DHCP の設定

このセクションでは、DHCP の設定について説明します。

- DHCP を設定するための前提条件 （1 ページ）
- DHCP の設定に関する制限 （2 ページ）
- DHCP に関する情報 （3 ページ）
- DHCP の設定方法 （13 ページ）
- DHCP の機能の履歴 （24 ページ）

DHCP を設定するための前提条件

次の前提条件が DHCP スヌーピングおよびオプション 82 に適用されます。

- 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 サーバーや 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 サーバー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 サーバーとして機能するデバイスを設定してください。DHCP サーバー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 スヌーピングが正常に機能するには、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続し、信頼できない DHCP メッセージが信頼できるインターフェイスにだけ転送されるようにする必要があります。サービス プロバイダ 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 サーバー バインディング データベースを使用するには、Cisco IOS DHCP サーバー 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 サーバー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 サーバーとして機能するデバイスを設定してください。DHCP サーバー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 サーバーの 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 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。

DHCP の設定に関する制限

DHCP スヌーピング、DHCP リレーエージェントをサポートする送信（Tx）スイッチドポート アナライザ（SPAN）または出力 SPAN は使用しないことを推奨します。Tx での SPAN が必要な場合は、DHCP パケットの転送パスに含まれる VLAN ポートを使用しないでください。

DHCP に関する情報

DHCP サーバ

DHCP サーバーは、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サーバー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サーバーに要求を転送します。スイッチは、DHCP サーバーとして機能できます。DHCP サーバーは、要求された設定をクライアントに送信するときに、メッセージを他のサーバーに転送しません。

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、エンドユーザーに接続された信頼できないインターフェイスとDHCPサーバー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スヌーピングが正常に機能するには、すべてのDHCPサーバを信頼できるインターフェイスを介してスイッチに接続し、信頼できないDHCPメッセージが信頼できるインターフェイスにだけ転送されるように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 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 スヌーピングがイネーブルになっている場合に、最大スヌーピングキューサイズの 1000 を超える。

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。

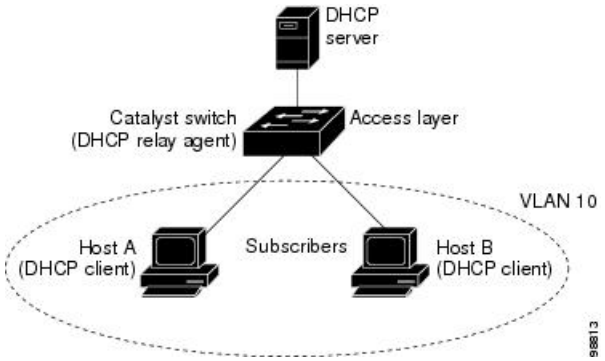
オプション 82 データ挿入

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有効であり、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 で有効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 サーバーがアクセス 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 を有効にすると、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 と回線 ID を設定できます。
- 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 サーバーに転送します。
- 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ーにリレーされた場合、DHCP サーバー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）。

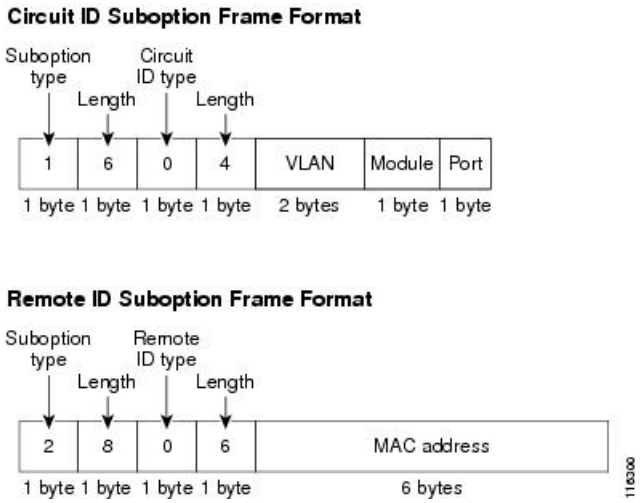
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

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 *2:* サブオプションのパケット形式

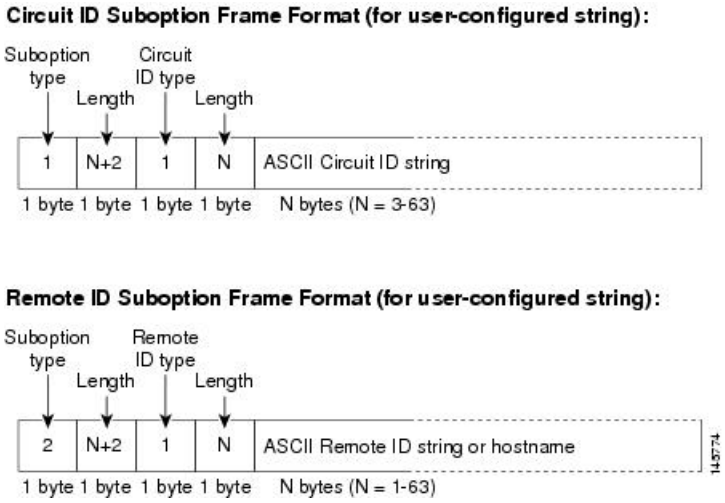


図「ユーザー設定のサブオプションのパケット形式」は、ユーザー設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力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

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 77 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と EOL 記号が続きます。

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。

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
10.1.1.1 512 001.0001.0005 3EBE2881 Gi1/1                                   e5e1e733
10.1.1.1 512 001.0001.0002 3EBE2881 Gi1/1                                   4b3486ec
10.1.1.1 1536 001.0001.0004 3EBE2881 Gi1/1                                  f0e02872
10.1.1.1 1024 001.0001.0003 3EBE2881 Gi1/1                                  ac41adf9
10.1.1.1 1 001.0001.0001 3EBE2881 Gi1/1                                     34b3273e
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、アクティブスイッチで管理されます。新しいスイッチは、スタックに追加されると、アクティブスイッチから 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、アクティブスイッチ上で生成されます。新しいアクティブスイッチが選定された場合、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、アクティブスイッチではなくなった場合、アクティブスイッチにあったすべての 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を使用すると、既存のアクティブスイッチは変更されず、パーティション分割されたスイッチに属しているバインディングはエージアウトします。パーティション分割されたスタックの新しいアクティブスイッチで、新たな着信 DHCP パケットの処理が開始されます。

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]
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

機能	デフォルト設定
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** ユーザー 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 サーバーとスイッチ スタック

DHCPバインディングデータベースは、アクティブスイッチで管理されます。新しいアクティブスイッチが割り当てられると、新しいアクティブスイッチに、TFTP サーバーで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。スイッチの切り替えが発生した場合、新しいアクティブスイッチは、SSO機能を使用して以前のアクティブスイッチで同期されたデータベースファイルを使用します。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。

DHCP サーバ ポートベースのアドレス割り当て

DHCP サーバー 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 の設定方法

DHCP サーバの設定

スイッチは、DHCP サーバーとして機能できます。管理ポートを備えた DHCP クライアント用に DHCP サーバーを使用する場合は、管理 VRF を使用して DHCP プールと対応するインターフェイスの両方を設定する必要があります。

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **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`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次のタスク

- 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 サーバーおよび 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、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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **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。
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

	コマンドまたはアクション	目的
		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	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、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。 • **interface range** *port-range* • **interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	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`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCP for IPv6 アドレス割り当ての設定

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当ての設定時には、次の前提条件が適用されます。

- 次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - IPv6 アドレスが明示的に設定されていない場合は、**ipv6 enable** コマンドを使用して IPv6 ルーティングを有効にします。
  - レイヤ 3 インターフェイスで DHCPv6 ルーティングが有効になっている必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイス。
  - レイヤ 3 モードの EtherChannel ポートチャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- デバイスは、DHCPv6 クライアント、サーバー、またはリレーエージェントの役割を果たすことが可能です。DHCPv6 クライアント、サーバー、およびリレー機能は、インターフェイスで相互に排他的です。
- Cisco IOS XE Gibraltar 16.11.1 以降、DHCPv6 アドレスには、RFC5453 で指定されている予約済みインターフェイス識別子の範囲に含まれないインターフェイス識別子が含まれるようになります。

DHCPv6 サーバー機能の有効化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバー機能を無効にするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスで DHCPv6 サーバー機能を有効にするには、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool 7`	DHCP プール コンフィギュレーション モードを開始して、IPv6 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。
ステップ 4	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} **Example:** `Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime 3600`	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効な状態を維持するタイムインターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。時間間隔なしの場合は、**infinite** を指定します。
ステップ 5	**link-address** *IPv6-prefix* **Example:** `Device(config-dhcpv6)# link-address 2001:1002::0/64`	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバーは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
ステップ 6	**vendor-specific** *vendor-id* **Example:** `Device(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 7	**suboption** *number* { **address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} **Example:** `Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::`	（任意）ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。

	Command or Action	Purpose
ステップ 8	**exit** **Example:** `Device(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 9	**exit** **Example:** `Device(config-dhcpv6)# 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。
ステップ 10	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	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 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Device(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバー機能を有効にします。 • *poolname*：（任意）IPv6 DHCP プールのユーザー定義の名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）サーバーが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージを交換する方式を許可します。 • **preference** 値：（任意）サーバーによって送信されるアドバタイズメント メッセージ内のプリファレンス オプションで指定するプリファレンス値を設定します。範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバーが SOLICIT メッセージに含まれるクライアントの提案を考慮するかど

	Command or Action	Purpose
		うかを指定します。デフォルトでは、サーバーはクライアントのヒントを無視します。
ステップ 12	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 13	次のいずれかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	Example:
	`Device# show ipv6 dhcp pool`
	または
	`Device# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバー機能がインターフェイス上で有効であることを確認します。

ステップ 14	**copy running-config startup-config** **Example:** `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。

DHCPv6 クライアント機能の有効化

インターフェイスで DHCPv6 クライアントを有効にするには、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	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 4	**ipv6 address dhcp** [**rapid-commit**] **Example:** `Device(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバーから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てに2つのメッセージを交換する方式を許可します。
ステップ 5	**ipv6 dhcp client request** [**vendor-specific**] **Example:** `Device(config-if)# ipv6 dhcp client request vendor-specific`	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 6	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 dhcp interface** **Example:** `Device# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスで有効になっていることを確認します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバーデータベースを有効にして設定する手順については、『Cisco IOS IP Configuration Guide』の「Configuring DHCP」の章にある「DHCP Configuration Task List」のセクション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 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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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* • **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。
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	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC 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	**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 gigabitethernet 1/1/0 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。

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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-type interface-number* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。
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。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次のタスク

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 の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

表 *4 :* 新しい機能の履歴

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	DHCP	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 サーバー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/サーバー モデルに基づいています。指定された DHCP サーバー 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。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	DHCP クライアントオプション 12	DHCP クライアントオプション 12 機能により、クライアントのホスト名が指定されます。Dynamic Host Configuration Protocol（DHCP）サーバーからインターフェイスの IP アドレスを取得する際に、クライアントデバイスが応答内の DHCP Hostname オプションを受信すると、このオプションのホスト名が設定されます。DHCP は、IP ネットワークにおける動作のための設定情報を取得するために DHCP クライアントによって使用されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。