CHAPTER 78

Dynamic Host Configuration Protocol（DHCP）スヌーピング

（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、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

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

技術マニュアルのアイデア フォーラムに参加する

DHCP スヌーピングの前提条件

なし。

DHCP スヌーピングの制約事項

DHCP スヌーピング設定時の制約事項

- DHCP スヌーピング データベースには少なくとも 12,000 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、スイッチでは次の 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

  次のコマンドを入力しても、スイッチからはエラー メッセージが返され、設定は適用されません。

DHCP スヌーピング設定時の注意事項

- 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にする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- DHCP サーバの設定については、次の資料を参照してください。

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book.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の両方）が表示されます。

DHCP スヌーピングの最小限の設定

1. DHCP サーバを定義し、設定します。次の資料を参照してください。

   http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book.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。

   デフォルトでは、すべての VLAN で DHCP スヌーピングは非アクティブです。「VLAN 上での DHCP スヌーピングのイネーブル化」（P.78-12）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介して接続されていることを確認します。

   デフォルトでは、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。「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.78-13）を参照してください。

4. DHCP スヌーピング データベース エージェントの設定を設定します。

   この手順では、再起動またはスイッチオーバー後に、データベース エントリがリストアされます。「DHCP スヌーピング データベース エージェント」（P.78-14）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にします。

   この機能は、この手順を完了するまでアクティブになりません。「DHCP スヌーピングのグローバルなイネーブル化」（P.78-9）を参照してください。

DHCP リレーのスイッチを設定する場合、次の追加手順が必要です。

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 クライアントと異なるサブネットにある場合、クライアント側の VLAN のヘルパー アドレス フィールドで、IP アドレスを設定します。

2. 信頼できないポートで DHCP Option 82 を設定します。

   「信頼できないポートの DHCP Option 82 機能のイネーブル化」（P.78-10）を参照してください。

DHCP スヌーピングの概要

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済み DHCP サーバとの間でファイアウォールのような役割を果たすセキュリティ機能です。DHCP スヌーピング機能では、次のアクティビティが実行されます。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- 信頼できるソースおよび信頼できないソースからの DHCP トラフィックのレートを制限する。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

ダイナミック ARP インスペクション（DAI）などの他のセキュリティ機能でも、DHCP スヌーピング バインディング データベースに保存されている情報が使用されます。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。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ルート プロセッサ（RP）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。

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。

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 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 スヌーピング機能では、止められた DHCP メッセージから抽出された情報を使用して、データベースがダイナミックに構築され、維持されます。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

DHCP スヌーピング機能では、スイッチで特定の DHCP メッセージを受信すると、データベースが更新されます。たとえば、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、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切れると、またはホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベース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、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

パケットの検証

スイッチでは、DHCP スヌーピングがイネーブルな VLAN の信頼できないインターフェイス上で受信した DHCP パケットが検証されます。次の条件が発生（この場合パケットは破棄される）しない限り、スイッチでは、DHCP パケットが転送されます。

- スイッチで、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でパケットを受信し、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 スヌーピングの MAC アドレス検証オプションがオンの場合だけ、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を持つ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機能で DHCP Option 82 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。信頼ポートとして集約スイッチに接続されているエッジ スイッチで、ポートを設定します。

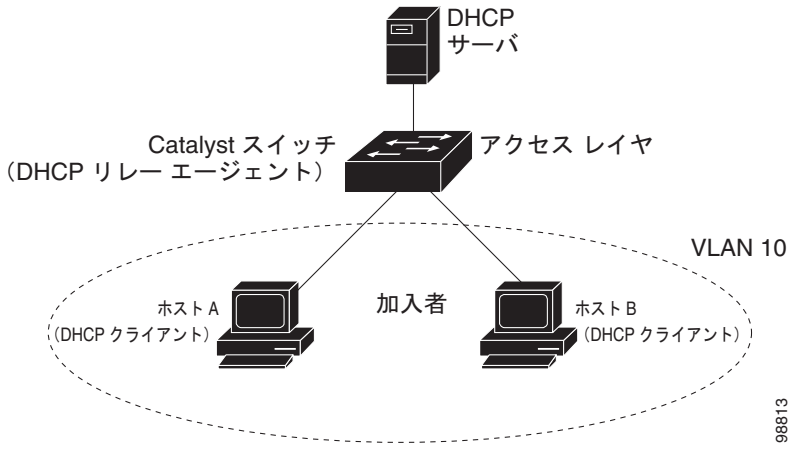
（注）　信頼できないポート機能で DHCP Option 82 がイネーブルである場合は、集約スイッチでダイナミック ARP インスペクションを使用して、信頼できない入力インターフェイスを保護します。

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。

図 78-1 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。各 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 エージェントをヘルパー アドレスによって設定することで、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 78-1　メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



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

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。Option 82 情報には、スイッチの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（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 認証済みユーザ 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 スヌーピングを使用した 802.1X 認証」（P.83-16）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、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、このリモート ID 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実装を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる 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。

- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同じサブネット上にある場合は、サーバはこの応答をブロードキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

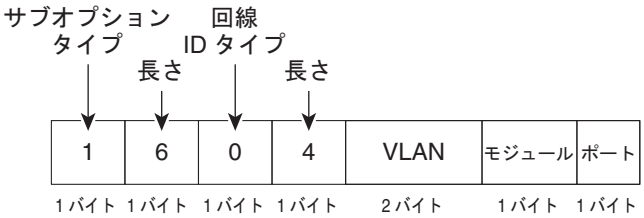
上記の一連のイベントが発生する間、図 78-2 に示す次のフィールドの値は変更されません。

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

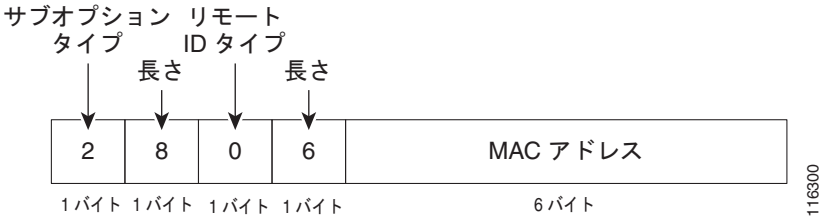
図 78-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力される場合にこれらのパケット形式を使用します。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

図 78-2　　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。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。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、この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、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 （リース時間が期限切れの時刻を示している場合があるため、これは可能です）。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、ファイル内のエントリは無視されます。

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。

DHCP スヌーピングのデフォルト設定

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	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピング 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 スヌーピングを設定する方法

DHCP スヌーピングのグローバルなイネーブル化

（注）　このコマンドは、最後の設定手順として設定してください（または、予定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てください）。これは、DHCP スヌーピングをグローバルにイネーブル化すると、ポートを設定しない限り、スイッチが 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`	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 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の DHCP Option 82 機能のイネーブル化

（注）　信頼できないポートの 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。信頼できないデバイスが接続されている集約スイッチでは、**ip dhcp snooping information option allowed-untrusted** コマンドは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）Option 82 情報が含まれている DHCP の着信パケットを受け付けるよう、信頼できないポートをイネーブル化します。 デフォルト設定では無効になっています。
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 パケット内のクライアント ハードウェア アドレスが、送信元 MAC 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ているレイヤ 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 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、すべての VLAN で DHCP スヌーピング機能は非アクティブです。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 でイネーブル化されている場合、DHCP スヌーピング機能では、MFC3 の VACL テーブルで 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、PFC または DFC 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 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（-）でつなげて入力します。
- 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、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにするもう 1 つの方法を示します。

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

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにするもう 1 つの方法を示します。

```
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 slot/port | port-channel number}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した 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。

次に、ギガビット イーサネット ポート 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 gigabitethernet 5/12
Router(config-if)# ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet5/12             yes          unlimited
Router#
```

次に、ギガビット イーサネット ポート 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 gigabitethernet 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)
------------------------     -------     ----------------
GigabitEthernet5/12             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 slot/port | port-channel number}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した 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。

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、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しなければならない場合があります。
- 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。

次に、ギガビット イーサネット ポート 5/12 を、DHCP パケットのレート制限によって 100 pps に設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 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)
------------------------   -------     ----------------
GigabitEthernet5/12           no           100
Router#
```

DHCP スヌーピング データベース エージェント

- 「DHCP スヌーピング データベース エージェントの前提条件」（P.78-15）
- 「DHCP スヌーピング データベース エージェントの制約事項」（P.78-15）

DHCP スヌーピング データベース エージェントの前提条件

なし。

DHCP スヌーピング データベース エージェントの制約事項

- 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。
- スイッチのストレージ デバイスの記憶域が消費されることを避けるため、ファイルは TFTP 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 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。

DHCP スヌーピング データベース エージェントのデフォルト設定

なし。

DHCP スヌーピング データベース エージェントの設定方法

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 つまたは複数の作業を行います。

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。

データベース エージェントの設定例

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。

```
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経過するまでに残された時間を表します。

出力結果にはこのほか、スタートアップ時の失敗として、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。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。期限切れリース 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。無効なインターフェイス カウンタは、読み取りが行われた時点で、エ

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。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で無視されたバインディングの総数を表します。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*	この 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	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。

```
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

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	`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#
```

DHCP スヌーピング 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。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    GigabitEthernet6/10
```

表 78-1 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 78-1　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 バインディングか、またはスタティックに設定されたバインディングです。
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

技術マニュアルのアイデア フォーラムに参加する