           10
Fa4/3      ip trk       active       40.1.1.21                           10
```

次に、レイヤ 2 アクセス ポートで IP/MAC フィルタを使用してスタティック ホストの IPSG をイネーブルにし、インターフェイス Fa4/3 上の 5 つの有効 IP/MAC バインディングを確認して、このインターフェイス上のバインディング数が最大限度に達したかどうかを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip-mac trk   active       40.1.1.24        00:00:00:00:03:04  1
Fa4/3      ip-mac trk   active       40.1.1.20        00:00:00:00:03:05  1
Fa4/3      ip-mac trk   active       40.1.1.21        00:00:00:00:03:06  1
Fa4/3      ip-mac trk   active       40.1.1.22        00:00:00:00:03:07  1
Fa4/3      ip-mac trk   active       40.1.1.23        00:00:00:00:03:08  1
```

次に、すべてのインターフェイスのすべての IP/MAC バインディングを表示する例を示します。CLI で非アクティブ エントリと一緒にすべてのアクティブ エントリが表示されていることを確認します。インターフェイスでホストが学習されると、この新しいエントリは、アクティブとマークされます。同じホストが現在のインターフェイスから切断され、別のインターフェイスの接続されると、ホストが検出され次第、新しい IP/MAC バインディング エントリがアクティブとして表示されます。ここで、前のインターフェイス上のこのホストの古いエントリは、非アクティブとしてマークが付けられます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.1       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
```

次に、すべてのインターフェイスのすべてのアクティブ IP/MAC バインディングを表示する例を示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet4/1     ACTIVE
```

次に、すべてのインターフェイスのすべての非アクティブ IP/MAC バインディングを表示する例を示します。ホストは、最初に GigabitEthernet 3/1 で学習されてから、GigabitEthernet 4/1 に移動されました。したがって、GigabitEthernet 3/1 で学習された IP/MAC バインディング エントリが非アクティブとしてマーク付けされます。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
```

```
200.1.1.3       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet3/1     INACTIVE
```

次に、すべてのインターフェイスのすべての IP デバイス トラッキング ホスト エントリのカウントを表示する例を示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
------------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
------------------------------------------------------------------------
Fa4/3                  5
```

PVLAN ホスト ポート上のスタティック ホストの IPSG

PVLAN ホスト ポート上でスタティック ホストの IPSG を設定できます。

PVLAN ホスト ポート上で IP フィルタを使用してスタティック ホストの IPSG 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)# **vlan** <*n1*>	コンフィギュレーション VLAN モードを開始します。
ステップ 2	Switch(config-vlan)# **private-vlan primary**	PVLAN ポートにプライマリ VLAN を確立します。
ステップ 3	Switch(config-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 4	Switch(config)# **vlan** <*n2*>	コンフィギュレーション VLAN モードを開始します。
ステップ 5	Switch(config-vlan)# **private-vlan isolated**	PVLAN ポートに独立 VLAN を確立します。
ステップ 6	Switch(config-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 7	Switch(config)# **vlan** <*n1*>	コンフィギュレーション VLAN モードを開始します。
ステップ 8	Switch(config-vlan)# **private-vlan association 201**	独立 PVLAN ポートに VLAN を関連付けます。
ステップ 9	Switch(config-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 10	Switch(config)# **interface fastEthernet** <*a/b*>	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 11	SSwitch(config-if)# **switchport mode private-vlan host**	（任意）ポートを PVLAN ホストとして確立します。
ステップ 12	SSwitch(config-if)# **switchport private-vlan host-association** <a> <b>	（任意）このポートを対応する PVLAN に関連付けます。
ステップ 13	Switch(config-if)# **ip device tracking maximum** <*n*>	このポート上でバインディングの最大限度を確立します。
ステップ 14	Switch(config-if)# **ip verify source tracking** [**port-security**]	このポート上でスタティック ホストの IPSG をアクティブにします。
ステップ 15	Switch(config-if)# **end**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 16	Switch# **show ip device tracking all**	設定を確認します。
ステップ 17	Switch# **show ip verify source** *interface-name*	設定を確認します。

次に、PVLAN ホスト ポート上で IP フィルタを使用し、スタティック ホストの IPSG をイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------
40.1.1.24       0000.0000.0304  200  FastEthernet4/3        ACTIVE
40.1.1.20       0000.0000.0305  200  FastEthernet4/3        ACTIVE
40.1.1.21       0000.0000.0306  200  FastEthernet4/3        ACTIVE
40.1.1.22       0000.0000.0307  200  FastEthernet4/3        ACTIVE
40.1.1.23       0000.0000.0308  200  FastEthernet4/3        ACTIVE
```

出力では、インターフェイス Fa4/3 で学習された 5 つの有効な IP/MAC バインディングを示しています。PVLAN の場合、バインディングはプライマリ VLAN ID と関連付けられます。したがって、この例ではプライマリ VLAN ID である 200 が表に表示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa4/3      ip trk       active       40.1.1.23                           200
Fa4/3      ip trk       active       40.1.1.24                           200
Fa4/3      ip trk       active       40.1.1.20                           200
Fa4/3      ip trk       active       40.1.1.21                           200
Fa4/3      ip trk       active       40.1.1.22                           200
Fa4/3      ip trk       active       40.1.1.23                           201
Fa4/3      ip trk       active       40.1.1.24                           201
Fa4/3      ip trk       active       40.1.1.20                           201
Fa4/3      ip trk       active       40.1.1.21                           201
Fa4/3      ip trk       active       40.1.1.22                           201
```

この出力からは、5 つの有効な IP-MAC バインディングはプライマリとセカンダリの両方の VLAN 上にあることがわかります。