



## DHCP 機能の設定

---

この章では、Catalyst 3750 スイッチに、Dynamic Host Configuration Protocol (DHCP) スヌーピング機能および Option 82 データ挿入機能を設定する手順について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注) この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンス、および『*Cisco IOS IP and IP Routing Command Reference*』 Release 12.1 の「*IP Addressing and Services*」を参照してください。

---

この章で説明する内容は、次のとおりです。

- [DHCP 機能の概要 \(p.19-2\)](#)
- [DHCP 機能の設定 \(p.19-4\)](#)
- [DHCP 情報の表示 \(p.19-6\)](#)

## DHCP 機能の概要

DHCP は、中央のサーバからホストの IP アドレスをダイナミックに割り当てるために、LAN 環境で広範囲に使用されています。この機能により、IP アドレス管理のオーバーヘッドを著しく軽減することができます。また、DHCP により、IP アドレスをホストに永続的に割り当てる必要がなくなり、ネットワークに接続しているホストだけが IP アドレスを使用するので、制限された IP アドレススペースの節約に役立ちます。

## DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングおよび DHCP スヌーピングバインディングテーブルの構築および維持により、ネットワークセキュリティを提供する DHCP のセキュリティ機能です。信頼できないメッセージとは、ネットワークまたはファイアウォール外部から受信したメッセージで、ネットワーク内でのトラフィック攻撃の原因となるものを指します。

DHCP スヌーピングバインディングテーブルには、MAC (メディアアクセス制御) アドレス、IP アドレス、リース時間、バインディングタイプ、VLAN 番号、およびスイッチ上の信頼できないローカルインターフェイスに対応するインターフェイス情報が格納されています。信頼できるインターフェイスに相互接続しているホストに関連する情報は格納されていません。信頼できないインターフェイスとは、ネットワークまたはファイアウォール外部からメッセージを受信するように設定されたインターフェイスを指します。信頼できるインターフェイスとは、ネットワーク内からのメッセージのみを受信するように設定されたインターフェイスです。

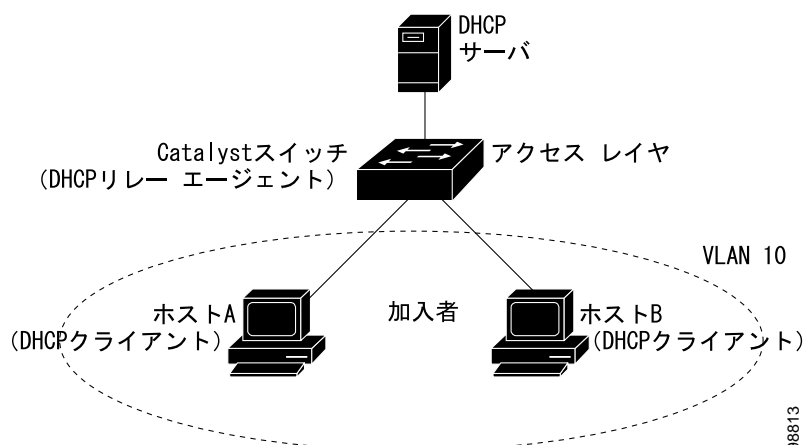
DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールに似た機能を果たします。また、エンドユーザに接続する信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続する信頼できるインターフェイスとを区別する方法も提供します。

## Option 82 データ挿入

住宅地のメトロポリタンイーサネットアクセス環境では、DHCP により、多数の加入者への IP アドレスの割り当てを集中管理することができます。スイッチで DHCP Option 82 機能がイネーブルの場合は、(MAC アドレスのほかに) ネットワークへの接続に使用されるスイッチポートにより、加入者を識別します。加入者 LAN の複数のホストは、アクセススイッチ上の同一ポートに接続することができ、一意に識別されます。

[図 19-1](#) は、中央集中型 DHCP サーバが、アクセスレイヤでスイッチに接続している加入者に IP アドレスの割り当てを行うメトロポリタンイーサネットネットワークの例です。DHCP クライアントおよびこれに対応する DHCP サーバは、同じ IP ネットワークまたはサブネット上には存在しないため、DHCP リレーエージェント (Catalyst スイッチ) は、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の DHCP メッセージを伝送するように、ヘルパーアドレスを使用して設定されます。

図 19-1 メトロポリタンイーサネットネットワークの DHCP リレー エージェント



スイッチで DHCP スヌーピング情報 Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- ホスト (DHCP クライアント) は、DHCP 要求を生成して、ネットワーク上にブロードキャストします。
- スイッチが 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) およびパケットの受信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。
- 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 サーバで、パケットを受信します。サーバが Option 82 対応の場合は、リモート ID、回線 ID、またはその両方を使用して、IP アドレスを割り当てて、単一のリモート ID または回線 ID に割り当てることができる IP アドレス数を制限するなど、ポリシーの実装を行います。さらに DHCP サーバは、DHCP 応答内に Option 82 フィールドをそのまま含めます。
- スイッチにより要求がサーバにリレーされた場合、DHCP サーバはこれに対する応答をスイッチにユニキャストします。スイッチでは、リモート ID あるいは回線 ID フィールドを調べて、自分が挿入した Option 82 データ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、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。

## DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに参加すると、スイッチはスタック マスターから DHCP スヌーピング設定を受信します。メンバーがスタックから脱退した場合は、スイッチに関連付けられたすべての DHCP スヌーピング バインディングが無効になります。

スタック マージが発生し、スタック マスターがもはやスタック マスターでなくなると、そのスタック マスター内のすべての DHCP スヌーピング バインディング (スタック マスターは除く) が失われます。スタック分割により、既存のスタック マスターは変更されませんが、分割されたスイッチに所属するバインディングは、無効になります。分割されたスタックの新しいマスターは、新たに着信する DHCP パケットの処理を開始します。スイッチ スタックの詳細については、[第 5 章「スイッチ スタックの管理」](#)を参照してください。

## DHCP 機能の設定

ここでは、スイッチに DHCP スヌーピングおよび Option 82 を設定する手順について説明します。

- DHCP のデフォルト設定 ( p.19-4 )
- DHCP スヌーピング設定時の注意事項 ( p.19-4 )
- DHCP スヌーピングおよび Option 82 のイネーブル化 ( p.19-4 )

### DHCP のデフォルト設定

表 19-1 に、DHCP のデフォルト設定を示します。

表 19-1 DHCP のデフォルト設定

機能	デフォルト設定
グローバルにイネーブルにされた DHCP スヌーピング	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
DHCP スヌーピング制限レート	設定なし
DHCP スヌーピングの信頼	信頼されない
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注意事項

ここでは、DHCP スヌーピングの設定時の注意事項を説明します。

- スイッチでは、DHCP スヌーピングをグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN 上でイネーブルになるまで、アクティブではありません。
- スイッチで DHCP スヌーピングをグローバルにイネーブルにすると、スヌーピングがディセーブルになるまで、次の Cisco IOS コマンドを使用できません。次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。
  - `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 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 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 trusted` インターフェイス コンフィギュレーション コマンド
- スイッチに DHCP オプション情報を設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりすることができる IP アドレスを指定する、またはデバイスに DHCP オプションを設定する必要があります。
  - ご使用のスイッチが DHCP サーバである場合、詳細に関しては、「[DHCP サーバの設定](#)」( p.4-6 ) を参照してください。
  - DHCP サーバがシスコ デバイスである場合は、『*Cisco IOS IP and IP Routing Configuration Guide for Release 12.1*』の「Configuring DHCP」の章の「IP Addressing and Services」を参照してください。それ以外の場合は、サーバに付属のマニュアルを参照してください。

### DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip dhcp snooping</b>	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	<b>ip dhcp snooping vlan <i>vlan-id</i> [<i>vlan-id</i>]</b>	VLAN または VLAN 範囲で、DHCP スヌーピングをイネーブルにします。VLAN ID 番号を使用して単一の VLAN を指定することも、また、先頭および最後の VLAN ID を使用して VLAN 範囲を指定することもできます。指定できる範囲は 1 ~ 4094 です。
ステップ 4	<b>ip dhcp snooping information option</b>	スイッチをイネーブルにして、DHCP サーバへの DHCP 要求メッセージの DHCP リレー情報 (Option 82 フィールド) を挿入または削除します。  デフォルトではイネーブルです。
ステップ 5	<b>interface <i>interface-id</i></b>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	<b>ip dhcp snooping trust</b>	(任意) インターフェイスを <i>trusted</i> または <i>untrusted</i> と設定します。信頼されないクライアントからメッセージを受信するようにインターフェイスを設定するには、 <b>no</b> キーワードを使用します。デフォルトでは <i>untrusted</i> です。
ステップ 7	<b>ip dhcp snooping limit rate <i>rate</i></b>	(任意) インターフェイスが受信できる毎秒ごとの DHCP パケット数を設定します。指定できる範囲は 1 ~ 4294967294 です。デフォルトでは、レート制限は設定されていません。   (注) 信頼されないレート制限を毎秒100パケット以下にすることを推奨します。通常、レート制限は、信頼されないインターフェイスに適用されます。信頼されるインターフェイスにレート制限を設定する場合、信頼されるインターフェイスは DHCP トラフィックをスイッチに集約する可能性があるため、レート制限をより大きな値に調整する必要があります。
ステップ 8	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	<b>show running-config</b>	設定を確認します。
ステップ 10	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 で DHCP スヌーピングをグローバルにイネーブルにし、ポート上でレート制限を毎秒 100 パケットに設定する方法を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

## DHCP 情報の表示

スイッチ上のすべてのインターフェイスに関する DHCP スヌーピング バインディング テーブルおよび設定情報を表示することができます。

### バインディング テーブルの表示

各スイッチの DHCP スヌーピング バインディング テーブルには、信頼されないポートに対応するバインディング エントリがあります。このテーブルには、信頼されるポートと相互接続するホストに関する情報はありません。相互接続されたスイッチには、それぞれ固有の DHCP スヌーピング バインディング テーブルがあるためです。

次に、スイッチの DHCP スヌーピング バインディング エントリを表示する例を示します。

```
Switch# show ip dhcp snooping binding
-----
MacAddress          IpAddress          Lease(sec)  Type           VLAN  Interface
-----
00:30:94:C2:EF:35   41.0.0.51          286         dynamic        41    gigabitethernet2/0/1
00:D0:B7:1B:35:DE   41.0.0.52          237         dynamic        41    gigabitethernet2/0/1
00:00:00:00:00:01   40.0.0.46          286         dynamic        40    gigabitethernet1/0/2
00:00:00:00:00:03   42.0.0.33          286         dynamic        42    gigabitethernet3/0/2
00:00:00:00:00:02   41.0.0.53          286         dynamic        41    gigabitethernet2/0/2
```

表 19-2 には、`show ip dhcp snooping binding` コマンド出力のフィールドを示します。

表 19-2 show ip dhcp snooping binding コマンドの出力

フィールド	説明
MacAddress	クライアントのハードウェア MAC アドレス
IpAddress	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(sec)	IP アドレスのリース時間
Type	バインディング タイプ (DHCP スヌーピングにより学習されるダイナミックなバインディング、またはスタティックに設定されるバインディング)
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 ホストに接続するインターフェイス

### DHCP スヌーピング設定の表示

次に、スイッチの DHCP スヌーピング設定を表示する例を示します。

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Interface          Trusted      Rate limit (pps)
-----
gigabitethernet1/0/1   yes         unlimited
gigabitethernet2/0/2   no          5000
gigabitethernet2/0/3   yes         unlimited
gigabitethernet2/0/4   yes         unlimited
```