



Cisco IOS リリース 15.2(8)E (Catalyst マイクロスイッチ シリーズ) IP アドレッシングサービス コンフィギュレーションガイド

DHCP の設定 2

DHCP を設定するための前提条件 2

DHCP の設定に関する制限 3

DHCP の設定に関する情報 4

DHCP の設定方法 12

DHCP の設定例 21

その他の参考資料 22

DHCP 設定の機能履歴 23

Full Cisco Trademarks with Software License ?

DHCP の設定

DHCP を設定するための前提条件

ここでは、DHCP スヌーピングおよび Option 82 の前提条件について説明します。

- デバイスの DHCP スヌーピングをグローバルにイネーブルにする必要があります。
- デバイス上でグローバルに DHCP スヌーピングをイネーブル化するには、DHCP サーバおよび DHCP リレー エージェントとして機能するデバイスを、事前に設定しイネーブルしておく必要があります。
- デバイスを 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。
- デバイスで 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 スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。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デバイス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、デバイスがエッジデバイスから Option 82 情報を含むパケットを受信する集約デバイス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 スヌーピング用にデバイスを使用するには、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、デバイス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、デバイスのシステムクロックが NTP と同期化されたときにだけ、デバイス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。

- デバイスで 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。
- デバイスが 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 クライアントのデバイス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

ここでは、DHCP スヌーピングおよび Option 82 の制限について説明します。

- 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、この機能を使用する加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。
- 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。
- デバイス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。
- 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。
- 信頼できないデバイスが接続された集約デバイスに **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。
- 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。
- 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 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。

DHCP の設定に関する情報

DHCP サーバ

DHCP サーバは、デバイス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。デバイスは DHCP サーバとして動作することができます。

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 サーバまたは別のデバイス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 スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。

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、デバイス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、デバイス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、カスタマーのデバイスなど、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、およびデバイス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。

デバイスが信頼できないインターフェイス上でパケットを受信した場合は、こ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されていれば、デバイスは送信元 MAC アドレスを DHCP クライアントハードウェアのアドレスと比較します。アドレスが一致した場合（デフォルト）、デバイスはこのパケットを転送します。アドレスが一致しない場合、デバイスはパケットをドロップします。

デバイスは、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。
- デバイスが 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デバイスであり、DHCP Option 82 情報を挿入するエッジデバイスに接続されているデバイスは、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、集約デバイス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。

集約デバイスを信頼できないインターフェイス経由でエッジデバイスに接続できる場合、**ip dhcp snooping information option allow-untrusted** コマンドを入力すると、集約デバイスはエッジデバイス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。集約デバイスは、信頼できないデバイス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。集約デバイスで、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、その場合でもデバイスは 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。集約デバイス上のエッジデバイスとの接続ポートは、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 ペイロード内の 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** を使用して、この動作を元に戻すことができます。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。

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
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 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、デバイス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。

デバイス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、デバイス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、デバイス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、デバイス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。デバイスは、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。

デバイスは、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。デバイス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。デバイスは、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 G11/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB G11/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB G11/0/4 584a38f0
```

END

デバイスが起動し、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、デバイス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、デバイスはエントリを無視します。

- デバイス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（デバイス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。

オプション 82 データ挿入

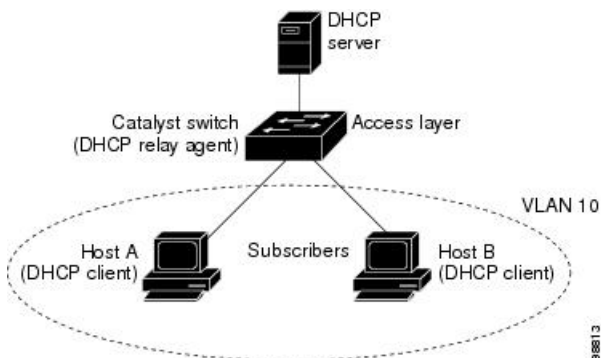
住宅地域にあるメトロポリタンイーサネットアクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。デバイスで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。加入者 LAN 上の複数のホストをアクセスデバイスの同一ポートに接続でき、これらは一意に識別されます。



(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 サーバがアクセスレイヤのデバイス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。
- この DHCP 要求を受信したデバイスは、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 サブオプションがデバイスの 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、デバイスはこの IP アドレスを DHCP パケットに追加します。
- デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバ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。
- デバイスがサーバへの要求を中継した場合、DHCP サーバはそのデバイスに応答をユニキャストします。デバイスはリモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データが挿入されていることを確認します。デバイスは 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）。

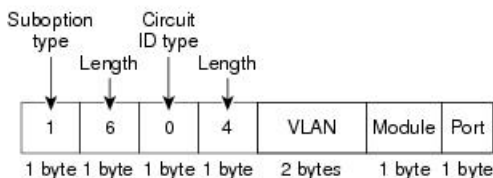
- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

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デバイスでは、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。

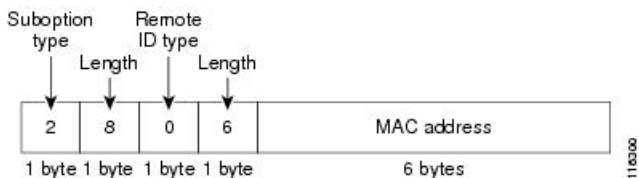
図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option** コマンドを入力すると、デバイスはパケット形式を使用します。

図 2: サブオプションのパケット形式

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format



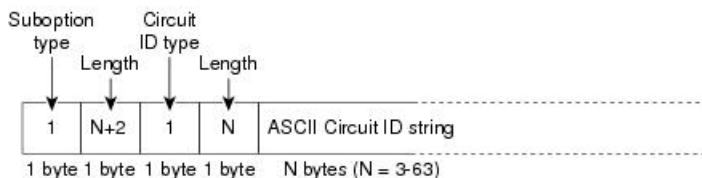
図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。デバイスでは、DHCP スヌーピングをグローバルに有効にし、**ip dhcp snooping information option format remote-id** コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** コマンドを入力した場合に、これらのパケット形式が使用されます。

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。

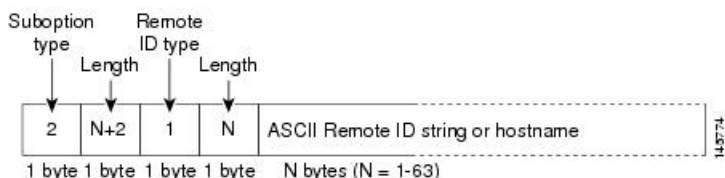
- 回線 ID サブオプション フィールド
 - 回線 ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
 - リモート ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。

図 3: ユーザ設定のサブオプションの packets 形式

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



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



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デバイスは、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ありません。

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。

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 の設定方法

DHCP サーバの設定

デバイスは DHCP サーバとして動作することができます。

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。 <ul style="list-style-type: none">• 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。

	コマンドまたはアクション	目的
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、デバイスを **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 モードを有効にします。 <ul style="list-style-type: none"> • 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 :	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。

	コマンドまたはアクション	目的
	Device(config-if)# ip address 192.108.1.27 255.255.255.0	
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。 <ul style="list-style-type: none"> 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	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	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	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 スヌーピングおよび Option 82 のイネーブル化

デバイス上で 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

	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。 <ul style="list-style-type: none"> 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 例： Device(config)# 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。
ステップ 4	ip dhcp snooping vlan <i>vlan-range</i> 例： Device(config)# ip dhcp snooping vlan 10	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。 <ul style="list-style-type: none"> VLANID 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。
ステップ 5	ip dhcp snooping information option 例： Device(config)# ip dhcp snooping information option	デバイスが、転送された DHCP 要求メッセージにある DHCP リレー情報（Option 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	ip dhcp snooping information option format remote-id [<i>string ASCII-string</i> <i>hostname</i>] 例： Device(config)# ip dhcp snooping information option format remote-id string acsiistring2	(任意) リモート ID 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"> 63 文字までの ASCII 文字列（スペースなし） デバイスで設定されているホスト名 (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。

	コマンドまたはアクション	目的
		デフォルトのリモート ID はデバイス MAC アドレスです。
ステップ 7	interface interface-id 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 8	ip dhcp snooping vlan vlan information option format-type circuit-id [override] string ASCII-string 例： Device(config-if)# ip dhcp snooping vlan 1 information option format-type circuit-id override string override2	(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。 <ul style="list-style-type: none"> • 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 vlan-mod-port です。 • 回線 ID は 3 ~ 63 の ASCII 文字列 (スペースなし) を設定できます。 • (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。
ステップ 9	ip dhcp snooping trust 例： Device(config-if)# ip dhcp snooping trust	(任意) インターフェイスの信頼性を trusted または untrusted 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、 no キーワードを使用します。デフォルト設定は untrusted です。
ステップ 10	ip dhcp snooping limit rate rate 例： Device(config-if)# ip dhcp snooping limit rate 100	(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。 (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。
ステップ 11	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。

	コマンドまたはアクション	目的
ステップ 12	ip dhcp snooping verify mac-address 例 : Device (config) # ip dhcp snooping verify mac-address	(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デバイスを設定します。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。
ステップ 13	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。

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	デバイスの DHCP スヌーピング設定を表示します。
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。

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 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

デバイス上で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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> デフォルトは 300 秒（5 分）です。指定できる範囲は 15 ~ 86400 秒です。

	コマンドまたはアクション	目的
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。
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 gigabitethernet1/0/1 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。 <ul style="list-style-type: none"> • <i>vlan-id</i> に指定できる範囲は 1 ~ 4904 です。 <i>seconds</i> 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、デバイス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 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。 <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
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 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

デバイス上での 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 の設定例

例 : DHCP リレーエージェントの設定

次に、DHCP リレーエージェントを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# service dhcp
Device(config)# end
```

例 : パケット転送アドレスの指定

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip helper-address 172.16.1.2
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# end
```

例 : DHCP スヌーピングおよび Option 82 のイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10
Device(config)# ip dhcp snooping information option
Device(config)# ip dhcp snooping information option format remote-id string acsiistring2
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip dhcp snooping vlan 1 information option format-type
circuit-id override string override2
Device(config-if)# ip dhcp snooping trust
Device(config-if)# ip dhcp snooping limit rate 100
Device(config-if)# exit
Device(config)# ip dhcp snooping verify mac-address
Device(config)# end
```

例 : 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

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

```

Device(config)# ip dhcp snooping database timeout 300
Device(config)# ip dhcp snooping database write-delay 15
Device(config)# exit
Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5
interface gigabitethernet1/0/1 expiry 1000

```

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

次に、DHCP サーバのポートベースのアドレス割り当てをイネーブルにする方法の例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ip dhcp use subscriber-id client-id
Device(config)# ip dhcp subscriber-id interface-name
Device(config)# interface
Device(config-if)# ip dhcp server use subscriber-id client-id
Device(config-if)# end

```

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Cisco IOS</i> リリース 15.2(7)E (<i>Catalyst</i> マイクロスイッチ) 統合プラットフォーム コマンド リファレンス

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>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。</p> <p>http://www.cisco.com/go/mibs</p>

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>	http://www.cisco.com/support

DHCP 設定の機能履歴

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。

リリース	機能	機能情報
Cisco IOS Release 15.2(7)E3k	DHCP の設定	DHCP サーバーは、デバイス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。

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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>