CHAPTER 48

# DHCP スヌーピングの設定

この章では、Cisco IOS Release 12.2SX に Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する手順について説明します。

（注） この章で使用している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 の『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

この章で説明する内容は、次のとおりです。



## DHCP スヌーピングの設定

ここでは、DHCP スヌーピング機能について説明します。

# DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバ間のファイアウォールのように機能するセキュリティ機能です。DHCP スヌーピング機能では以下の処理を実行します。

- 信頼しない送信元から受信した DHCP メッセージを検証し、無効なメッセージをフィルタリングします。
- 信頼できる送信元と信頼できない送信元からの DHCP トラフィックのレートを制限します。
- DHCP スヌーピング バインディング データベースを構築し維持します。これには、専用 IP アドレスのある信頼できないホストに関する情報が含まれています。
- 信頼できないホストからの後続要求を検証するために DHCP スヌーピング バインディング データベースを利用します。

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）などの他のセキュリティ機能も、DHCP スヌーピング バインディング データベースに格納されている情報を使用します。

DHCP スヌーピングは VLAN 単位でイネーブルにします。デフォルトでは、この機能はすべての VLAN で非アクティブです。この機能は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

DHCP スヌーピング機能は Route Processor（RP; ルート プロセッサ）上でソフトウェアに実装されています。したがって、対応 VLAN の全 DHCP メッセージが PFC で代行受信され、処理用に RP へ転送されます。

# 信頼できる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信頼できないのかを判別します。信頼できない送信元は、トラフィック攻撃を開始したり他の悪意のある動作を行う可能性があります。そのような攻撃を防ぐために、DHCP スヌーピング機能はメッセージをフィルタリングし、信頼できない送信元からのトラフィックのレートを制限します。

エンタープライズ ネットワークでは、管理制御下の装置は信頼できる送信元です。これらの装置には、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを超える装置やネットワーク外の装置は信頼できない送信元です。ホスト ポートおよび不明な DHCP サーバは、通常信頼できない送信元として取り扱われます。

信頼できないポートの不明なネットワーク上の DHCP サーバは、*スプリアス DHCP サーバ*といいます。スプリアス DHCP サーバは、DHCP サーバをイネーブルにしてロードされた任意の機器です。例として、DHCP サーバをイネーブルにしてロードされたデスクトップ システムとラップトップ システムや、ネットワークに接続された側で DHCP 要求を受け入れるワイヤレス アクセス ポイントがあります。スプリアス DHCP サーバが検出されない場合、ネットワーク障害のトラブルシューティングが困難になります。スプリアス DHCP サーバを検出するには、応答がスイッチに返信されるように、ダミーの DHCPDISCOVER パケットをすべての DHCP サーバに送信します。

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装置は信頼できない送信元です（カスタマーのスイッチなど）。ホスト ポートも信頼できない送信元です。

スイッチでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

全インターフェイスのデフォルトの信頼状態は untrusted です。DHCP サーバ インターフェイスを trusted に設定する必要があります。ネットワーク内の装置（スイッチやルータ）に接続する場合、他のインターフェイスを trusted に設定することも可能です。通常、ホスト ポート インターフェイスを trusted には設定しません。

（注）　信頼できない DHCP メッセージが信頼されるインターフェイスだけに転送されるため、DHCP スヌーピングが正しく機能するには、すべての DHCP サーバが、信頼できるインターフェイスを介してスイッチに接続されている必要があります。

# 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 データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

DHCP スヌーピング機能は、代行受信された DHCP メッセージから抽出された情報を使用してダイナミックデータベースを構築し維持します。DHCP スヌーピングがイネーブルの VLAN とホストが関連付けられている場合、データベースには信頼できない各ホストのエントリが専用 IP アドレスとともに含まれています。信頼できるインターフェイスを通じて接続されたホストのエントリがデータベースには含まれていません。

スイッチが特定の DHCP メッセージを受信すると、DHCP スヌーピング機能はデータベースを更新します。たとえば、スイッチが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。IP アドレスのリース期限が過ぎたり、スイッチがホストから DHCPRELEASE メッセージを受信すると、この機能によってデータベース内のエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、専用 IP アドレス、リース期間、バインディングの種類、ホストに関連付けられた VLAN（仮想 LAN）の番号およびインターフェイス情報が含まれています。

# パケット検証

スイッチは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。以下の条件が発生しないかぎり（パケットがドロップされる場合）、スイッチは DHCP パケットを転送します。

- スイッチがネットワークまたはファイアウォール外部の DHCP サーバから（DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY などの）パケットを受信した場合。
- スイッチが信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピング MAC アドレス確認オプションがオンになっている場合にだけ実行されます。
- スイッチが、DHCP スヌーピング バインディング テーブル内にエントリが存在する信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- スイッチが、リレー エージェントの IP アドレス（0.0.0.0 以外）を含む DHCP パケットを受信した場合。

信頼できない集約スイッチのポートに接続された信頼できるエッジ スイッチをサポートするため、信頼できないポートの DHCP Option 82 機能をイネーブルにして、信頼できない集約スイッチのポートが Option 82 情報を含む DHCP パケットを受信するようにできます。集約スイッチに接続するエッジ スイッチのポートを、信頼できるポートとして設定します。

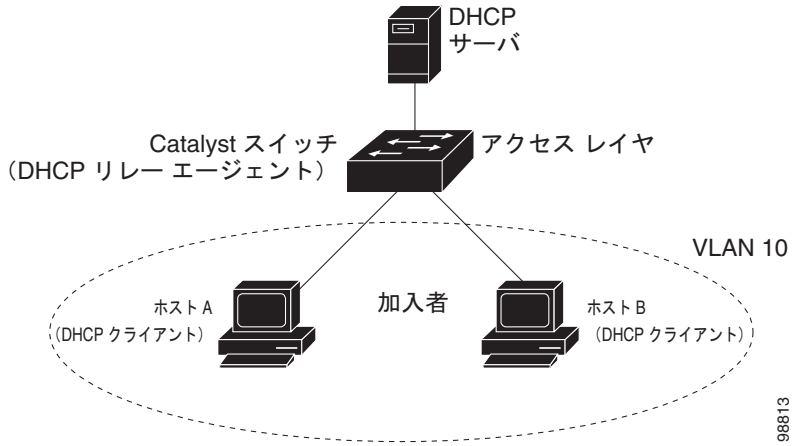
（注）　信頼できないポートの DHCP Option 82 機能がイネーブルである場合は、集約スイッチでダイナミック ARP インスペクション検査を使用して、信頼できない入力インターフェイスを保護します。

# DHCP スヌーピングの 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 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、こ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。加入者 LAN 上の複数のホストをアクセス スイッチの同一ポートに接続でき、これらは一意に識別されます。

図 48-1 は、メトロポリタン イーサネット ネットワーク内において、アクセス レイヤのスイッチに接続されている各加入者の IP アドレスを、一元的な DHCP サーバが割り当てる例を示します。DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェントにヘルパー アドレスを設定することで、ブロードキャスト転送を可能にし、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 48-1　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**




スイッチに対して DHCP スヌーピング情報の Option 82 機能をイネーブルにすると、以下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、パケット内に 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（回線 ID サブオプション）が含まれます。
- IEEE 802.1X ポートベース認証がイネーブルの場合、スイッチはホストの 802.1X 認証済ユーザ ID 情報（RADIUS 属性サブオプション）もパケットに追加します。「DHCP スヌーピングを使った 802.1X 認証の使用」（P.54-10）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、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

- DHCP サーバ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 または回線 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えます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる 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 Option 82 フィールドをエコーします。
- 要求がスイッチによってサーバに中継されている場合は、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、および場合によっては回線 ID フィールドを検査することで、このスイッチ自身が最初に Option 82 データを挿入したことを確認します。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。

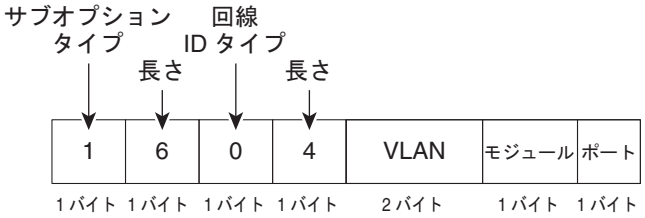
上記の一連のイベントが発生する間、図 48-2 に示す以下のフィールドの値は変更されません。

- 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
  - 回線 ID タイプの長さ

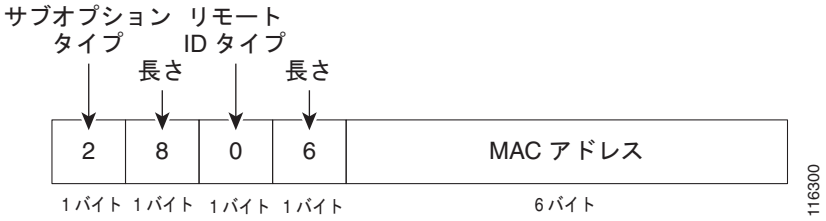
図 48-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化されている場合、および **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合です。回線 ID サブオプションの場合は、モジュール フィールドはモジュールのスロット番号となります。

**図 48-2　　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**




# DHCP スヌーピング データベース エージェントの概要

リロード後もバインディングを維持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。このエージェントを使用しないと、DHCP スヌーピングによって確立されたバインディングはリロード後に失われてしまい、同様に接続も失われます。

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。スイッチはリロード時にこのファイルを読み取り、バインディング用のデータベースを構築します。スイッチはデータベースが変更されるたびにこのファイルに書き込むことで、このファイルを最新に保ちます。

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。各エントリの最後に示されるチェックサムは、ファイルの冒頭から、エントリに関連付けられたすべてのバイトの合計に基づいて計算されます。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構成されます。

ブートアップ時、計算されたチェックサムと保存されたチェックサムが等しい場合は、スイッチはファイルから各エントリを読み取り、各バインディングを DHCP スヌーピング データベースに追加します。計算されたチェックサムが保存されたチェックサムと異なる場合は、ファイルから読み取られたこのエントリは無視され、エントリ以降のすべてのエントリも無視されます。また、スイッチはファイルから読み取ったエントリのうち、リース期間が失効しているすべてのエントリも無視します。この場合は、リース期間としてすでに経過した期間が示されているので、スイッチはこの値に基づき判断します。エントリ内で参照されるインターフェイスが、システム上にすでに存在しない場合、ルータ ポートである場合、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場合も、このエントリは無視されます。

スイッチが新たな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は、スイッチは変更されたエントリをスヌーピング データベースから抽出し、これら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。

# DHCP スヌーピングのデフォルト設定

表 48-1 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示します。

**表 48-1　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 |
| 信頼できないポートの DHCP Option 82 機能 | ディセーブル |
| DHCP スヌーピング レート制限 | なし |
| DHCP スヌーピング信頼状態 | Untrusted |
| DHCP スヌーピング VLAN | ディセーブル |
| DHCP スヌーピング スプリアス サーバ検出 | ディセーブル |
| DHCP スヌーピング検出スプリアス間隔 | 30 分 |

# DHCP スヌーピング設定時の制約事項および注意事項

このセクションでは、DHCP スヌーピング設定時の制約事項および注意事項について説明します。



## DHCP スヌーピング設定時の制約事項

DHCP スヌーピングを設定する場合は、次の制約事項に従ってください。

- DHCP スヌーピング データベースには少なくとも 8,000 バインディングが格納されます。
- DHCP スヌーピングをイネーブルにすると、スイッチでは以下の Cisco IOS DHCP コマンドを使用できなくなります。
  - **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

  これらのコマンドを入力すると、スイッチはエラー メッセージを返し、設定は適用されません。

## DHCP スヌーピング設定時の注意事項

DHCP スヌーピングを設定する際に、以下の注意事項に従ってください。

- 少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにして、DHCP をスイッチでグローバルにイネーブルにするまで、DHCP スヌーピングはアクティブにはなりません。
- 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化するには、DHCP サーバおよび DHCP リレー エージェントとして機能する装置を、事前に設定およびイネーブル化しておく必要があります。
- DHCP サーバの設定については、次の URL で、『*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
- レイヤ 2 LAN 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、このポートを信頼できるポートとして設定します。
- レイヤ 2 LAN 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、このポートを信頼できないポートとして設定します。
- 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 スヌーピングをイネーブルにすると、プライマリ VLAN の設定はすべて、関連付けられたセカンダリ VLAN に伝播します。
  - プライマリ VLAN で DHCP スヌーピングを設定してから、関連付けられたセカンダリ VLAN で DHCP スヌーピングを別の値で設定すると、セカンダリ VLAN の設定は無効になります。

- プライマリ VLAN で DHCP スヌーピングが設定されていない場合に、セカンダリ VLAN で DHCP スヌーピングを設定すると、設定はセカンダリ VLAN だけで有効になります。
- セカンダリ VLAN 上で DHCP スヌーピングを手動設定すると、次のメッセージが表示されます。

```
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を含む）が表示されます。

# DHCP スヌーピングの最小設定

DHCP スヌーピング機能の最小設定手順は以下のとおりです。

1. DHCP サーバを定義し、設定します。

   DHCP サーバの設定については、次の URL で、『*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

2. 少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにします。

   デフォルトで、DHCP スヌーピングがすべての VLAN で非アクティブです。「VLAN 上での DHCP スヌーピングのイネーブル化」（P.48-12）を参照してください。

3. DHCP サーバが信頼できるインターフェイスを通じて接続されていることを確認します。

   デフォルトでは、全インターフェイスの信頼状態は untrusted です。「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.48-14）を参照してください。

4. DHCP スヌーピング データベース エージェントを設定します。

   この手順により、再起動またはスイッチオーバー後にデータベース エントリが復元されるようになります。「DHCP スヌーピング データベース エージェントの設定」（P.48-16）を参照してください。

5. DHCP スヌーピングをグローバルにイネーブル化します。

   この機能は、この手順を完了するまで有効になりません。「DHCP スヌーピングのグローバルなイネーブル化」（P.48-10）を参照してください。

DHCP リレーをスイッチで設定する場合、以下の追加ステップが必要です。

1. DHCP リレー エージェント IP アドレスを定義し、設定します。

   DHCP サーバが DHCP クライアントとは別のサブネット内にある場合、サーバ IP アドレスをクライアント側 VLAN のヘルパー アドレス フィールドに設定します。

2. 信頼できないポート機能上に DHCP Option 82 を設定します。

   「信頼できないポート上の DHCP Option 82 機能のイネーブル化」（P.48-11）を参照してください。

# DHCP スヌーピングの設定

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 スヌーピングのグローバルなイネーブル化

（注）　最後の設定手順としてこのコマンドを設定します（またはスケジュールされているメンテナンス期間中に DHCP 機能をイネーブルにします）。DHCP スヌーピングをグローバルにイネーブル化すると、各ポートを設定しないかぎり、スイッチは DHCP 要求をドロップするためです。

DHCP スヌーピングをグローバルにイネーブル化するには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `Router(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 2 | `Router(config)# do show ip dhcp snooping \| include Switch` | 設定を確認します。 |

次に、DHCP スヌーピングをグローバルにイネーブル化する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# do show ip dhcp snooping | include Switch
Switch DHCP snooping is enabled
Router(config)#
```

（注）　DHCP スヌーピングがディセーブルで、DAI がイネーブルの場合、スイッチはすべてのホストをシャットダウンします。これは、ARP テーブルのすべての ARP エントリが、存在しない DHCP データベースと照合されるためです。DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用して ARP パケットの許可および拒否を行います。

# DHCP Option 82 データ挿入のイネーブル化

DHCP Option 82 データ挿入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 | `Router(config)# ip dhcp snooping information option` | DHCP Option 82 データ挿入をイネーブルにします。 |
| ステップ 2 | `Router(config)# do show ip dhcp snooping \| include 82` | 設定を確認します。 |

次に、DHCP Option 82 データ挿入をディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is disabled
Router(config)#
```

次に、DHCP Option 82 データ挿入をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is enabled
Router(config)#
```

# 信頼できないポート上の DHCP Option 82 機能のイネーブル化

**（注）** 信頼できないポート上の DHCP Option 82 機能をイネーブルにした場合、スイッチは信頼できないポートで受信された Option 82 情報を含む DHCP パケットをドロップしません。信頼できない装置が接続された集約スイッチでは、**ip dhcp snooping information option allowed-untrusted** コマンドを入力しないでください。

信頼できないポートで Option 82 情報を含む DHCP パケットを受信できるようにするには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `Router(config)# ip dhcp snooping information option allow-untrusted` | （任意）信頼できないポートで Option 82 情報を含む着信 DHCP パケットを受信できるようにします。<br>デフォルト設定は、ディセーブルです。 |
| ステップ 2 | `Router(config)# do show ip dhcp snooping` | 設定を確認します。 |

次に、信頼できないポートの DHCP Option 82 機能をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option allow-untrusted
Router(config)#
```

# DHCP スヌーピングの MAC アドレス検証のイネーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルにすると、信頼できないポートで受信した DHCP パケット内の送信元 MAC アドレスが、クライアント ハードウェア アドレスと一致するかどうかが検証されます。送信元 MAC アドレスはパケットに関連付けられたレイヤ 2 フィールドで、クライアント ハードウェア アドレスは DHCP パケット内のレイヤ 3 フィールドです。

DHCP スヌーピングの MAC アドレス検証をイネーブル化するには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `Router(config)# ip dhcp snooping verify mac-address` | DHCP スヌーピングの MAC アドレス検証をイネーブルにします。 |
| ステップ 2 | `Router(config)# do show ip dhcp snooping \| include hwaddr` | 設定を確認します。 |

次に、DHCP スヌーピングの MAC アドレス検証をディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is disabled
Router(config)#
```

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is enabled
Router(config)#
```

# VLAN 上での DHCP スヌーピングのイネーブル化

デフォルトでは、DHCP スヌーピング機能がすべての VLAN で非アクティブです。この機能は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

VLAN でイネーブルになると、DHCP スヌーピング機能によって MFC3 の VACL テーブル内に 4 つのエントリが作成されます。これらのエントリにより、PFC3 はこの VLAN 上のすべての DHCP メッセージを代行受信し、RP に送信します。DHCP スヌーピング機能は RP 上でソフトウェアに実装されています。

VLAN 上での 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 | `Router(config)# ip dhcp snooping vlan {{vlan_ID [vlan_ID]} \| {vlan_range}` | VLAN または VLAN 範囲に対して DHCP スヌーピングをイネーブルにします。 |
| ステップ 2 | `Router(config)# do show ip dhcp snooping` | 設定を確認します。 |

DHCP スヌーピングは 1 つの VLAN、または特定の VLAN 範囲に対して設定できます。

- 1 つの VLAN で設定するには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲を設定するには、開始 VLAN 番号と終了 VLAN 番号を入力するか、または一組の VLAN 番号をダッシュ（-）でつなげて指定します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10 12
Router(config)#
```

次に、別の方法で VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12
```

次に、別の方法で VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10,11,12
```

次に、VLAN 10 ～ 12、および VLAN 15 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-12,15
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following Interfaces:

Insertion of option 82 is enabled
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
Router#
```

# レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定

レイヤ 2 LAN インターフェイス上で DHCP 信頼状態を設定するには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `Router(config)# interface {type[1] slot/port \| port-channel number}` | 設定するインターフェイスを選択します。<br>（注）　**switchport** コマンドが設定された LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスだけを選択してください。 |
| ステップ 2 | `Router(config-if)# ip dhcp snooping trust` | インターフェイスを trusted として設定します。 |
| ステップ 3 | `Router(config-if)# do show ip dhcp snooping \| begin pps` | 設定を確認します。 |

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                      Trusted     Rate limit (pps)
------------------------       -------     ----------------
FastEthernet5/12               yes         unlimited
Router#
```

次に、ポート FastEthernet 5/12 を信頼できないポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                      Trusted     Rate limit (pps)
------------------------       -------     ----------------
FastEthernet5/12               no          unlimited
Router#
```

# スプリアス DHCP サーバ検出の設定

スプリアス DHCP サーバを検出するには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `Router(config)# ip dhcp snooping detect spurious vlan range` | 指定した VLAN 範囲でスプリアス DHCP サーバの検出をイネーブルにします。 |
| ステップ 2 | `Router(config)# ip dhcp snooping detect spurious interval time` | 間隔を設定します。デフォルトは 30 分です。 |
| ステップ 3 | `Router# show ip dhcp snooping detect spurious` | スプリアス DHCP サーバ検出を確認します。 |

次の例では、VLAN 20 ～ 25 で DHCP スプリアス サーバ検出を設定し、間隔を 50 分に設定する方法を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping detect spurious vlan 20-25
```

```
Router(config)# ip dhcp snooping detect spurious interval 50
Router# do show ip dhcp snooping detect spurious
Spurious DHCP server detection is enabled.

Detection VLAN list : 20-25
Detection interval : 50 minutes
Router#
```

# レイヤ 2 LAN インターフェイスでの DHCP スヌーピング レート制限の設定

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定するには、次の作業を行います。

| | コマンド | 目的 |
|---|---|---|
| **ステップ 1** | `Router(config)# interface {`*type*[1] *slot/port* \| **port-channel** *number*`}` | 設定するインターフェイスを選択します。<br>**（注）** **switchport** コマンドが設定された LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスだけを選択してください。 |
| **ステップ 2** | `Router(config-if)# ip dhcp snooping limit rate` *rate* | DHCP パケットのレート制限を設定します。 |
| **ステップ 3** | `Router(config-if)# do show ip dhcp snooping \| begin pps` | 設定を確認します。 |

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定する場合は、次の点に注意してください。

- 信頼できないインターフェイスでのレートは、100 pps（パケット/秒）以下に制限することを推奨します。
- 信頼できるインターフェイスにレート制限を設定する場合は、DHCP スヌーピングをイネーブルにしている VLAN を複数収容するトランク ポートでは、レート制限を高い値に設定することを推奨します。
- DHCP スヌーピングでは、レート制限を超過したポートは errdisable ステートとなります。

次の例は、ポート FastEthernet 5/12 を、DHCP パケットのレート制限によって 100 pps に制限する方法を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# ip dhcp snooping limit rate 100
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
FastEthernet5/12           no          100
Router#
```

# DHCP スヌーピング データベース エージェントの設定

DHCP スヌーピング データベース エージェントを設定するには、次の 1 つ以上の作業を行ってください。

| コマンド | 目的 |
|---|---|
| Router(config)# **ip dhcp snooping database** { *_url* \| **write-delay** *seconds* \| **timeout** *seconds* } | 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。 |
| Router# **show ip dhcp snooping database** [**detail**] | 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。 |
| Router# **clear ip dhcp snooping database statistics** | 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。 |
| Router# **renew ip dhcp snooping database** [**validation none**] [*url*] | 指定の URL にあるファイルからのエントリの読み取りを要求します。 |
| Router# **ip dhcp snooping binding** *mac_address* **vlan** *vlan_ID ip_address* **interface** *ifname* **expiry** *lease_in_seconds* | バインディングをスヌーピング データベースに追加します。 |

DHCP スヌーピング データベース エージェントを設定する場合は、次の点に注意してください。

- DHCP スヌーピング データベースには少なくとも 8,000 バインディングが格納されます。
- スイッチの記憶装置の記憶領域が消費されることを避けるため、ファイルは TFTP（簡易ファイル転送プロトコル）サーバ上に保存します。
- スイッチオーバーが発生した場合、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保存されていれば、新たにアクティブになったスーパーバイザ エンジンはこのバインディング リストを使用できます。
- ネットワークベースの URL（TFTP、FTP（簡易転送プロトコル）など）では、スイッチが一連のバインディングを初めて書き込む前に、設定した URL に空のファイルを作成しておく必要があります。

# データベース エージェントの設定例

ここでは、データベース エージェントの設定例を紹介します。

- 「例 1：データベース エージェントのイネーブル化」（P.48-17）
- 「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」（P.48-18）
- 「例 3：DHCP スヌーピング データベースへの情報の追加」（P.48-19）

## 例 1：データベース エージェントのイネーブル化

次の例は、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方法を示します。

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

Router#
```

出力結果の最初の 3 行は、設定した URL、および関連するタイマー設定値を表します。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満了するまでに残された時間を表します。

この他の出力結果として、Startup Failures に、スタートアップ時の読み取りまたはファイル作成の試みに失敗した回数が表示されます。

**（注）** TFTP サーバ上に一時ファイルを作成するには、**touch** コマンドを使用して、TFTP サーバのデーモン ディレクトリ内に作成します。一部の UNIX 実装では、ファイルには完全な読み取りおよび書き込みアクセス許可（777）を設定する必要があります。

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。リモート ファイル内のエントリが、スイッチがすでにバインディングを持つ MAC アドレスと VLAN の組み合わせを表す場合は、リモート ファイルの読み取り時にこ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、このような状況によって無視されたバインディングの数を示します。Invalid interfaces カウンタは、読み取りが行われた時点で、エントリが参照するインターフェイスがシステム内にすでに存在しない場合、ルータである場合、または DHCP スヌーピングにおいて信頼できるインターフェイス（存在する場合）である場合に無視されたバインディングの数を示します。Unsupported vlans は、エントリの示す VLAN がシステム上でサポートされないために無視されたエントリの数を示します。Parse failures カウンタは、ファイル内のエントリの意味をスイッチが解析できなかったために無視されたエントリの数を示します。

スイッチは、このように無視されたバインディングに対し、2 種類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。これらのカウンタは、Last ignored bindings counters として表示されます。もう 1 つは Total ignored bindings counters で、スイッチのブートアップ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合計数を示します。これらの 2 種類のカウンタは、**clear** コマンドによって消去されます。合計カウンタのセットには、最後に消去した時点からの無視されたバインディングの累積数が示されていると見なすことができます。

## 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** | `Router# 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** | `Router# renew ip dhcp snoop data` *url* | スイッチに、指定の URL からファイルを読み取るように指示します。 |
| **ステップ 3** | `Router# 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** | `Router# show ip dhcp snoop bind` | バインディングの読み取りが正常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。

```
Router# show 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 Succeeded 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
Router# 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.
```

```
Router#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Router# 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 Succeeded 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
Router#
Router# 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
Router# clear ip dhcp snoop bind
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Router#
```

## 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** | `Router# 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** | `Router# 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** | `Router# show ip dhcp snooping binding` | DHCP スヌーピング データベースをチェックします。 |

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。

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

Router# 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
Router#
```

# バインディング テーブルの表示

個々のスイッチ用の DHCP スヌーピング バインディング テーブルは、信頼できないポートに対応するバインディング エントリを保持します。このテーブルには、信頼できるポートと相互接続するホストについての情報は含まれません。相互接続する各スイッチは、それぞれ独自の 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。

```
Router# 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
```

表 48-2 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 48-2　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、またはスタティック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 |

**ヒント**　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

**ヒント**