



## DHCP の設定

---

- [機能情報の確認, 1 ページ](#)
- [DHCP に関する情報, 1 ページ](#)
- [DHCP 機能の設定方法, 9 ページ](#)
- [DHCP サーバポートベースのアドレス割り当ての設定, 21 ページ](#)

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェアリリースの [Bug Search Tool](#) およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## DHCP に関する情報

### 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。スイッチは、DHCP サーバとして機能できます。

## 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、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。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、信頼できるインターフェイスとして設定できるものの例として、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あります。信頼できないインターフェイスには、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があります。

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。

- DHCP OFFER パケット、DHCP ACK パケット、DHCP NAK パケット、DHCP REQUEST 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 DHCP RELEASE または DHCP DECLINE 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イッチ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イッチに接続できる場合、**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イッチ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イッチとの接続ポートは、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。

通常、ワイヤレスクライアントにパケットをブロードキャストするのは望ましくありません。したがって、DHCP スヌーピングは、宛先ブロードキャスト MAC アドレス (ffff.ffff.ffff) をサーバからワイヤレスクライアントに送信される DHCP パケットのユニキャスト MAC アドレスに置き換えます。ユニキャスト MAC アドレスは DHCP ペイロードの CHADDR フィールドから取得されます。この処理は、DHCP OFFER、DHCP ACK および DHCP NACK メッセージなどのクライアント パケットにサーバ用に適用されます。**ip dhcp snooping wireless bootp-broadcast enable** は、この動作を戻すために使用できます。ワイヤレス BOOTP ブロードキャストがイネーブルの場合、サーバからのブロードキャスト DHCP パケットは、宛先 MAC アドレスを変更せずにワイヤレスクライアントに転送されます。

## 関連トピック

[DHCP スヌーピングおよび Option 82 を設定するための前提条件](#)、(15 ページ)

## Option 82 データ挿入

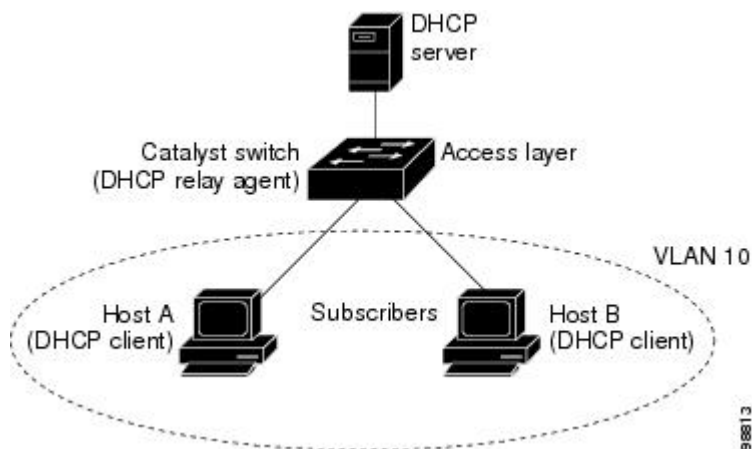
住宅地域にあるメトロポリタンイーサネットアクセス環境では、DHCPは多数の加入者に対し、IPアドレスの割り当てを一元的に管理できます。スイッチでDHCPスヌーピングのOption 82機能をイネーブルにすると、加入者装置はMACアドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。サブスクリイバLAN上の複数のホストをアクセススイッチの同じポートに接続できます。これらのホストは一意に識別されます。



(注) DHCP Option 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、Option 82 を使用する加入者装置が割り当てられた VLAN でイネーブルである場合に限りサポートされます。

次の図に、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 スイッチ) 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 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 サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID (**vlan-mod-port**) です。リモート ID および回線 ID は設定できます。サブオプションの設定の詳細については、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、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 応答内にオプション 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、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

- 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

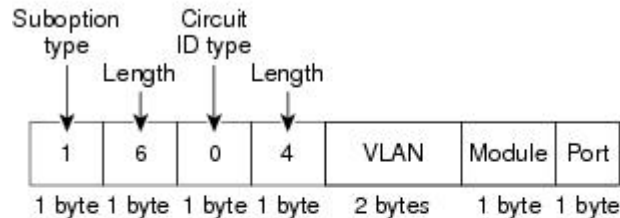
回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable (SFP) モジュール スロットを搭載するスイッチでは、ポート 3 がギガビットイーサネット 1/0/1 ポート、ポート 4 がギガビットイーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビットイーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」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 サブオプションのパケット形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、

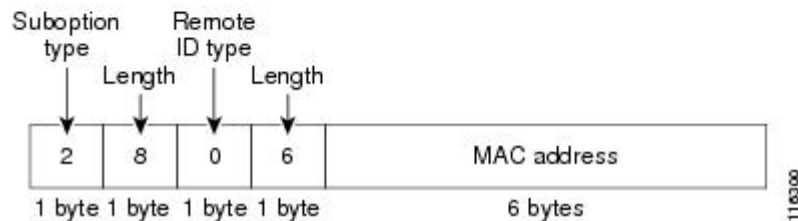
ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 2：サブオプションの packets 形式

### Circuit ID Suboption Frame Format



### Remote ID Suboption Frame Format



図「ユーザ設定のサブオプションの packets 形式」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 packets 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 packets 形式が使用されます。

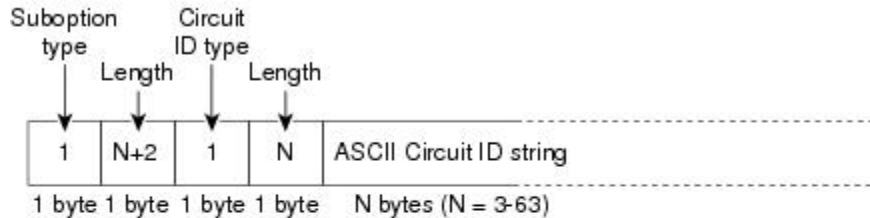
packets では、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 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。

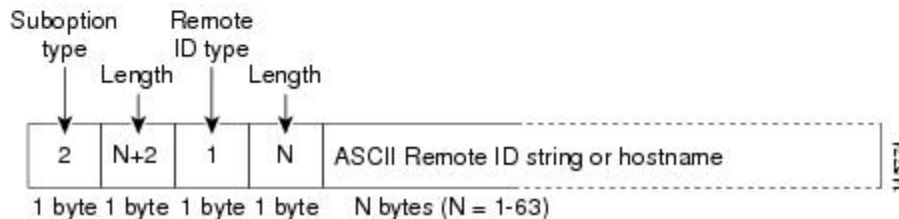
° 設定した文字列の長さに応じて、長さの値が変化する。

図 3: 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。手動および自動アドレス バインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

## 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、64,000 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спек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。

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 Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 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加入すると、スイッチでは、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。メンバがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージングアウトします。

すべてのスヌーピング統計情報は、スタック マスター上で生成されます。新しいスタック マスターが選出された場合、統計カウンタはリセットされます。

スタックのマージが発生し、スタック マスターではなくなった場合、スタック マスターにあったすべての DHCP スヌーピング バインディングが失われます。スタック パーティションでは、既存のスタック マスターに変更はなく、パーティション化スイッチに属しているバインディングは、エージングアウトします。パーティション化スイッチの新しいマスターでは、新たな着信 DHCP パケットの処理が開始されます。

## DHCP 機能の設定方法

### DHCP スヌーピングのデフォルト設定

表 1: DHCP 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 <sup>1</sup>
DHCP リレー エージェント	イネーブル <sup>2</sup>

機能	デフォルト設定
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）。
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。
DHCP スヌーピングをグローバルにイネーブル	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
パケットを信頼できない入力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 <sup>3</sup>	ディセーブル
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	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
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。

<sup>1</sup> 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。

<sup>2</sup> 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。

<sup>3</sup> この機能は、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

- 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。
- `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。

## DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。

スイッチを DHCP サーバとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

## DHCP サーバとスイッチ スタック

DHCP バインディングデータベースは、スタック マスターで管理されます。新しいスタック マスターが割り当てられると、新しいマスターでは、TFTP サーバから保存されているバインディング データベースがダウンロードされます。スタック マスターに障害が発生した場合、未保存のすべてのバインディングが失われます。失われたバインディングに関連付けられていた IP アドレスは、解放されます。自動バックアップは、`ip dhcp database url [timeout seconds | write-delay seconds]` 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設定する必要があります。

スタックのマージが発生すると、スタック メンバになるスタック マスターでは、すべての DHCP リースバインディングが失われます。スタック パーティションでは、パーティションにある新しいマスターが、既存の DHCP リースバインディングなしで、新しい DHCP サーバとして動作します。

## DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

### 手順の概要

1. `enable`
2. `configureterminal`
3. `service dhcp`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Switch# <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 3	<b>service dhcp</b>  例： Switch(config)# <b>service dhcp</b>	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。
ステップ 4	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>  例： Switch# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b>  例： Switch# <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。

## 次の作業

これらの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の「*Configuring DHCP*」の項を参照してください。

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

## パケット転送アドレスの指定

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なります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `interface vlan vlan-id`
4. `ip address ip-address subnet-mask`
5. `ip helper-address address`
6. `end`
7. 次のいずれかを使用します。
  - `interface range port-range`
  - `interface interface-id`
8. `switchport mode access`
9. `switchport access vlan vlan-id`
10. `end`
11. `show running-config`
12. `copy running-config startup-config`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><code>enable</code></p> <p>例 :</p> <pre>Switch&gt; enable</pre>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b>  例： Switch# <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 3	<b>interface vlan vlan-id</b>  例： Switch (config)# interface vlan 1	VLAN ID を入力してスイッチ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。
ステップ 4	<b>ip address ip-address subnet-mask</b>  例： Switch (config-if)# ip address 192.108.1.27 255.255.255.0	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。
ステップ 5	<b>ip helper-address address</b>  例： Switch (config-if)# ip helper-address 172.16.1.2	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。
ステップ 6	<b>end</b>  例： Switch (config-if)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	次のいずれかを使用します。 <ul style="list-style-type: none"> <li>• <b>interface range port-range</b></li> <li>• <b>interface interface-id</b></li> </ul> 例： Switch (config)# interface gigabitethernet1/0/2	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。
ステップ 8	<b>switchport mode access</b>  例： Switch (config-if)# switchport mode access	ポートの VLAN メンバーシップ モードを定義します。

	コマンドまたはアクション	目的
ステップ 9	<b>switchport access vlan</b> <i>vlan-id</i>  例： Switch (config-if)# switchport access vlan 1	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。
ステップ 10	<b>end</b>  例： Switch (config-if)# end	特権 EXEC モードに戻ります。
ステップ 11	<b>show running-config</b>  例： Switch# <b>show running-config</b>	入力を確認します。
ステップ 12	<b>copy running-config startup-config</b>  例： Switch# <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 スヌーピングおよび Option 82 を設定するための前提条件

DHCP スヌーピングおよび Option 82 の前提条件は次のとおりです。

- 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。
- 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。
- スイッチを DHCP 要求に応答するようにする場合は、DHCP サーバとして設定する必要があります。
- 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。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。
- 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。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。

- DHCP スヌーピングで Cisco IOS DHCP サーババインディングデータベースを使用するには、Cisco IOS DHCP サーババインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジスイッチから Option 82 情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - 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。空のファイルを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、ネットワーク タイム プロトコル (NTP) をイネーブルにし、設定することを推奨します。
  - 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。
- 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。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。
- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス (SVI) に設定する必要があります。
- 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。

## 関連トピック

[DHCP スヌーピング, \(2 ページ\)](#)



## 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、次の手順に従います。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping**
4. **ip dhcp snooping vlan***vlan-range*
5. **ip dhcp snooping information option**
6. **ip dhcp snooping information option format remote-id** [*stringASCII-string* | *hostname*]
7. **ip dhcp snooping information option allow-untrusted**
8. **ip dhcp snooping wireless bootp-broadcast enable** (任意)
9. **interface***interface-id*
10. **ip dhcp snooping vlan***vlan***information option format-type circuit-id** [*override*] *stringASCII-string*
11. **ip dhcp snooping trust**
12. **ip dhcp snooping limit rate***rate*
13. **exit**
14. **ip dhcp snooping verify mac-address**
15. **end**
16. **show running-config**
17. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 : Switch# <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 3	<b>ip dhcp snooping</b>  例 : Switch(config)# <b>ip dhcp snooping</b>	DHCP スヌーピングをグローバルにイネーブル化します。

	コマンドまたはアクション	目的
ステップ 4	<b>ip dhcp snooping vlan</b> <i>vlan-range</i>  例：  <pre>Switch(config)# ip dhcp snooping vlan 10</pre>	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 ~ 4094 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。 <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 5	<b>ip dhcp snooping information option</b>  例：  <pre>Switch(config)# ip dhcp snooping information option</pre>	スイッチが、転送された DHCP 要求メッセージにある DHCP リレー情報（オプション 82 フィールド）を DHCP サーバに挿入したり削除したりできるようにイネーブルにします。これがデフォルト設定です。
ステップ 6	<b>ip dhcp snooping information option format remote-id</b> [ <i>stringASCII-string</i>   <i>hostname</i> ]  例：  <pre>Switch(config)# ip dhcp snooping information option format remote-id string acsiistring2</pre>	（任意）リモート ID サブオプションを設定します。 リモート ID は次のように設定できます。 <ul style="list-style-type: none"> <li>• 63 文字までの ASCII 文字列（スペースなし）</li> <li>• スイッチに設定されたホスト名</li> </ul> （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。
ステップ 7	<b>ip dhcp snooping information option allow-untrusted</b>  例：  <pre>Switch(config)# ip dhcp snooping information option allow-untrusted</pre>	（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、エッジスイッチからのオプション 82 情報付き着信 DHCP スヌーピングパケットを受け入れるようにこのコマンドによってスイッチをイネーブルにします。 デフォルト設定では無効になっています。 （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。
ステップ 8	<b>ip dhcp snooping wireless bootp-broadcast enable</b> （任意）  例：  <pre>Switch(config)# ip dhcp snooping wireless bootp-broadcast enable</pre>	サーバによって送信されたブロードキャストアドレスが、DHCP パケットをワイヤレスクライアントに転送するときに、スイッチによって保持されるようにします。

	コマンドまたはアクション	目的
ステップ 9	<b>interface</b> <i>interface-id</i>  例 :  <pre>Switch(config)# interface gigabitethernet2/0/1</pre>	設定するインターフェイスを指定し、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。
ステップ 10	<b>ip dhcp snooping vlan</b> <i>vlan</i> <b>information option format-type circuit-id</b> <b>[override] string</b> <i>ASCII-string</i>  例 :  <pre>Switch(config-if)# ip dhcp snooping vlan 1 information option format-type curcuit-id override string ovrride2</pre>	<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 ~ 4094 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 <b>vlan-mod-port</b> 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) <b>override</b> 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>
ステップ 11	<b>ip dhcp snooping trust</b>  例 :  <pre>Switch(config-if)# ip dhcp snooping trust</pre>	(任意) インターフェイスの信頼性を <b>trusted</b> または <b>untrusted</b> に設定します。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、 <b>no</b> キーワードを使用します。デフォルト設定は <b>untrusted</b> です。
ステップ 12	<b>ip dhcp snooping limit rate</b> <i>rate</i>  例 :  <pre>Switch(config-if)# ip dhcp snooping limit rate 100</pre>	<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>
ステップ 13	<b>exit</b>  例 :  <pre>Switch(config-if)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	<b>ip dhcp snooping verify mac-address</b>  例 :  <pre>Switch(config)# ip dhcp snooping verify mac-address</pre>	(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。

	コマンドまたはアクション	目的
ステップ 15	<b>end</b>  例： Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 16	<b>show running-config</b>  例： Switch# <b>show running-config</b>	入力を確認します。
ステップ 17	<b>copy running-config startup-config</b>  例： Switch# <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。

## Cisco IOS DHCP サーバデータベースのイネーブル化

Cisco IOS DHCP サーバデータベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

## DHCP スヌーピング情報のモニタリング

表 2: DHCP 情報を表示するためのコマンド

<b>show ip dhcp snooping</b>	スイッチの DHCP スヌーピングの設定を表示します。
<b>show ip dhcp snooping binding</b>	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。
<b>show ip dhcp snooping database</b>	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。
<b>show ip dhcp snooping statistics</b>	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。

<code>show ip source binding</code>	動的および静的に設定されたバインディングを表示します。
-------------------------------------	-----------------------------



(注) DHCP スヌーピングがイネーブルでインターフェイスがダウンステートに変更された場合、静的に設定されたバインディングは削除されません。

## DHCP サーバポートベースのアドレス割り当ての設定

### DHCP サーバポートベースのアドレス割り当ての設定の概要

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はなりません。

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。

### ポートベースのアドレス テーブルのデフォルト設定

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

- 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。
- 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 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

スイッチ上で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をイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp snooping database {flash[number]:/filename | ftp://user:password@host/filename | http://[[username:password]@]{hostname | host-ip}[/directory] /image-name.tar | rcp://user@host/filename} | tftp://host/filename**
4. **ip dhcp snooping database timeoutseconds**
5. **ip dhcp snooping database write-delayseconds**
6. **end**
7. **ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiryseconds**
8. **show ip dhcp snooping database [detail]**
9. **show running-config**
10. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 :  Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b>  例 :  Switch# <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 3	<b>ip dhcp snooping database {flash[number]:/filename   ftp://user:password@host/filename   http://[[username:password]@]{hostname   host-ip}[/directory] /image-name.tar   rcp://user@host/filename}   tftp://host/filename</b>  例 :  Switch(config)# <b>ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</b>	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"> <li>• <b>flash[number]:/filename</b>                (任意) スタック マスターのスタック メンバ番号を指定するには、<i>number</i> パラメータを使用します。<i>number</i> の指定できる範囲は 1 ~ 9 です。</li> <li>• <b>ftp://user:password@host/filename</b></li> <li>• <b>http://[[username:password]@]{hostname   host-ip}[/directory] /image-name.tar</b></li> <li>• <b>rcp://user@host/filename</b></li> <li>• <b>tftp://host/filename</b></li> </ul>
ステップ 4	<b>ip dhcp snooping database timeoutseconds</b>  例 :  Switch(config) # <b>ip dhcp snooping database timeout 300</b>	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。
ステップ 5	<b>ip dhcp snooping database write-delayseconds</b>  例 :  Switch(config) # <b>ip dhcp snooping database write-delay 15</b>	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。指定できる範囲は 15 ~ 86400 秒です。デフォルトは 300 秒 (5 分) です。

	コマンドまたはアクション	目的
ステップ 6	<b>end</b>  例：  Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>ip dhcp snooping</b> <b>binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</b>  例：  Switch# <b>ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</b>	(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 に指定できる範囲は 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。  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。
ステップ 8	<b>show ip dhcp snooping database [detail]</b>  例： Switch # <b>show ip dhcp snooping database detail</b>	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。
ステップ 9	<b>show running-config</b>  例：  Switch# <b>show running-config</b>	入力を確認します。
ステップ 10	<b>copy running-config startup-config</b>  例：  Switch# <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 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

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。



## 手順の概要

1. **enable**
2. **configureterminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interfaceinterface-id**
6. **ip dhcp server use subscriber-id client-id**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Switch# <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 3	<b>ip dhcp use subscriber-id client-id</b>  例： Switch(config)# <b>ip dhcp use subscriber-id client-id</b>	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。
ステップ 4	<b>ip dhcp subscriber-id interface-name</b>  例： Switch(config)# <b>ip dhcp subscriber-id interface-name</b>	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。
ステップ 5	<b>interfaceinterface-id</b>  例： Switch(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、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。

	コマンドまたはアクション	目的
ステップ 6	<b>ip dhcp server use subscriber-id client-id</b>  例：  Switch(config-if)# <b>ip dhcp server use subscriber-id client-id</b>	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。
ステップ 7	<b>end</b>  例：  Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b>  例：  Switch# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b>  例：  Switch# <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。

### 次の作業

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 サーバポートベースのアドレス割り当てのモニタリング

表 3: DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
<b>show interface</b> <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。
<b>show ip dhcp pool</b>	DHCP アドレス プールを表示します。
<b>show ip dhcp binding</b>	Cisco IOS DHCP サーバのアドレスバインディングを表示します。

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
DHCP 設定情報および手順	『IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S』 <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book.html</a>

### エラーメッセージデコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージデコーダ ツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## DHCP スヌーピングおよび Option 82 の機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。
	<p>次のコマンドのサポートが導入されました。</p> <ul style="list-style-type: none"> <li>• DHCP スヌーピングの統計情報を表示する <b>show ip dhcp snooping statistics</b> ユーザ EXEC コマンド</li> <li>• スヌーピングの統計情報カウンタをクリアする <b>clear ip dhcp snooping statistics</b> 特権 EXEC コマンド</li> </ul>