CHAPTER 41

DHCP スヌーピングの設定

この章では、Cisco 7600 シリーズ ルータに 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） DHCP スヌーピング機能には、PFC3 と Release 12.2(18)SXE およびそれ以降のリリースが必要です。PFC2 では、DHCP スヌーピングはサポートされません。

この章で説明する主な内容は、次のとおりです。

（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 にある『Cisco 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

DHCP スヌーピングの概要

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済み DHCP サーバとの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、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する。
- 信頼できる送信元および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、管理する。このデータベースには、リースされた IP アドレスを持つ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後続リクエストを検証する。

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なっています。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、MSFC 上のソフトウェアで実行されます。したがって、イネーブルな VLAN へのすべての DHCP メッセージは、PFC で止められ、処理のために MSFC に送信されます。

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、トラフィックの送信元が信頼できるかどうかを判別します。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、信頼できる送信元です。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。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。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、信頼できないソースです（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 6500 シリーズのスイッチでは、その接続インターフェイスの信頼状態を設定することによって、ソース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、信頼できない状態です。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ルータ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 スヌーピング機能では、DHCP メッセージを傍受して抽出した情報を使用して、データベースを動的に構築して保持します。DHCP スヌーピングがイネーブルになっている 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、リースされた IP アドレスを持つ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 データベース内の各エントリには、ホストの MAC アドレス、リースされた 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。

パケット検証

ルータでは、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。

- ルータで、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。
- ルータ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。
- ルータが、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ある信頼できないホストから DHCPRELEASE メッセージまたは 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。
- ルータが、リレー エージェントの IP アドレス（0.0.0.0 以外）を保持する DHCP パケットを受信した場合。

リリース 12.2(18)SXF1 よりも前のリリースでは、ルータで、信頼できないポートで Option 82 情報を保持する DHCP パケットは破棄されます。リリース 12.2(18)SXF1 およびそれ以降のリリースで、信頼できない収集ルータ ポートに接続されている信頼エッジ ルータをサポートする場合、信頼できないポート機能で DHCP Option 82 をイネーブルにできます。これによって、信頼できない集約ルータ ポートでは、Option 82 情報が保存されている DHCP パケットを受信します。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 ルータで、ポートを設定します。

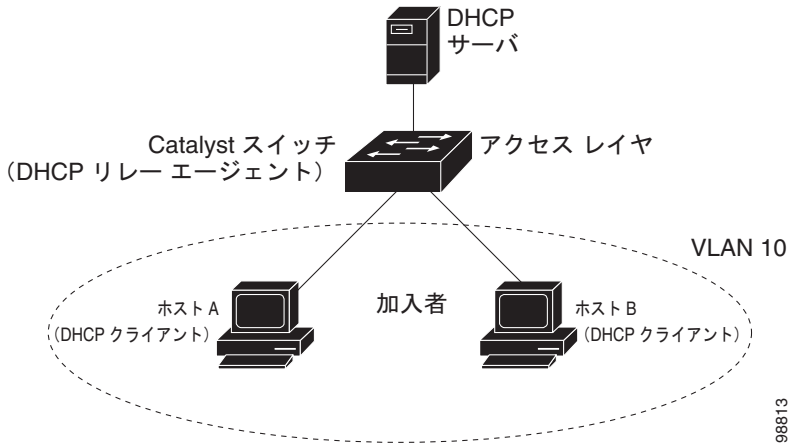
（注） 信頼できないポート機能で DHCP Option 82 がイネーブルである場合は、集約ルータでダイナミック ARP インスペクションを使用して、信頼できない入力インターフェイスを保護します。

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。ルータで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者デバイスは MAC アドレスだけでなく、このデバイスをネットワークに接続するルータ 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 ルータ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 41-1 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 レイヤのルータ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 41-1　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



ルータに対して DHCP スヌーピング情報の Option 82 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。
- ルータはこの 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、ルータの 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。
- 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、ルータは DHCP パケット内にこの IP アドレスを追加します。
- ルータは、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。
- 要求がルータによってサーバにリレーされている場合は、DHCP サーバは応答をルータ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。ルータはリモート 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、最初に Option 82 データが挿入されていることを確認します。ルータは 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ルータ ポートにパケットを転送します。

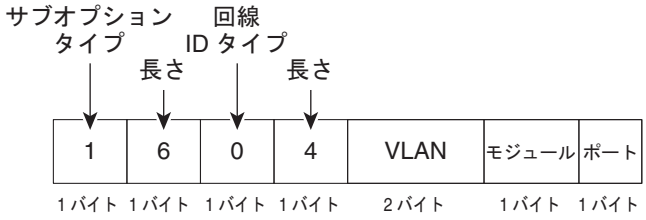
上記の一連のイベントが発生する間、図 41-2 に示す次のフィールドの値は変更されません。

- 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

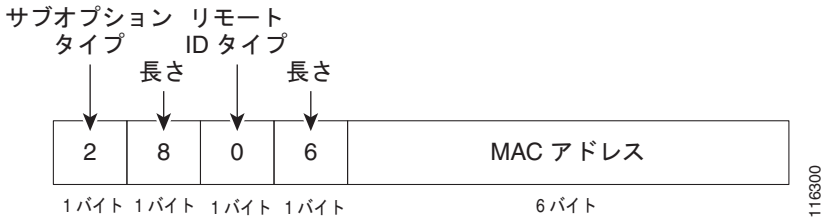
図 41-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。ルータがこれらのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化されている場合、および **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合です。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

図 41-2　　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。ルータ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。ルータ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エントリを以前の書き込みに関連するエントリと区別するのに役立ちます。

次に、バインディング ファイルの例を示します。

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

各エントリは、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保持します。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ています。

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、ルータ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、ルータは、リース期間が期限切れになったファイルのすべてのエントリも無視します。（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、この可能性があります）。エントリ内で参照されるインターフェイスが、システム上に存在しなくなった場合、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が無視されます。

ルータ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、ルータは変更されたエントリのセットをスヌーピング データベースから抽出し、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 41-1 に、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 41-1　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 スヌーピング設定時の制約事項および注意事項

ここでは、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、次の制約事項に注意してください。

- PFC2 では、DHCP スヌーピングはサポートされません。
- リリース 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースで、最大 512 のバインディングが保存されます。512 を超える DHCP バインディングを追加する場合、すべてのバインディングがデータベースから削除されます。
- リリース 12.2(18)SXF5 とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 8,000 のバインディングが保存されます。
- リリース 12.2(18)SRA とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 64,000 のバインディングが保存されます。

DHCP スヌーピング設定時の注意事項

DHCP の設定時には、次の注意事項に従ってください。

- DHCP スヌーピングは、この機能を少なくとも 1 つの VLAN 上でオンにし、ルータ上でグローバルにオンにするまで、アクティブになりません。サービス DHCP がイネーブルであることを確認してください（サービス DHCP はデフォルトでイネーブルに設定されています）。
- ルータ上で DHCP スヌーピングをグローバルにイネーブル化する前に、DHCP サーバおよび DHCP リレー エージェントとして機能するデバイス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 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/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm
- 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なっているすべての 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設定

DHCP スヌーピング機能の最小限の設定手順は、次のとおりです。

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 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/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

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.41-12）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.41-14）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 エントリが復元されます。「DHCP スヌーピング データベース エージェントの設定」（P.41-15）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.41-10）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、サーバ 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.41-11）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）　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、ルータが 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。
	`Router(config)# no ip dhcp snooping`	DHCP スヌーピングをディセーブルにします。
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)#
```

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。
	`Router(config)# no ip dhcp snooping information option`	DHCP Option 82 データ挿入をディセーブルにします。
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、ルータ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ルータでは、**ip dhcp snooping information option allowed-untrusted** コマンドは入力しないでください。

リリース 12.2(18)SXF1 およびそれ以降のリリースで、Option 82 情報が含まれている DHCP 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するには、次のタスクを実行します。

	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。 デフォルト設定はディセーブルです。
	`Router(config)# no ip dhcp snooping information option allow-untrusted`	信頼できないポートの DHCP Option 82 機能のディセーブル化
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 フィールドであり、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。
	`Router(config)# no ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をディセーブルにします。
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、PFC3 では、この VLAN 上のすべての DHCP メッセージが止められ、MSFC に送信されます。DHCP スヌーピング機能は、MSFC ソフトウェアで実行されます。

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。
	`Router(config)# no ip dhcp snooping`	DHCP スヌーピングをディセーブルにします。
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[1] 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` `Router(config-if)# no ip dhcp snooping trust`	インターフェイスを trusted として設定します。 デフォルトの（untrusted）状態に戻します。
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* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト 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 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、ファスト 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 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#
```

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。 （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。

	コマンド	目的
ステップ 3	`Router(config-if)# no ip dhcp snooping limit rate`	DHCP パケットのレート制限をディセーブルにします。
ステップ 4	`Router(config-if)# do show ip dhcp snooping | begin pps`	設定を確認します。

1. *type* = **ethernet**、**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、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 スヌーピングがイネーブルになっている 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、ファスト 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 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、次の作業の 1 つまたは複数を実行します。

コマンド	目的
`Router(config)# ip dhcp snooping database { _url | write-delay seconds | timeout seconds }`	（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。
`Router(config)# no ip dhcp snooping database [write-delay | timeout]`	設定を消去します。
`Router# 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。
`Router# 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。
`Router# 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。
`Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds`	（任意）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。
`Router# no ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname`	（任意）スヌーピング データベースからバインディングを削除します。

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、次の点に注意してください。

- リリース 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースで、最大 512 のバインディングが保存されます。512 を超える DHCP バインディングを追加する場合、すべてのバインディングがデータベースから削除されます。
- リリース 12.2(18)SXF5 とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 8,000 のバインディングが保存されます。
- ルータのストレージ 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、FTP など）では、ルータ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.41-16）
- 「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.41-17）
- 「例 3：DHCP スヌーピング データベースへの情報の追加」（P.41-19）

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 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

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。

この他の統計情報として出力結果で示されるスタートアップ時の失敗は、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を表します。

（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、ルータ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。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。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。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、ルータ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。

ルータは、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」であり、ルータの起動時からのすべての読み取りによって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** コマンドによってクリアされます。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	`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*	ルータに、指定の URL からファイルを読み取るように指示します。

	コマンド	目的
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 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
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 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
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

個々のルータが持つ 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。相互接続する各ルータは、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、ルータの 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 41-2 に、**show ip dhcp snooping binding** コマンド出力のフィールドの説明を示します。

表 41-2　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

表 41-2　show ip dhcp snooping binding コマンドの出力結果 （続き）

フィールド	説明
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