



DHCP の設定

DHCP の設定に関する情報

この章では、スイッチに **Dynamic Host Configuration Protocol (DHCP)** スヌーピング機能、**Option 82** データ挿入機能、および **DHCP** サーバのポートベースのアドレス割り当て機能を設定する方法について説明します。また、**IP** ソース ガード機能の設定方法についても説明します。

DHCP スヌーピング

DHCP は、中央のサーバからホスト **IP** アドレスを動的に割り当てるために **LAN** 環境で広く使用されており、それによって **IP** アドレス管理のオーバーヘッドが大幅に軽減されます。**DHCP** では、ネットワークに接続されたホストだけが **IP** アドレスを使用し、**IP** アドレスを永続的にホストに割り当てる必要がなくなるため、限られた **IP** アドレス空間を節約できます。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから **DHCP** クライアントに **IP** アドレスを割り当て、それらのアドレスを管理します。**DHCP** サーバがそのデータベースから要求された設定パラメータを取得して **DHCP** クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ **DHCP** サーバに要求を転送します。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で **DHCP** パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、**IP** データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、**DHCP** メッセージを受け取ると、新しい **DHCP** メッセージを生成して、出力インターフェイス上で送信します。

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と **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 テーブルとも呼ばれる) の作成および管理によってネットワーク セキュリティを確保する **DHCP** セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと **DHCP** サーバの間でファイアウォールに似た役割を果たします。**DHCP** スヌーピングを使用することにより、エンド ユーザに接続された信頼できないインターフェイスと **DHCP** サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

注: **DHCP** スヌーピングを正しく機能させるためには、すべての **DHCP** サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない **DHCP** メッセージとは、ネットワークまたはファイアウォールの外側から送信されたメッセージのことです。サービス プロバイダー環境で **DHCP** スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信頼できないインターフェイスとなります。

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、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合 (デフォルト)、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スwitchが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スwitchに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スwitchに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スwitchによって挿入された Option 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソースガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジ スwitchとの接続ポートは、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。

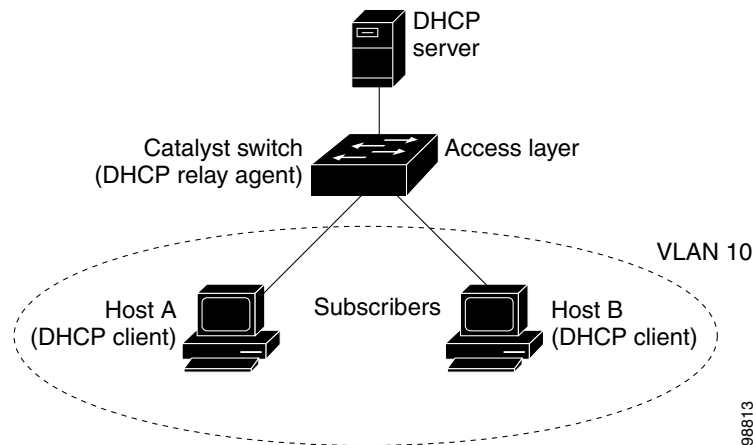
Option 82 データ挿入

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。サブスクリバ LAN 上の複数のホストをアクセス スwitch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。

注: DHCP オプション 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、この機能を使用するサブスクリバ デバイスが割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 60 (415 ページ) 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。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント (Catalyst スwitch) にヘルパー アドレスを設定することにより、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 60 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。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスで、回線 ID サブオプションは、パケットが受信されるポートの識別子 **vlan-mod-port** です。
- 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、スイッチはこの IP アドレスを DHCP パケットに追加します。
- 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、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。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。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。

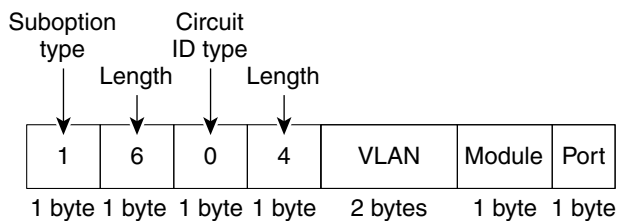
デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、[図 61 \(416 ページ\)](#)にある次のフィールドの値は変化しません。

- 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
 - リモート ID タイプの長さ

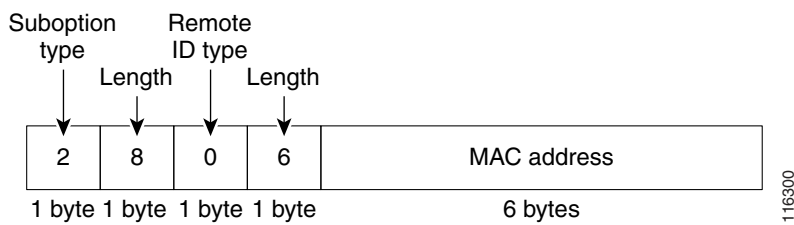
回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。図 61 (416 ページ) に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションの packet フォーマットを示します。スイッチがこれらの packet 形式を使用するのは、DHCP スヌーピングをグローバルに有効にし、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合です。

図 61 サブオプションの packet 形式

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format

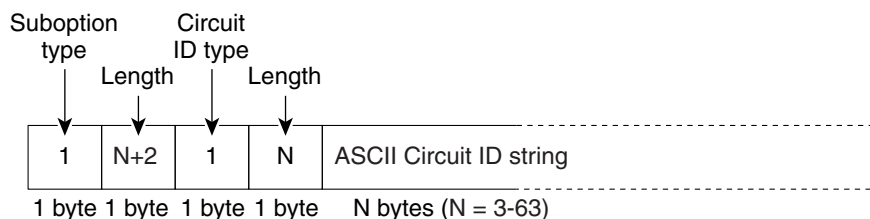
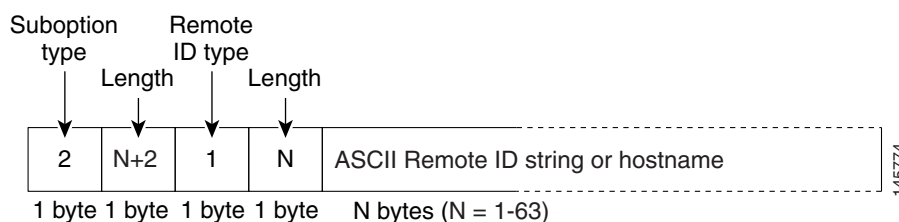


(417 ページ) は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションの packet 形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらの packet が使用されます。

packet では、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
 - 回線 ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
 - リモート ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。

図 62 ユーザ設定のサブオプションのパケット形式

Circuit ID Suboption Frame Format (for user-configured string):**Remote ID Suboption Frame Format (for user-configured string):**

Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てるのが可能です。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ (バインディング) は、IP アドレス、それに関連付けられた MAC アドレス、リース期間 (16 進形式)、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。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。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、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。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

DHCP の設定に関する情報

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内(書き込み遅延および中断タイムアウトの値によって設定される)に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを **DHCP** スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スwitchがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している(スイッチはリース期間の終了時にバインディング エントリを削除しないことがある)。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッドインターフェイスまたは **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。

DHCP スヌーピングのデフォルト設定

表 46 DHCP スヌーピングのデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。 ¹
DHCP リレー エージェント	有効 ²
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル(無効なメッセージは廃棄)。2.(419 ページ)
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。2.(419 ページ)

表 46 DHCP スヌーピングのデフォルト設定(続き)

機能	デフォルト設定
DHCP スヌーピングをグローバルにイネーブル化	無効
DHCP スヌーピング情報オプション	有効
パケットを信頼できない入カインターフェイスで受け取る DHCP スヌーピング オプション ³	無効
DHCP スヌーピング レート制限	未設定
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	無効
DHCP スヌーピングの MAC アドレス検証	有効
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 注:スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワークアドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
3. この機能は、スイッチがエッジスイッチによって Option 82 が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- DHCP スヌーピングは、スイッチ上で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 で DHCP スヌーピングがイネーブルになるまでアクティブになりません。
- 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。
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- スイッチ上で文字数の多いサーキット ID を設定する場合、NVRAM またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わせられた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルである場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ 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、ポートを信頼できるポートとして設定してください。
- スイッチ 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、ポートを信頼できないポートとして設定してください。

DHCP の設定に関する情報

- 信頼できないデバイスが接続されたアグリゲーション スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスがオプション 82 情報をスプーフィングする可能性があります。
- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

注: RSPAN VLAN で DHCP スヌーピングをイネーブルにしないでください。RSPAN VLAN で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN 宛先ポートに届かない可能性があります。

DHCP スヌーピング バインディング データベースの注意事項

- NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
- ネットワーク ベースの URL (TFTP や FTP など) については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
- データベースに正しいリース期間が記録されるように、NTP をイネーブルにし、設定することを推奨します。詳細については、「[手動での日時の設定 \(117 ページ\)](#)」を参照してください。
- NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。

パケット転送アドレス

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address address** インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようにします。

DHCP サーバ ポートベースのアドレス割り当て

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代替りのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代替りのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当て設定時の注意事項を説明します。

- 1つのポートに付き割り当てることができる IP アドレスは 1 つだけです。
- 専用アドレス(事前に設定されたアドレス)は、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドではクリアできません。
- 事前に設定されたアドレスは、通常の動的な IP アドレス割り当てからは自動的に除外されます。ホスト プールでは、事前に設定されたアドレスは使用できませんが、1 つの DHCP アドレス プールに対して複数のアドレスを事前に設定することはできます。
- DHCP プールから事前に設定された予約への割り当てを制限する(予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない)ために、**reserved-only DHCP** プール コンフィギュレーション コマンドを入力することができます。

DHCP の設定方法

DHCP リレー エージェントの設定

	コマンド	目的
1.	configure terminal	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。
2.	service dhcp	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
3.	end	特権 EXEC モードに戻ります。

パケット転送アドレスの指定

	コマンド	目的
1.	configure terminal	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。
2.	interface vlan <i>vlan-id</i>	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
3.	ip address <i>ip-address subnet-mask</i>	インターフェイスに IP アドレスおよび IP サブネットを設定します。

コマンド	目的
4. ip helper-address <i>address</i>	DHCP パケット転送アドレスを指定します。 ヘルパーアドレスは特定の DHCP サーバアドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパーアドレスを設定できます。
5. exit	グローバル コンフィギュレーション モードに戻ります。
6. interface range <i>port-range</i> または interface <i>interface-id</i>	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
7. switchport mode access	ポートの VLAN メンバシップ モードを定義します。
8. switchport access vlan <i>vlan-id</i>	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
9. end	特権 EXEC モードに戻ります。

DHCP スヌーピングおよび Option 82 のイネーブル化

コマンド	目的
1. configure terminal	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。
2. 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。
3. ip dhcp snooping vlan <i>vlan-range</i>	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。指定できる範囲は 1 ~ 4096 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
4. ip dhcp snooping information option	スイッチが DHCP サーバへの DHCP 要求メッセージにおいて DHCP リレー情報 (Option 82 フィールド) を挿入および削除できるようにします。これがデフォルトの設定です。
5. ip dhcp snooping information option format remote-id [<i>string ASCII-string</i> <i>hostname</i>]	(任意) リモート ID サブオプションを設定します。 次のようにリモート ID を設定できます。 <ul style="list-style-type: none">■ 63 文字までの ASCII 文字列 (スペースなし)■ スイッチのホスト名 注: ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID はスイッチ MAC アドレスです。

コマンド	目的
6. ip dhcp snooping information option allow-untrusted	<p>(任意)スイッチがエッジ スイッチに接続された集約スイッチである場合、スイッチがエッジ スイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを受け入れるようにします。</p> <p>デフォルト設定では無効になっています。</p> <p>注:このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。</p>
7. interface interface-id	<p>設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。</p>
8. ip dhcp snooping vlan vlan information option format-type circuit-id [override] string ASCII-string	<p>(任意)指定したインターフェイスの回線 ID サブオプションを設定します。</p> <p>1 ~ 4096 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、フォーマットは vlan-mod-port です。</p> <p>回線 ID は 3 ~ 63 の ASCII 文字列(スペースなし)を設定できます。</p> <p>(任意)override キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。</p>
9. ip dhcp snooping trust	<p>(任意)インターフェイスを信頼できるインターフェイスまたは信頼できないインターフェイスとして設定します。信頼できないクライアントからの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、no キーワードを使用します。デフォルト設定は untrusted です。</p>
10. ip dhcp snooping limit rate rate	<p>(任意)インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは、レート制限は設定されません。</p> <p>注:信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングを使った複数の VLAN に割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になることがあります。</p>
11. exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
12. ip dhcp snooping verify mac-address	<p>(任意)信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。</p>
13. end	<p>特権 EXEC モードに戻ります。</p>

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

コマンド	目的
1. configure terminal	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。
2. ip dhcp snooping database {flash:/filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}/{directory} /image-name.tar rctp://user@host/filename} tftp://host/filename	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 <ul style="list-style-type: none"> ■ flash:/filename ■ ftp://user:password@host/filename ■ http://[[username:password]@]{hostname host-ip}/{directory}/image-name.tar ■ rctp://user@host/filename ■ tftp://host/filename
3. ip dhcp snooping database timeout seconds	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間(秒数)を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ~ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
4. ip dhcp snooping database write-delay seconds	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。範囲は 15 ~ 86400 秒です。デフォルトは 300 秒(5分)です。
5. end	特権 EXEC モードに戻ります。
6. ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds	(任意)DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。 vlan-id の範囲は 1 ~ 4904 です。 seconds の範囲は 1 ~ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 注: このコマンドは、スイッチをテストまたはデバッグするときに使用します。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

コマンド	目的
1. configure terminal	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。
2. ip dhcp use subscriber-id client-id	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
3. ip dhcp subscriber-id interface-name	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。

コマンド	目的
4. interface <i>interface-id</i>	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
5. ip dhcp server use subscriber-id client-id	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
6. end	特権 EXEC モードに戻ります。

IP アドレスの事前割り当て

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。DHCP プールから事前に設定された予約への割り当てを制限するために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。ネットワークまたはプール上の範囲の一部である予約されていないアドレスがクライアントには提供されず、他のクライアントはプールによるサービスを受けられません。このコマンドの入力により、ユーザは、共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視する DHCP プールを持つスイッチのグループを設定できます。

コマンド	目的
1. configure terminal	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。
2. ip dhcp pool <i>poolname</i>	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名は、記号文字列 (Engineering など) または整数 (0 など) です。
3. network <i>network-number</i> [<i>mask</i> <i>/prefix-length</i>]	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。
4. address <i>ip-address client-id string</i> [<i>ascii</i>]	インターフェイス名で指定された DHCP クライアントの IP アドレスを予約します。 <i>string</i> : ASCII 値、または 16 進数値のいずれかです。
5. reserved-only	(任意) DHCP アドレス プールでは、予約されたアドレスだけを使用します。デフォルトでは、プール アドレスは制限されません。
6. end	特権 EXEC モードに戻ります。

DHCP のモニタリングおよびメンテナンス

コマンド	目的
show interface <i>interface id</i>	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。
ip dhcp snooping database timeout <i>seconds</i>	データベース転送プロセスを打ち切るまでの時間 (秒) を指定します。
ip dhcp snooping database write-delay <i>seconds</i>	バインディング データベースが変更された後に、転送を遅らせる期間 (秒) を指定します。

コマンド	目的
clear ip dhcp snooping database statistics	DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアします。
renew ip dhcp snooping database	DHCP スヌーピング バインディング データベースを更新します。
show ip dhcp snooping database [detail]	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp pool	DHCP プール設定を確認します。
copy running-config startup-config	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 の設定例

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化:例

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージ内のクライアント ID フィールドを一切無視して、その代わりに、加入者の ID を使用しています。加入者 ID はインターフェイスのショート名に基づきます。また、クライアントの事前割り当てされた IP アドレスは 10.1.1.7 です。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>
```

次に、事前割り当てされたアドレスが DHCP プールに正常に予約された例を示します。

```
switch# show ip dhcp pool dhcppool
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
```

その他の参考資料

```

Current index   IP address range      Leased/Excluded/Total
10.1.1.1       10.1.1.1 - 10.1.1.254  0    / 4 / 254
1 reserved address is currently in the pool
Address         Client
10.1.1.7       Et1/0

```

DHCP スヌーピングのイネーブル化:例

次に、DHCP スヌーピングをグローバルおよび VLAN 10 でイネーブルにし、ポートのレート制限を 1 秒あたり 100 パケットに設定する例を示します。

```

Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip dhcp snooping limit rate 100

```

その他の参考資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連ドキュメント

関連項目	マニュアル タイトル
Cisco IOS 基本コマンド	『Cisco IOS Configuration Fundamentals Command Reference』
Cisco IOS DHCP コマンド	『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』
Cisco IOS DHCP 設定 Cisco IOS DHCP サーバ ポート ベースのアドレス割り当て	『Cisco IOS IP Configuration Guide』の「IP Addressing and Services」の章
Cisco IOS DHCP 設定作業リスト	『Cisco IOS IP Configuration Guide』の「Configuring DHCP」の章

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	-

MIB

MIB	MIB のリンク
-	Cisco IOS XR ソフトウェアを使用して MIB を特定およびダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニュー (http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml) からプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	-