CHAPTER 32

DHCP スヌーピングおよび IP ソース ガードの設定

この章では、Catalyst 6500 シリーズ スイッチで Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）スヌーピングおよびソース ガードを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

（注） この章で使用しているスイッチ コマンドの完全構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。また、次の関連資料も参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/cmd_ref/index.htm

DHCP スヌーピングの機能概要

DHCP スヌーピングは、DHCP パケットをフィルタリングし、DHCP スヌーピング バインディング テーブルを作成し維持することにより、DHCP メッセージを使用して開始された DoS 攻撃に対するセキュリティを提供します。DHCP スヌーピングは、trusted（信頼性のある）および untrusted（信頼性のない）ポートの両方を使用します。

trusted ポートから受信した DHCP パケットは、検証なしで転送されます。一般的に、trusted ポートは DHCP サーバまたはリレー エージェントに到達するのに使用します。スイッチが untrusted ポートから DHCP パケットを受信すると、DHCP スヌーピングは、クライアントからの DHCP パケットのみが許可されて、情報のスヌーピングが実行されていないことを確認します。

DHCP スヌーピング バインディング テーブルには、スイッチの untrusted ポート上にある DHCP クライアントに関する MAC（メディア アクセス制御）アドレス、IP アドレス、リース期間（秒）、および VLAN（仮想 LAN）ポート情報が含まれています。DHCP スヌーピング バインディング テーブルに含まれる情報は、リース期間が終了するか DHCP スヌーピングが VLAN でディセーブルになると、バインディング テーブルから削除されます。

これらの DHCP メッセージは、DHCP バインディング テーブルを作成するのに使用します。

- DHCPACK ― バインディング エントリがない場合、新しいダイナミック DHCP バインディング エントリを追加します。
- DHCPNAK ― 既存の DHCP バインディング エントリを削除します。
- DHCPRELEASE ― バインディング エントリがある場合にダイナミック DHCP エントリを削除します。
- DHCPDECLINE ― バインディング エントリがある場合にダイナミック DHCP バインディング エントリを削除します。

各スイッチでは、ローカルの untrusted ポートだけに対する DHCP スヌーピング バインディング テーブルを保持しています。テーブルには、他のスイッチに直接接続されているホストの DHCP スヌーピング バインディング テーブルに関する情報は格納されず、trusted ポート経由で接続されているホストの情報も含まれていません。trusted ポートには、リレー エージェントまたは DHCP サーバなどの直接接続されているエンティティや、そのようなエンティティへの転送パスがあります。リレー エージェントまたは DHCP サーバへのパスは、信頼されている必要があります。

DHCP スヌーピング設定時の注意事項

ここでは、ネットワークに DHCP を設定する際の注意事項について説明します。

- DHCP　スヌーピングをイネーブルにしてハイ　アベイラビリティではないスイッチオーバーを実行した場合、DHCP スヌーピング バインディング テーブルの内容が消失します。この設定を使用することは推奨しません。
- DHCP スヌーピングは、Policy Feature Card（PFC; ポリシー フィーチャ カード）およびこれ以降のバージョンでサポートされます。
- DHCP スヌーピング バインディング テーブルは、16,384 エントリに制限されています。制限に到達すると、古いエントリがリース期間に到達するまで新しいエントリを追加できません。
- 802.1X-DHCP および DHCP スヌーピングは相互に排他的です。802.1X-DHCP と DHCP スヌーピングの両方に VLAN を設定できません。Access Control List（ACL; アクセス制御リスト）に 802.1X および DHCP スヌーピングの両方を設定した場合、ACL 内で高い位置にいる方がもう一方の機能を上書きします。
- Dynamic ARP Inspection（DAI）、DHCP スヌーピング、および IP ソース ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。設定の詳細については、「ダイナミック ARP 検査」（p.15-40）を参照してください。

VLAN での DHCP スヌーピングの設定

一般的に、DHCP スヌーピングは、配線クローゼットなどのアクセスレベル ネットワークで使用されます。VLAN で DHCP スヌーピングをイネーブルにするには、その VLAN 上の DHCP クライアントに対する IP アドレスと MAC アドレスとのバインディング テーブルを作成します。

（注）　管理 VLAN sc0 および sc1 で DHCP をイネーブルにできません。

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

デフォルトでは、DHCP スヌーピングはディセーブルに設定されています。表 32-1 に、各 DHCP スヌーピング オプションのデフォルト設定値を示します。デフォルトの設定値を変更したい場合、「DHCP スヌーピングのイネーブル化」（p.32-4）を参照してください。

表 32-1　DHCP スヌーピングのデフォルト設定値

オプション	デフォルト値 / ステート
DHCP スヌーピング ホストのトラッキング情報オプション	ディセーブル
DHCP スヌーピング制限レート	Address Resolution Protocol（ARP; アドレス解決プロトコル）検査および 802.1X-DHCP で 1000 pps を共有します。レート制限は、PFC2 およびこれ以降のバージョンでサポートされます。
ポートでの DHCP スヌーピングの信頼	信頼しない
VLAN での DHCP スヌーピング	ディセーブル
DHCP スヌーピング バインディング データベースの自動保存オプション	ディセーブル
DHCP スヌーピング バインディング データベースのストレージ デバイスおよびファイル名	bootflash：dhcp-snooping-binding-database

DHCP スヌーピングのイネーブル化

DHCP スヌーピングは、セキュリティ VLAN ACL（VACL）を介して VLAN でイネーブルになっています。DHCP スヌーピング Access Control Entry（ACE; アクセス制御エントリ）を新規または既存のセキュリティ ACL に追加することにより、DHCP スヌーピングは VLAN でイネーブルに設定します。DHCP パケットのポリシーにしたがって、ACL 内の DHCP スヌーピングの位置を決定する必要があります。たとえば、特定のホストから DHCP パケットを拒否して他の DHCP パケットに対して DHCP スヌーピングを実行したい場合、DHCP スヌーピング ACE の前に拒否 ACE を配置する必要があります。

VLAN 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。

	作業	コマンド
ステップ 1	VACL に DHCP スヌーピングを追加します。	**set security acl ip** *acl_name* **permit dhcp-snooping**
ステップ 2	すべてのホストからの DHCP スヌーピングを許可するように VACL を設定します。	**set security acl ip** *acl_name* **permit ip any any**
ステップ 3	VACL を保存します。	**commit security acl** *acl_name*
ステップ 4	ACL を VLAN に追加します。	**set security acl map** *acl_name* **10**

次に、VLAN 上で DHCP スヌーピングを設定する例を示します。

```
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.
Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console> (enable)
```

（注）　DHCP スヌーピングをイネーブルにするためだけに VACL を作成する場合、VACL にはリストの最後に暗黙の拒否があり、他のパケットは暗黙の許可がないかぎり許可されません。

（注）　802.1X-DHCP および DHCP スヌーピングは相互に排他的です。VLAN に両方の機能を設定しないでください。

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライマリおよびセカンダリ（隔離またはコミュニティ）Private VLAN（PVLAN; プライベート VLAN）で別々に 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 バインディング テーブルには、プライマリ VLAN のバインディング情報のみが含まれていてセカンダリ VLAN の情報は含まれていません。DHCP スヌーピングを PVLAN でイネーブルにしてセカンダリ VLAN でイネーブルにしない場合、パケットは PVLAN で確認されていても、DHCP スヌーピング バインディング テーブル エントリは追加されません。

DHCP スヌーピング ホスト トラッキング情報オプションのイネーブル化

ホスト トラッキング情報オプションをイネーブルにする場合、DHCP リレー エージェント情報オプション（オプション 82）が転送されるクライアント パケットに追加されます。リレー エージェント オプションにはエージェント回線 ID およびエージェント リモート ID 情報が含まれています。回線 ID サブオプションには、クライアントのポートおよび VLAN 番号が含まれています。リモート ID サブオプションにはスイッチの MAC アドレスが含まれています。ホストトラッキング情報を挿入する前に、スイッチは DHCP メッセージに既存のリレー情報オプションやゼロ以外の giaddr フィールドがないことを確認します。ホストトラッキング情報を削除する前に、スイッチは、DHCP 応答メッセージが trusted ポートからのもので、リモート ID とローカル スイッチの MAC アドレスが一致することを確認します。パケットが trusted ポートからきたものでアドレスが一致しない場合、パケットは転送されます。

DHCP スヌーピングのホストトラッキング情報オプションを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	DHCP スヌーピング ホストのトラッキング情報オプションをイネーブルにします。	**set dhcp-snooping information host-tracking enable**
ステップ 2	ホストトラッキング情報オプションの MAC アドレスを表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピング ホストトラッキング情報オプションを設定する例を示します。

```
Console> (enable) set dhcp-snooping information host-tracking enable
DHCP Snooping Information Option Enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)
```

DHCP スヌーピングの MAC アドレス一致オプションのイネーブル化

MAC アドレス一致オプションをイネーブルにする場合、イーサネット ヘッダーの送信元 MAC アドレスが、untrusted ポートからくる DHCP パケットの DHCP ペイロードにある chaddr フィールドと一致します。一致しない場合、パケットは廃棄されて untrusted ポートで廃棄されたパケットのカウンタが増加します。この機能は、デフォルトではイネーブルです。

DHCP スヌーピングの MAC アドレス一致オプションを設定するには、次の作業を行います。

	作業	コマンド
ステップ 1	DHCP スヌーピングの MAC アドレス一致オプションをイネーブルにします。	**set dhcp-snooping match-mac enable**
ステップ 2	DHCP スヌーピング設定を表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピングの MAC アドレス一致オプションを設定する例を示します。

```
Console> (enable) set dhcp-snooping match-mac enable
DHCP Snooping MAC address matching enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)
```

DHCP スヌーピングの設定例

これらの設定例は、DHCP スヌーピングをイネーブルにする例を示したものです。

例 1：DHCP スヌーピングのイネーブル化

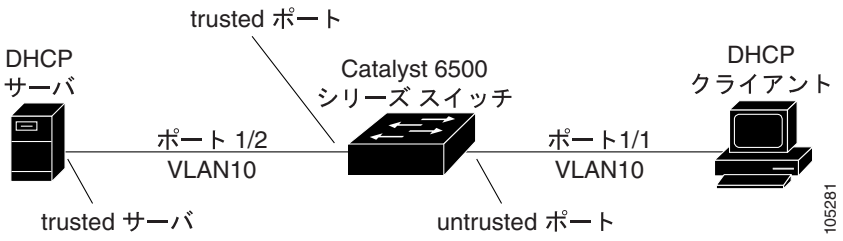
次に、DHCP サーバがポート 1/2 にある VLAN 10 の DHCP スヌーピングをイネーブルにする例を示します。

```
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.
Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s)  1/2 state set to trusted for DHCP Snooping.
Console> show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> show port dhcp-snooping 1/1-2
Port      Trust
----      ------
1/1     untrusted
1/2     trusted
Console> (enable)
```

（注）　DHCP スヌーピングをイネーブルにしたあとに DHCP スヌーピング ホスト トラッキングを設定したい場合、**set dhcp-snooping information-option host-tracking** コマンドを入力します。

図 32-1 に、クライアント / サーバ ネットワークに DHCP スヌーピングを設定するのに使用する一般的なトポロジーを示します。

図 32-1　クライアントおよびサーバ用に設定された DHCP スヌーピング



例 2：MSFC を DHCP リレー エージェントとして使用した DHCP スヌーピングのイネーブル化

次に、DHCP ホスト トラッキングをイネーブルにして Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）をリレー エージェントとして設定する例を示します。

（注）　この例では、クライアントは信頼性がなく、MSFC をリレー エージェントとするスイッチにアクセスします。MFSC リレー エージェント スイッチは、信頼できるトランク ポートを介して MSFC DHCP サーバ スイッチに接続します。

次に、MFSC を DHCP リレー エージェントとして設定する例を示します。

```
service dhcp
on int vlan 810
    ip address 192.168.80.241 255.255.255.0
    ip helper-address 192.168.94.247
    ip dhcp relay information trusted
on int vlan 4094
    ip address 192.168.94.241 255.255.255.0
```

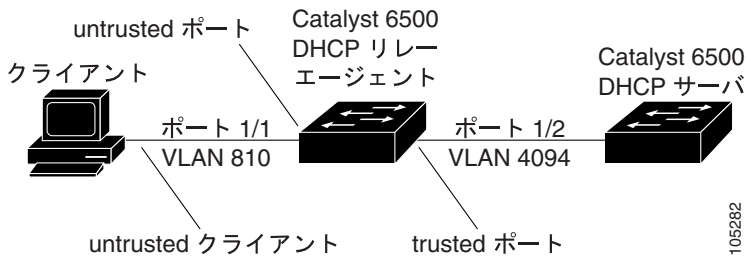
次に、MFSC を DHCP サーバとして設定する例を示します。

```
service dhcp
ip dhcp excluded-address 192.168.80.241
!
ip dhcp pool net810
   network 192.168.80.0 255.255.255.0
on int vlan 4094
   ip address 192.168.94.247 255.255.255.0
```

（注）　MSFC ポートは、DHCP スヌーピングの trusted ポートとしてシステムに設定されています。

図 32-2 に、MSFC をリレー エージェントとして設定した場合の一般的なトポロジーを示します。

図 32-2　リレー エージェントとしての MSFC



DHCP スヌーピング情報の表示

ここにあるコマンドを使用して DHCP スヌーピング バインディング テーブルと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、untrusted ポートに対応するバインディング エントリがあります。各相互接続スイッチには独自のバインディング テーブルがあるため、このテーブルには trusted ポートと相互接続しているホストに関する情報はありません。

作業	コマンド
DHCP スヌーピング バインディング テーブル情報を表示します。	**show dhcp-snooping bindings**

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。

```
Console# show dhcp-snooping bindings
MacAddress          IpAddress        Lease(sec)     VLAN  Port
------------------  ---------------  ----------     ----  -----

00-01-7b-9b-05-3f   192.168.80.221   86377          810   1/8
```

表 32-2 に、**show dhcp-snooping binding** コマンドの出力に含まれるフィールドを説明します。

表 32-2　show dhcp-snooping bindings コマンド出力

フィールド	説明
MAC Address	クライアントのハードウェア 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の IP アドレス
Lease (seconds)	IP アドレス リース期間
VLAN	クライアント ポートの VLAN 番号
Port	DHCP クライアント ホストに接続しているポート

DHCP スヌーピング設定と統計情報の表示

作業	コマンド
スイッチの DHCP スヌーピング設定を表示します。	**show dhcp-snooping config**

次に、DHCP スヌーピング ホスト トラッキングおよび一致 MAC 設定を表示する例を示します。

```
Console# show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console#
```

作業	コマンド
スイッチの DHCP スヌーピング統計情報を表示します。	**show dhcp-snooping statistics**

次に、スイッチの DHCP スヌーピング統計情報を表示する例を示します。

```
Console# show dhcp-snooping statistics
Packets forwarded                             =          125
Packets dropped                               =          3
Packets dropped from untrusted ports          =          0
Number of bindings entries                    =          5
Console#
```

作業	コマンド
スイッチの DHCP スヌーピング ポート設定を表示します。	**show port dhcp-snooping**

次に、スイッチの DHCP スヌーピング ポート設定を表示する例を示します。

```
Console# show port dhcp-snooping
Port     Trust
-----  -----------
 3/1   untrusted
 3/2   trusted
 3/3   untrusted
 3/4   trusted
 3/5   trusted
 3/6   untrusted
 3/7   untrusted
 3/8   untrusted
(テキスト出力は省略)
 3/31  untrusted
 3/32  untrusted
 3/33  untrusted
 3/34  untrusted
 3/35  untrusted
 3/36  untrusted
 3/37  untrusted
 3/38  untrusted
 3/39  untrusted
 3/40  untrusted
 3/41  trusted
 3/42  trusted
 3/43  trusted
 3/44  untrusted
 3/45  untrusted
 3/46  untrusted
 3/47  untrusted
 3/48  untrusted
Console>
```

フラッシュ デバイスへの DHCP スヌーピング バインディング エントリの保存

DHCP スヌーピング バインディング エントリは、フラッシュ デバイスに保存できるため、スイッチの再設定後すぐにバインディングを復元できます。

auto-save *interval* オプションは、DHCP スヌーピング バインディングの自動保存インターバルの設定用です。インターバルの有効範囲は、1 ～ 35000（分）です。0 を指定すると、フラッシュ デバイスへのバインディングの定期的保存がディセーブルとなり、フラッシュに保存されているバインディング ファイルが削除されます。0 を指定しても、ユーザが指定したファイル名は消去されません。ユーザが指定したファイル名は、**clear config all** コマンドを入力すると、消去され、デフォルトのファイル名に戻ります。

device:filename オプションは、バインディングを保存するフラッシュ デバイスおよびファイル名の指定用です。デフォルトでは、フラッシュ デバイスは bootflash で、デフォルト ファイル名は、[dhcp-snooping-bindings-database] です。ファイル名が設定されていない場合、バインディングはフラッシュ デバイスにデフォルト ファイル名で自動的に保存されます。

DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを指定します。	**set dhcp-snooping bindings-database auto-save** *interval*

次に、DHCP スヌーピング バインディング エントリの **auto-save** オプションをイネーブルにして、バインディングを定期的に保存するインターバルを 600 分に指定する例を示します。

```
Console> (enable) set dhcp-snooping bindings-database auto-save 600
DHCP Snooping auto-save interval set to 600 minutes.
Console> (enable)
```

バインディング保存用のフラッシュ デバイスおよびファイル名を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
バインディング保存用のフラッシュ デバイスおよびファイル名を指定します。	**set dhcp-snooping bindings-database** *device:*[*filename*]

次に、バインディング保存用のフラッシュ デバイスおよびファイル名を設定する例を示します。

```
Console> (enable) set dhcp-snooping bindings-database disk1:dhcp-bindings
DHCP Snooping bindings storage file set to disk1:dhcp-bindings.
Console> (enable)
```

次に、DHCP スヌーピング バインディング データベースの設定を表示する例を示します。

```
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-01-64-41-60-ff.
DHCP Snooping auto save interval is 600.
DHCP Snooping bindings storage file is disk1:dhcp-bindings.
Console> (enable)
```

IP ソース ガードの機能概要

IP ソース ガードは、特定のポートの DHCP スヌーピングを介して取得した IP アドレスのみを許可することで、IP スプーフィングを回避します。最初に、DHCP スヌーピングでキャプチャされた DHCP パケットを除く、ポート上のすべての IP トラフィックがブロックされます。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、Port Access Control List（PACL; ポートアクセス制御リスト）がその IP アドレスからのトラフィックを許可するポートにインストールされます。このプロセスでは、クライアント IP トラフィックを、DHCP サーバから取得した送信元 IP アドレスに制限します。PACL 許可リストにない送信元 IP アドレスを持つ IP トラフィックはフィルタリングで除外されます。このフィルタリングによって、隣接ホストの IP アドレスを要求することによるホストのネットワーク攻撃能力を制限できます。

（注）　DHCP スヌーピングをイネーブルにしている VLAN が大量にあるトランク ポートで、IP ソース ガードをイネーブルにする場合、ACL ハードウェア リソースが不足し、そのポートに接続しているクライアントがトラフィックを送信できなくなる可能性があります。ポートごとに 10 個の IP アドレスに制限されているため、このような設定は推奨しません。

IP ソース ガードは、送信元 IP アドレス フィルタリングを使用します。これは、その送信元 IP アドレスに基づいた IP トラフィックをフィルタリングするものです。IP 送信元バインディング エントリと一致する送信元 IP アドレスがある IP トラフィックのみが許可されます。

ポートの新しい DHCP スヌーピング バンディング エントリが作成されたり削除されたりする際に、ポートの 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させるために、ポート PACL がハードウェアで変更されて再び適用されます。デフォルトで、ポートで DHCP スヌーピング バインディングなしで IP ソース ガードをイネーブルにする場合、すべての IP トラフィックを拒否するデフォルトの PACL がポートにインストールされます。IP ソース ガードをディセーブルにする場合、IP 送信元フィルタ PACL がポートから削除されます。

IP ソース ガードの設定時の注意事項

ここでは、ネットワークで IP ソース ガードを設定する際の注意事項について説明します。

- IP ソース ガードは、PFC3 およびこれ以降のバージョンでサポートされます。
- ポートごとに 10 個の IP アドレスに制限されています。
- IP ソース ガードはトランク ポートでは推奨しません。
- IP ソース ガードは、PACL と共存できません。
- IP ソース ガードは、EtherChannel 対応ポートでサポートされていません。また EtherChannel は IP ソース ガード対応ポートではサポートされていません。
- IP ソース ガードをイネーブルにすると、スタティック ARP 検査などの VLAN ベースの ACL 機能はディセーブルになります。
- DAI、DHCP スヌーピング、および IP ソース ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。設定の詳細については、「ダイナミック ARP 検査」(p.15-40)を参照してください。

ポートでの IP ソース ガードのイネーブル化

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。

	作業	コマンド
ステップ 1	ポートをポート ベースに設定します。	**set port security-acl 3/1 port-based**
ステップ 2	IP ソース ガードをイネーブルにします。	**set port dhcp-snooping 3/1 source-guard enable**
ステップ 3	DHCP スヌーピングをイネーブルにします。	**set security acl ip dhcpsnoop permit dhcp-snooping**
ステップ 4	ポートで他のトラフィックの転送を許可します。	**set security acl ip dhcpsnoop permit ip any any**
ステップ 5	ACL 設定を保存します。	**commit security acl dhcpsnoop**
ステップ 6	VLAN で ACL をイネーブルにします。	**set security acl map dhcpsnoop 10**
ステップ 7	ポートでの DHCP スヌーピングの信頼をイネーブルにします。	**set port dhcp-snooping 1/2 trust enable**

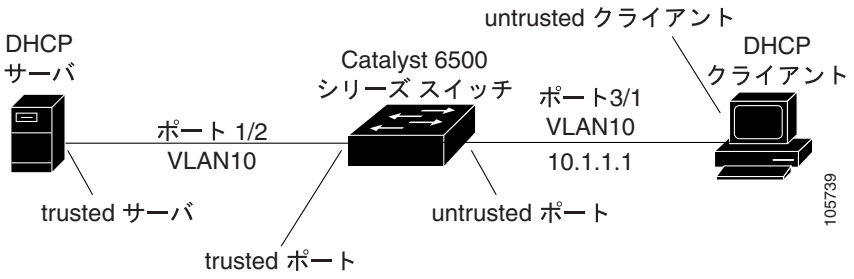
（注）　IP ソース ガードをイネーブルにする前に、ポートが属する VLAN の DHCP スヌーピングをイネーブルにする必要があります。ポートをセキュリティ ACL のポート ベースまたはマージ モードに設定する必要があります。DHCP スヌーピング untrusted ポートでのみ IP ソース ガードをイネーブルにします。

次に、IP ソース ガードをイネーブルにする例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
Warning:Vlan-based ACL features will be disabled on port 3/1.
ACL interface is set to port-based mode for port(s) 3/1.
Console> (enable) set port dhcp-snooping 3/1 source-guard enable
IP Source Guard enabled on port(s)  3/1.

Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s)  1/2 state set to trusted for DHCP Snooping.
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
 save changes.

Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console>
```

図 32-3 に、untrusted ポートで IP ソース ガードを設定する場合の一般的なトポロジーを示します。

図 32-3　untrusted ポートでイネーブルな IP ソース ガード



IP ソース ガード情報の表示

show port dhcp-snooping コマンドを使用して、スイッチ上のすべてのポートの IP ソース ガード情報を表示できます。モジュールで IP ソース ガードの情報を表示するには、次の作業を行います。

作業	コマンド
ポートで IP ソース ガードに関する情報を表示します。	**show port dhcp-snooping 4**

次に、ポートで IP ソース ガードの設定を表示する例を示します。

```
Console> (enable) show port dhcp-snooping 3/25
Port     Trust      Source-Guard    Source-Guarded IP Addresses
-------- ---------- --------------  ---------------------------
 3/25    untrusted      enabled     192.168.80.6, 192.168.80.5,
                                    192.168.80.4, 192.168.80.3,
                                    192.168.80.2, 192.168.80.1
Console> (enable)
```