DHCP の設定

- 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，17 ページ
- DHCP の機能情報，21 ページ

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。

- DHCPOFFER 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。

- スイッチが 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 オプション 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、オプション 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オプション 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。

オプション 82 データ挿入

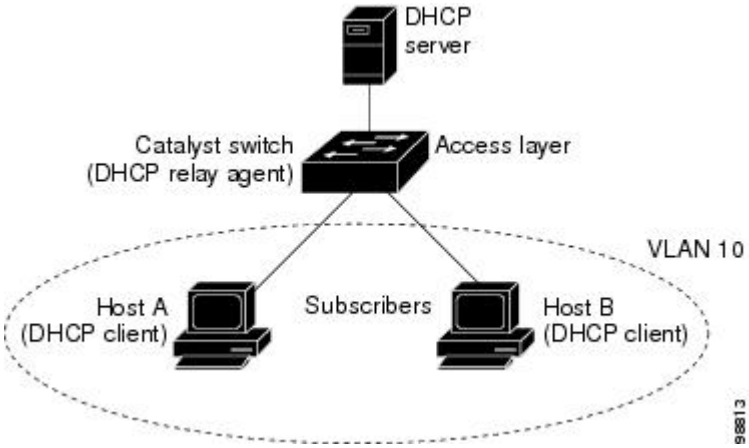
住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP 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、オプション 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 オプション 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。
- 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）。

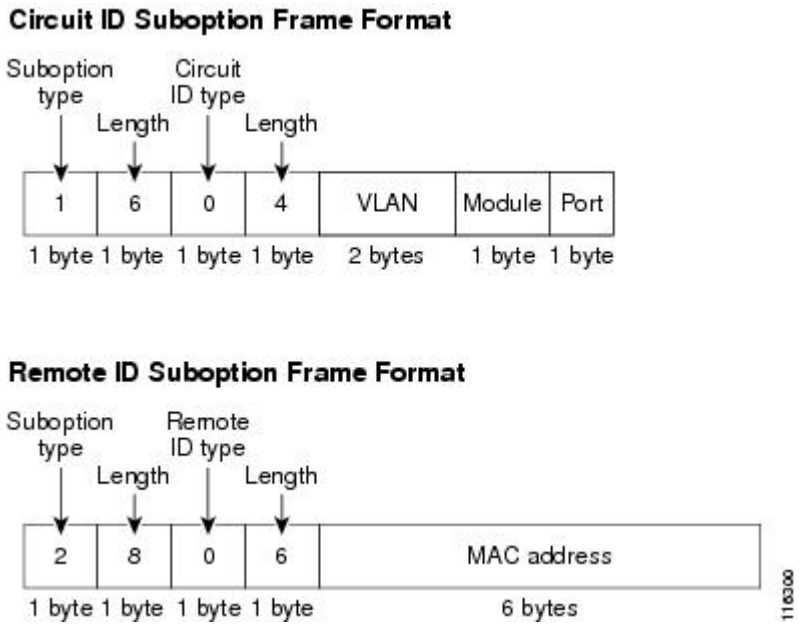
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

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* : サブオプションのパケット形式



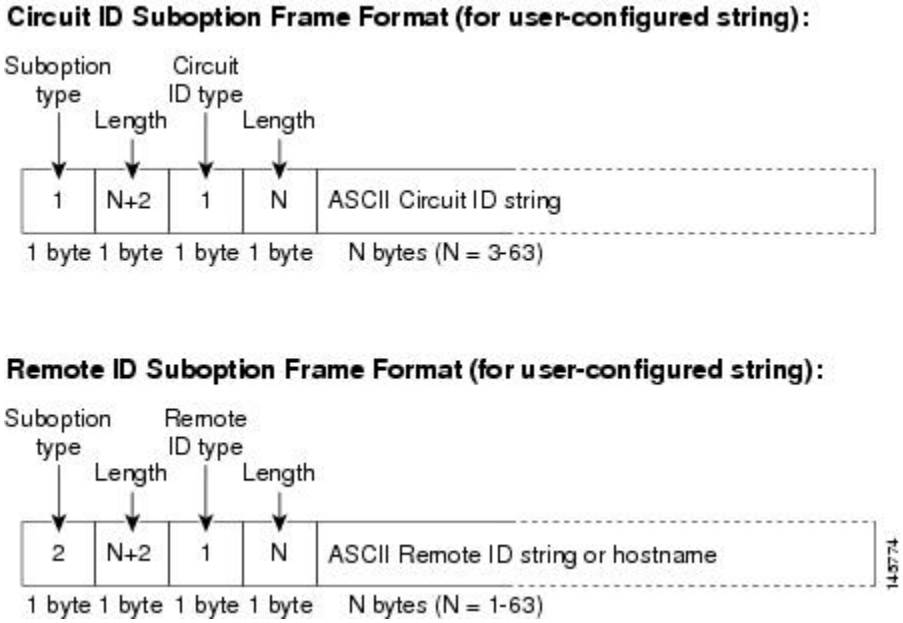
図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した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

パケットでは、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



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ことが可能です。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、その後に 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。

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。

- スイッチ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[1]
DHCP リレー エージェント	イネーブル[2]

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[3]	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。

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オプション 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 interface** 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	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	**configureterminal** 例： `Device# 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。
ステップ 3	**service dhcp** 例： `Device(config)# 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。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（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」の項の「*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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	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	**configureterminal** 例： `Device# 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。
ステップ 3	**interface vlan** *vlan-id* 例： `Device(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	**ip address** *ip-address subnet-mask* 例： `Device(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	**ip helper-address** *address* 例： `Device(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	**end** 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 7	次のいずれかを使用します。 • **interface range** *port-range* • **interface** *interface-id* 例： `Device(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	**switchport mode access** 例： `Device(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。
ステップ 9	**switchport access vlan** *vlan-id* 例： `Device(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	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（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オプション 82 を設定するための前提条件

DHCP スヌーピングおよびオプション 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 スイッチからオプション 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**ip dhcp snooping trust interface**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**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。

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

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 snooping statistics	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。
show ip source binding	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

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わ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、この代わりのデバイスに、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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	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	**configureterminal** 例： `Device# 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。
ステップ 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* 例： `Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	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。 • **flash**[*number*]**:**/*filename* （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、*number* パラメータを使用します。*number* の指定できる範囲は 1 ～ 9 です。 • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename* • **tftp:**//*host*/*filename*
ステップ 4	**ip dhcp snooping database timeout** *seconds* 例： `Device(config)# ip dhcp snooping database timeout 300`	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。

	コマンドまたはアクション	目的
ステップ 5	**ip dhcp snooping database write-delay** *seconds* 例： `Device(config)# ip dhcp snooping database write-delay 15`	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。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **expiry** *seconds* 例： `Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000`	（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	**show ip dhcp snooping database** [**detail**] 例： `Device# 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。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	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	**configureterminal** 例： `Device# 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。
ステップ 3	**ip dhcp use subscriber-id client-id** 例： `Device(config)# 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。
ステップ 4	**ip dhcp subscriber-id interface-name** 例： `Device(config)# 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。
ステップ 5	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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 6	**ip dhcp server use subscriber-id client-id** 例： `Device(config-if)# 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。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（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
show interface *interface id*	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。

DHCP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*DHCP* の機能情報

機能名	リリース	機能情報
DHCP	Cisco IOS XE Everest 16.6.1	DHCP はインターネット ホストに設定パラメータを提供します。DHCP は 2 つのコンポーネントで構成されます。1 つはホスト固有の設定パラメータを DHCP サーバからホストに配信するためのプロトコルで、もう 1 つはホストにネットワーク アドレスを割り当てるためのメカニズムです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバ ホストが、ダイナミックに設定されるホストに対して、ネットワーク アドレスを割り当て、設定パラメータを提供します。デフォルトでは、Cisco IOS ソフトウェアが稼働している Cisco デバイスには、DHCP サーバとリレー エージェント ソフトウェアが含まれています。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9400 シリーズ スイッチ