DHCP スヌーピングの設定

この章の内容は、次のとおりです。

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

機能のイネーブル化とグローバルなイネーブル化

DHCP スヌーピングを設定するときは、DHCP スヌーピング機能のイネーブル化と DHCP スヌーピングのグローバルなイネーブル化の違いを理解することが重要です。

機能のイネーブル化

DHCP スヌーピング機能は、デフォルトではディセーブルです。DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングまたはこれに依存する機能を設定できません。DHCP スヌーピングおよびその依存機能を設定するコマンドは、DHCP スヌーピングがディセーブルになっているときは使用できません。

DHCP スヌーピング機能をイネーブルにすると、スイッチで DHCP スヌーピング バインディング データベースの構築と維持が開始されます。DHCP スヌーピング バインディング データベースに依存する機能は、その時点から使用できるようになり、設定も可能になります。

DHCP スヌーピング機能をイネーブルにしても、グローバルにイネーブルになるわけではありません。DHCP スヌーピングをグローバルにイネーブルにするには、個別に行う必要があります。

DHCP スヌーピング機能をディセーブルにすると、スイッチから DHCP スヌーピングの設定がすべて削除されます。DHCP スヌーピングをディセーブルにして設定を維持したい場合は、DHCP スヌーピング機能をディセーブルにするのではなく、DHCP スヌーピングをグローバルにディセーブル化します。

グローバルなイネーブル化

DHCP スヌーピングのイネーブル化の実行後、DHCP スヌーピングはデフォルトでグローバルにディセーブルになります。グローバルなイネーブル化は第 2 レベルのイネーブル化です。これにより、DHCP スヌーピング バインディング データベースのイネーブル化とは別に、スイッチがアクティブに DHCP スヌーピングを実行しているかどうかを個別に制御できます。

DHCP スヌーピングをグローバルにイネーブルにすると、DHCP スヌーピングがイネーブルになっている VLAN の信頼できない各インターフェイスについて、受信した DHCP メッセージの検証が開始され、DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングをグローバルにディセーブルにすると、DHCP メッセージの検証と、信頼できないホストからの以降の要求の検証を停止します。DHCP スヌーピング バインディング データベースも削除されます。DHCP スヌーピングをグローバルにディセーブルにしても、DHCP スヌーピングの設定や、DHCP スヌーピング機能に依存するその他の機能の設定は削除されません。

信頼できる送信元と信頼できない送信元

DHCP スヌーピングがトラフィックの送信元を信頼するかどうかを設定できます。信頼できないソースの場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。こうした攻撃を防ぐため、DHCP スヌーピングは信頼できない送信元からのメッセージをフィルタリングします。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるスイッチです。これらのスイッチには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるスイッチやネットワーク外のスイッチは信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないスイッチは、信頼できない送信元です（カスタマー スイッチなど）。ホスト ポートは、信頼できない送信元です。

Cisco Nexus デバイスでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態になります。DHCP サーバインターフェイスは、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。ユーザのネットワーク内でスイッチ（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホストポートインターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（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。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングは、代行受信した DHCP メッセージから抽出した情報を使用し、ダイナミックにデータベースを構築し維持します。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

（注） DHCP スヌーピング バインディング データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

スイッチが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、データベースにエントリが追加されます。IP アドレスのリース期限が切れると、またはホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベースのエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

clear ip dhcp snooping binding コマンドを使用すると、バインディング データベースからエントリ削除できます。

DHCP スヌーピングの Option 82 データ挿入

DHCP では、多数の加入者に対する IP アドレスの割り当てを一元管理できます。Option 82 をイネーブルにすると、デバイスはネットワークに接続する加入者デバイス（およびその MAC アドレス）を識別します。加入者 LAN 上のマルチ 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。

Cisco NX-OS デバイスで Option 82 をイネーブルにすると、次のイベントが順番に発生します。

1. 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。
2. Cisco NX-OS デバイスはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（回線 ID サブオプション）が含まれます。ポート チャネルの背後にあるホストの場合、回線 ID にはポート チャネルの if_index が入力されます。

（注） vPC ピア スイッチの場合、リモート ID サブオプションには vPC スイッチの MAC アドレスが入ります。これは両方のスイッチにおいて一意です。この MAC アドレスは vPC ドメイン ID とともに計算されます。Option 82 情報は、DHCP 要求が他の vPC ピア スイッチに転送される前に最初に受信したスイッチで挿入されます。

3. 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。
4. 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、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる

IP アドレスの数を制限するポリシーなどです。DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。

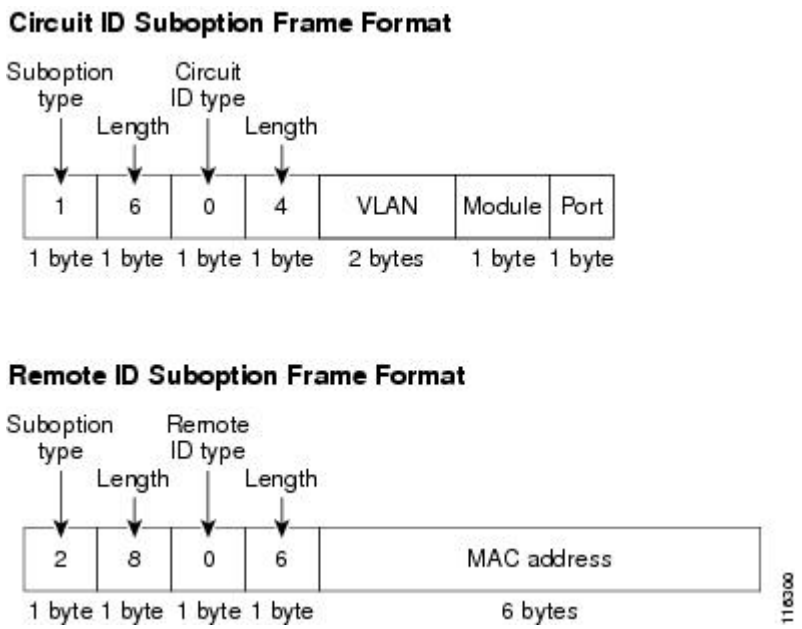
5 DHCP サーバは Cisco NX-OS デバイスに応答を送信します。Cisco NX-OS デバイスは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データを挿入したのがこのデバイス自身であることを確認します。Cisco NX-OS デバイスは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントと接続しているインターフェイスにパケットを転送します。

上記の一連のイベントが発生した場合、次の値は変更されません。

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

次の図は、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。Cisco NX-OS デバイスがこのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化され、Option 82 データの挿入と削除がイネーブルに設定された場合です。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

図 *1*：サブオプションのパケット形式



vPC 環境での DHCP スヌーピング

仮想ポート チャネル（vPC）では、2 台の Cisco NX-OS スイッチを 3 番目のスイッチに 1 つの論理ポート チャネルとして認識させることができます。3 番目のスイッチは、スイッチ、サーバ、またはポートチャネルをサポートするその他のネットワーク スイッチのいずれかにすることができます。

標準的な vPC 環境では、DHCP 要求は一方の vPC ピア スイッチに到達でき、応答は他方の vPC ピア スイッチに到達できるため、一方のスイッチには部分的な DHCP（IP-MAC）バインディング エントリが生成され、他方のスイッチにはバインディング エントリが生成されません。この問題は Cisco Fabric Service over Ethernet（CFSoE）分散を使用して、すべての DHCP パケット（要求および応答）が両方のスイッチに確実に認識されるようにすることで対処されます。これにより、vPC リンクの背後に存在するすべてのクライアントについて、両方のスイッチで同じバインディング エントリが作成および管理されるようになります。

CFSoE 分散ではまた、vPC リンク上の DHCP 要求および応答を 1 台のスイッチのみが転送するようにもできます。vPC 以外の環境では、両方のスイッチが DHCP パケットを転送します。

DHCP スヌーピング バインディング エントリの同期

ダイナミック DHCP バインディング エントリは、次のシナリオで同期される必要があります。

- リモート vPC がオンラインになったとき、その vPC リンクのすべてのバインディング エントリがピアと同期する必要があります。

- DHCP スヌーピングがピア スイッチでイネーブルの場合、リモートでアップ状態であるすべての vPC リンク用のダイナミック バインディング エントリは、ピアと同期する必要があります。

パケット検証

スイッチは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。次の条件が発生（この場合パケットは破棄される）しない限り、スイッチでは、DHCP パケットが転送されます。

- 信頼できないインターフェイスで DHCP 応答パケット（DHCPACK、DHCPNAK、または DHCPOFFER などのパケット）を受信した場合。
- 信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- リレー エージェントの IP アドレス（0.0.0.0 以外）を含む DHCP パケットを受信した場合。

さらに、DHCP パケットの厳密な検証をイネーブルにすることもできます。これにより、DHCP パケットのオプション フィールドが確認されます。これには、オプション フィールドの最初の 4 バイト内の「マジック クッキー」値も含まれます。デフォルトでは、厳密な検証はディセーブルになっています。これを **ip dhcp packet strict-validation** コマンドによりイネーブルにすると、DHCP スヌーピングで無効なオプション フィールドを含むパケットを処理した場合に、パケットがドロップされます。

DHCP リレー エージェントの概要

DHCP リレー エージェント

DHCP リレー エージェントを実行するようにデバイスを設定できます。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 パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCP メッセージを受信すると、新規の DHCP メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ アドレスを設定し（DHCP パケットの giaddr フィールド）、パケットにリレー エージェント情報のオプション（Option 82）を追加して（設定されている場合）、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Option 82 をイネーブルにすると、デバイスはデフォルトでバイナリの ifindex 形式を使用します。必要に応じて Option 82 設定を変更して、代わりに符号化ストリング形式を使用できます。デバイスがリレー エージェントとして機能し、Option 82 を挿入するように設定されると、回線 ID は、異なるポートに接続した場合でもすべてのホストで同じになります。クライアントによって挿入される一意の回線 ID を保持するには、**ip dhcp relay sub-option circuit-id customized** コマンドを使用できます。

（注） デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態で要求と一緒に転送します。

DHCP リレー エージェントに対する VRF サポート

DHCP ブロードキャスト メッセージを Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスのクライアントから別の VRF の DHCP サーバに転送するように、DHCP リレー エージェントを設定できます。単一の DHCP サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。

DHCP リレー エージェントに対する VRF サポートをイネーブルにするには、DHCP リレー エージェントに対する Option 82 をイネーブルにする必要があります。

DHCP リレー アドレスと VRF 情報を設定したインターフェイスに DHCP 要求が着信した場合、DHCP サーバのアドレスが、別の VRF のメンバであるインターフェイスのネットワークに属するものであれば、デバイスは要求に Option 82 情報を挿入し、サーバの VRF の DHCP サーバにそれが転送されます。Option 82 情報は次のとおりです。

VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

リンクの選択

DHCP 要求を受信するインターフェイスのサブネット アドレス。

サーバ識別子オーバーライド

DHCP 要求を受信するインターフェイスの IP アドレス。

（注） DHCP サーバは、VPN 識別子、リンクの選択、サーバ識別子オーバーライドの各オプションをサポートする必要があります。

デバイスは DHCP 応答メッセージを受信すると、Option 82 情報を取り除き、クライアントの VRF の DHCP クライアントに応答を転送します。

DHCP リレー バインディング データベース

リレー バインディングは、リレー エージェントのアドレスおよびサブネットに、DHCP または BOOTP クライアントを関連付けるエントリです。各リレー バインディングは、クライアントの MAC アドレス、アクティブなリレー エージェント アドレス、アクティブなリレー エージェント アドレス マスク、クライアントが接続されている論理および物理インターフェイス、giaddr リトライ回数、および合計リトライ回数を格納します。giaddr リトライ回数は、リレー エージェント アドレスに送信される要求パケットの数です。合計リトライ回数は、リレー エージェントによって送信される要求パケットの合計数です。1 つのリレー バインディング エントリが、各 DHCP または BOOTP クライアントに対して維持されます。

（注） DHCP スマート リレーをグローバルにイネーブルにするか、または任意のスイッチのインターフェイス レベルでイネーブルにする場合、すべてのスイッチのリレー バインディングは vPC ピアと同期する必要があります。

DHCPv6 リレー エージェントの概要

DHCPv6 リレー エージェント

DHCPv6 リレー エージェントを実行するようにデバイスを設定できます。DHCPv6 リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCPv6 メッセージを受信すると、新規の DHCPv6 メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ アドレス（DHCPv6 パケットの giaddr フィールド）をセットし、DHCPv6 サーバに転送します。

DHCPv6 リレー エージェントに対する VRF サポート

DHCPv6 ブロードキャスト メッセージを仮想ルーティング/転送（VRF）インスタンスのクライアントから別の VRF の DHCPv6 サーバに転送するように、DHCPv6 リレー エージェントを設定できます。単一の DHCPv6 サーバを使用して複数 VRF のクライアントに DHCPv6 サポートを提供できるため、VRF ごとに 1 つずつではなく、単一の IP アドレス プール使用することで、IP アドレスを節約できます。

Lightweight DHCPv6 リレー エージェントの概要

Lightweight DHCPv6 リレー エージェント

1 つ以上のルータへの IPv6 ノードのアグリゲーションには、さまざまなリンク レイヤ ネットワーク トポロジがあります。単一リンクに多くのノードがあるレイヤ 2 アグリゲーション ネットワーク（IEEE 802.1D ブリッジングなど）では、DHCP バージョン 6（DHCPv6）サーバまたは DHCP リレー エージェントは通常、DHCP クライアントがどのようにネットワークに接続されているかを認識しません。Cisco NX-OS リリース 7.3(0)N1(1) 以降では、デバイスのインターフェイスを設定して、クライアントとサーバ間の DHCPv6 メッセージを転送する Lightweight DHCPv6 リレー エージェント（LDRA）を実行できます。

LDRA 機能は主に DHCPv6 メッセージ交換にリレー エージェント オプションを挿入してクライアント側のインターフェイスを特定するために使用されます。LDRA は、クライアントおよびDHCPv6 リレー エージェントまたはサーバと同じ IPv6 リンクに存在します。

VLAN およびインターフェイスの LDRA

VLAN およびインターフェイスの LDRA を設定できます。LDRA はデフォルトでは有効になっていません。LDRA を有効にするには、グローバルおよびインターフェイス レベルで有効にする必要があります。インターフェイスは、クライアント側の信頼できるインターフェイス、クライアント側の信頼できないインターフェイス、サーバ側インターフェイスとして設定する必要があります。すべてのクライアント側インターフェイスは、信頼できるインターフェイス、または信頼できないインターフェイスとして設定する必要があります。デフォルトでは、LDRA のすべてのクライアント側インターフェイスが信頼できないインターフェイスとして設定されます。クライアント側インターフェイスが信頼できないインターフェイスであると考えられる場合、LDRA はクライアント側インターフェイスから受信した RELAY-FORWARD タイプのメッセージを破棄します。

VLAN の LDRA 設定は、クライアント側の信頼できる VLAN またはクライアント側の信頼できない VLAN として設定する必要があります。VLAN の LDRA 機能を設定すると、VLAN 内のすべてのポートやインターフェイスにこの機能が設定されます。ただし、VLAN のインターフェイスをクライアント側の信頼できないインターフェイスとして設定し、VLAN をクライアント側の信頼できる VLAN として設定した場合、インターフェイスの設定が VLAN の設定よりも優先されます。VLAN の少なくとも 1 つのインターフェイスをサーバ側のインターフェイスとして設定する必要があります。

Lightweight DHCPv6 リレー エージェントの注意事項と制約事項

- LDRA を実装するアクセス ノードは、IPv6 制御またはルーティングをサポートしていません。

- インターフェイスまたはポートは、同時にクライアント側とサーバ側の両方として設定することはできません。
- バーチャル ポート チャネルをサポートするには、LDRA 設定を vPC ピア で対称にする必要があります。
- LDRA は Cisco Fabricpath をサポートします。

vIP HSRP の拡張機能

Cisco NX-OS リリース 7.2(0)N1(1) 以降、vIP HSRP の拡張機能は、インターフェイス サブネットと異なるサブネットに存在する HSRP VIP 設定のサポートを提供します。この機能は IPv4 のみに適用されます。IPv6 には適用されません。次の拡張機能を使用できます。

- VLAN 設定へのスタティック ルートが VIP サブネットのホストを参照する際にホストの SUP から VIP で送信元への ARP を強化します。
- この機能が有効になっていると、定期的な ARP 同期が VPC ピアをサポートします。
- DHCP サーバとのすべての通信に L3 送信元アドレスおよびゲートウェイ アドレスとして VIP アドレスの使用が可能になります。
- 機能が有効になっていると、SVI IP の代わりに送信元を VIP をとして DHCP パケットをリレーするために DHCP リレー エージェントを強化します。

DHCP スヌーピングの注意事項および制約事項

DHCP スヌーピングを設定する場合は、次の注意事項および制約事項を考慮してください。

- DHCP スヌーピング データベースには 2,000 のバインディングを格納できます。
- DHCP をグローバルにイネーブル化し、さらに少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにするまで、DHCP スヌーピングはアクティブになりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するスイッチが設定され、イネーブルになっていることを確認してください。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL（VACL）が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- DHCP スヌーピングおよび DHCP リレー機能は、同一の VLAN ポート上ではサポートされません。
- デフォルトで、DHCP バインディングは、スイッチの再起動後に永続的に保存されません。スイッチの再起動後にも永続的なバインディングを保持するには、**copy r s** コマンドを使用

します。**copy r s** コマンドが発行されると、その時点で存在するすべてのバインディングは、スイッチの再起動後も永続的な状態になります。

- vPC リンク内のスイッチ間で DHCP 設定が同期されていることを確認します。同期されていないと、ランタイム エラーが発生し、パケットがドロップされる場合があります。
- リモート DHCP サーバとローカル DHCP サーバの両方を使用するには、DHCP リレー機能を設定し、ローカル DHCP サーバのユニキャスト アドレスを定義し、またはローカル DHCP サーバが常駐するサブネットのローカル ブロードキャスト アドレスを設定する必要があります。DHCP サーバのユニキャスト アドレスを定義せず、またはサブネットのローカル ブロードキャストアドレスを設定しない場合、ローカル DHCP パケットは配信できません。たとえば、この状況は SVI に IP DHCP アドレスを適用する場合に発生することがあります。
- インターフェイスに DHCPv6 サーバ アドレスを設定する場合、宛先インターフェイスはグローバル IPv6 アドレスと共に使用できません。

次の注意事項および制約事項は、FabricPath を含む実装に適用されます。

- DHCP スヌーピングは、CE-Fabric 境界スイッチ上でイネーブルにする必要があります。
- アクセス レイヤでネットワークを保護するために、DHCP スヌーピングはすべてのアクセス レイヤ スイッチ上でイネーブルになっています。
- DHCP は、FabricPath モードで設定されたポート上のバインディング エントリを学習しません。DHCP スヌーピングは、すべてのアクセス レイヤ スイッチで手動でイネーブルにする必要があります。
- ダイナミック ARP インスペクション（DAI）がイネーブルになっている場合、FabricPath ポート上で受信された ARP パケットは許可されます。
- FabricPath モードでは、ポート上で IPSG をイネーブルにすることはできません。
- システムのすべての FabricPath ポートは、信頼できるポートとして設定する必要があります。
- FabricPath の DHCP スヌーピングは、スイッチに設定されたすべての VLAN でイネーブルにする必要があります。スイッチ上のすべての VLAN の FabricPath をイネーブルにしない場合、DHCP がイネーブルにされていない VLAN で DHCP パケットはドロップされます。

  DHCP パケットがドロップされないようにするには、次の設定すべてを実行する必要があります。

  - **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにします。
  - **feature-set fabricpath** および **feature-set fabricpath** コマンドを使用して FabricPath 機能セットをインストールします。
  - **ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにイネーブルにします。
  - **ip dhcp snooping vlan***vlan* コマンドを使用して、スイッチの設定済み VLAN ごとに DHCP スヌーピングをイネーブルにします。

vIP HSRP 強化の注意事項と制約事項

- この機能は VPC のトポロジと組み合わせて HSRP でのみ動作します。HSRP スタンバイが VPC ペアでないシナリオでは、VPC 以外の場合で定期的な隣接関係の同期サポートがないため、この機能は動作しません。
- この機能は、IPv4 のみに適用され、IPv6 には適用されません。
- この機能のサポートは、通常の HSRP 専用であり、エニーキャスト HSRP 用ではありません。そのため、エニーキャスト HSRP がイネーブルの場合、この機能は動作しません。
- HSRP アクティブ/スタンバイ ボックスから VIP サブネット宛てに SUP が生成した IP トラフィック（たとえば、ping/traceroute/ICMP エラー パケット）は、引き続き vIP ではなく IPv4 SVI インターフェイス IP を送信元とします。ping と traceroute のループバック IP を使用して明示的にソースにするには、source キーワードとともにループバック IP を指定できます。
- VIP のサブネットでエントリを作成するためのスタティック ARP 設定はサポートされていません。
- DHCP リレー エージェントは DHCP サーバとの通信に常にプライマリ VIP アドレスを使用します。DHCP リレー エージェントは、プライマリ VIP が使用できる限りセカンダリ VIP アドレスの使用を考慮しません。
- inter-vrf のケースでは DHCP リレー エージェントの動作が異なり、DHCP パケットの Option-82 情報を使用する必要があります。DHCP サーバとクライアントは同じ VRF になります。inter-vrf リレーのための VIP の使用はサポートされません。

DHCP スヌーピングのデフォルト設定

次の表に、DHCP スヌーピング パラメータのデフォルト設定を示します。

表 *1*：*DHCP* スヌーピング パラメータのデフォルト値

パラメータ（Parameters）	デフォルト
DHCP スヌーピング機能	ディセーブル
DHCP スヌーピングのグローバルなイネーブル化	No
DHCP スヌーピング VLAN	なし
DHCP スヌーピングの Option 82 サポート	ディセーブル
DHCP スヌーピング信頼状態	信頼できない
DHCP リレー エージェントに対する VRF サポート	ディセーブル

パラメータ（Parameters）	デフォルト
DHCPv6 リレー エージェントに対する VRF サポート	ディセーブル
DHCP リレー エージェント	ディセーブル
DHCPv6 リレー エージェント	ディセーブル
DHCPv6 relay option type cisco	ディセーブル

DHCP スヌーピングの設定

DHCP スヌーピングの最小設定

1 DHCP スヌーピング機能をイネーブルにします。

2

手順

	コマンドまたはアクション	目的
ステップ 1	DHCP スヌーピング機能をイネーブルにします。	DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングを設定できません。 詳細については、DHCP スヌーピング機能のイネーブル化またはディセーブル化, （15 ページ）を参照してください。
ステップ 2	DHCP スヌーピングをグローバルにイネーブルにします。	詳細については、DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化, （15 ページ）を参照してください。
ステップ 3	少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。	デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。 詳細については、VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化, （16 ページ）を参照してください。
ステップ 4	DHCP サーバとスイッチが、信頼できるインターフェイスを使用して接続されていることを確認します。	詳細については、インターフェイスの信頼状態の設定, （19 ページ）を参照してください。

DHCP スヌーピング機能のイネーブル化またはディセーブル化

スイッチの DHCP スヌーピング機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP スヌーピングはディセーブルです。

はじめる前に

DHCP スヌーピング機能をディセーブルにすると、DHCP スヌーピングの設定がすべて消去されます。DHCP スヌーピングをオフにして DHCP スヌーピングの設定を維持したい場合は、DHCP をグローバルにディセーブル化します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **feature dhcp** 例： `switch(config)# feature dhcp`	DHCP スヌーピング機能をイネーブルにします。**no** オプションを使用すると、DHCP スヌーピング機能がディセーブルになり、DHCP スヌーピングの設定がすべて消去されます。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

スイッチに対して DHCP スヌーピング機能のグローバルなイネーブル化またはディセーブル化が可能です。DHCP スヌーピングをグローバルにディセーブルにすると、DHCP スヌーピングの実

行や DHCP メッセージのリレーはスイッチで停止されますが、DHCP スヌーピングの設定は維持されます。

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**[no] ip dhcp snooping** 例： `switch(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。**no** オプションを使用すると DHCP スヌーピングがディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLANに対するDHCPスヌーピングのイネーブル化またはディセーブル化

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。

はじめる前に

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

DHCP スヌーピングがイネーブルになっていることを確認してください。

（注） DHCP スヌーピングを使用して設定を行っている VLAN で VACL が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ipdhcp snooping vlan** *vlan-list* 例： `switch(config)# ip dhcp snooping vlan 100,200,250-252`	*vlan-list* で指定する VLAN の DHCP スヌーピングをイネーブルにします。**no** オプションを使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Option 82 データの挿入および削除のイネーブル化またはディセーブル化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除をイネーブルまたはディセーブルにできます。

はじめる前に

デフォルトでは、スイッチは DHCP パケットに Option 82 情報を挿入しません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ip dhcp snooping information option** 例： `switch(config)# ip dhcp snooping information option`	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。**no** オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP スヌーピング機能では、DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ip dhcp packet strict-validation** 例： `switch(config)# ip dhcp packet strict-validation`	DHCP スヌーピング機能で、DHCP パケットの厳密な検証をイネーブルにします。**no** オプションを使用すると、DHCP パケットの厳密な検証がディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの信頼状態の設定

各インターフェイスが DHCP メッセージの送信元として信頼できるかどうかを設定できます。DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

はじめる前に

デフォルトでは、すべてのインターフェイスは信頼できません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	次のいずれかのコマンドを入力します。 • **interfaceethernet***port*/*slot* • **interfaceport-channel***channel-number*	• 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。*port*/*slot* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 イーサネット インターフェイスです。 • 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。*port*/*slot* は、DHCP

	コマンドまたはアクション	目的

	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スヌーピングで trusted または untrusted に設定するレイヤ2ポートチャネルインターフェイスです。

ステップ 3	**[no] ip dhcp snooping trust** 例： `switch(config-if)# ip dhcp snooping trust`	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	**showrunning-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

DHCP リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP リレー エージェントはイネーブルです。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**config t**
	例：
	`switch# config t`
	`switch(config)#`
		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 2	**[no] ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレーエージェントをイネーブルにします。**no** オプションを使用すると、リレーエージェントがディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除をイネーブルまたはディセーブルにできます。

デフォルトでは、DHCP リレー エージェントは DHCP パケットに Option 82 情報を挿入しません。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**[no] ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレー機能をイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	**[no] ip dhcp relay information option** 例： `switch(config)# ip dhcp relay information option`	DHCP リレー エージェントによって転送されるパケットに対する Option 82 情報の挿入および削除をイネーブルにします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。**no** オプションを使用すると、この動作がディセーブルになります。

	コマンドまたはアクション	目的
ステップ 4	[no] ip dhcp relay sub-option circuit-id customized 例： switch(config)# ip dhcp relay sub-option circuit-id customized	（任意） クライアントによって挿入される一意の回線 ID の保持をイネーブルにします。no オプションを使用すると、この動作がディセーブルになります。 （注） デフォルトでは、回線 ID は、異なるポートに接続した場合でもすべてのホストで同じです。
ステップ 5	show ip dhcp relay 例： switch(config)# show ip dhcp relay	（任意） DHCP リレーの設定を表示します。
ステップ 6	show running-config dhcp 例： switch(config)# show running-config dhcp	（任意） DHCP 設定を表示します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF インスタンスの DHCP サーバにリレーできるよう、デバイスを設定することができます。

はじめる前に

DHCP リレー エージェントの Option 82 をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 2	**[no] ip dhcp relay information option vpn** 例： `switch(config)# ip dhcp relay information option vpn`	DHCP リレー エージェントに対して VRF サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	**[no] ip dhcp relay sub-option type cisco** 例： `switch(config)# ip dhcp relay sub-option type cisco`	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェント Option 82 サブオプションを設定する場合は、DHCP をイネーブルにして、シスコ独自の番号である 150、152、および 151 を使用します。**no** オプションを使用すると、DHCP では、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID サブオプションに対して、RFC 番号 5、11、151 が使用されるようになります。
ステップ 4	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 3 インターフェイスの DHCP リレー エージェントに対するサブネット ブロードキャスト サポートのイネーブル化またはディセーブル化

クライアントからのサブネットのブロードキャスト IP アドレスに DHCP パケットのリレーをサポートするように、デバイスを設定できます。この機能がイネーブルの場合、VLAN ACL（VACL）は、IP ブロードキャスト パケット、すべてのサブネット ブロードキャスト（プライマリ サブネット ブロードキャストおよびセカンダリ サブネット ブロードキャスト）パケットを許容します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 2	**interface** *interface slot/port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		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。*slot/port* は、DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルまたはディセーブルにするインターフェイスです。

ステップ 3	[**no**] **ip dhcp relay subnet-broadcast** 例： `switch(config-if)# ip dhcp relay subnet-broadcast`	DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**showip dhcp relay** 例： `switch# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 7	**showrunning-config dhcp** 例： `switch# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スタティック バインディングの作成

レイヤ 2 インターフェイスにスタティック DHCP ソース バインディングを作成できます。

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**ip source binding** *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*} 例： `switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3`	レイヤ 2 イーサネット インターフェイスにスタティックな送信元アドレスをバインドします。

	コマンドまたはアクション	目的
ステップ 3	**show ip dhcp snooping binding** 例： `switch(config)# ip dhcp snooping binding`	（任意） DHCP スヌーピングのスタティックおよびダイナミック バインディングを示します。
ステップ 4	**show ip dhcp snooping binding dynamic** 例： `switch(config)# ip dhcp snooping binding dynamic`	（任意） DHCP スヌーピングのダイナミック バインディングを示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイス 2/3 上に、VLAN 100 に関連付ける固定 IP ソース エントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

DHCPv6 リレー エージェントの設定

DHCPv6 リレー エージェントのイネーブル化またはディセーブル化

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ipv6 dhcp relay** 例： `switch(config)# ipv6 dhcp relay`	DHCPv6 リレー エージェントをイネーブルにします。**no** オプションを使用すると、リレー エージェントがディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCPv6 要求を、別の VRF の DHCPv6 サーバにリレーする機能をサポートするように、デバイスを設定できます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントがイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ipv6 dhcp relay option vpn** 例： `switch(config)# ipv6 dhcp relay option vpn`	DHCPv6 リレー エージェントに対して VRF サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **ipv6 dhcp relay option type cisco** 例： `switch(config)# ipv6 dhcp relay option type cisco`	これにより、DHCPv6 リレー エージェントが、ベンダー固有オプションの一部として仮想サブネット選択（VSS）の詳細情報を挿入します。**no** オプションを使用すると、DHCPv6 リレー エージェントが VSS 詳細情報を、VSS オプションの一部として（68）挿入します。これは、RFC-6607 で定義された動作です。このコマンドは、RFC-6607 に対応していないものの、クライアント VRF 名に基づいた IPv6 アドレスを割り当てる DHCPv6 サーバを使用する場合に役立ちます。
ステップ 4	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 リレー送信元インターフェイスの設定

DHCPv6リレーエージェントの送信元インターフェイスを設定できます。デフォルトでは、DHCPv6 リレー エージェントは発信パケットの送信元アドレスとしてリレー エージェント アドレスを使用します。送信元インターフェイスを設定すると、リレーされたメッセージの送信元アドレスとして、より安定したアドレス（ループバック インターフェイス アドレスなど）を使用することができます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントがイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	[**no**] **ipv6 dhcp relay source-interface***interface* 例： `switch(config)# ipv6 dhcp relay source-interface loopback 2`	DHCPv6 リレー エージェントの送信元インターフェイスを設定します。 （注） DHCPv6 リレー送信元インターフェイスは、グローバルに、インターフェイスごとに、またはその両方に設定できます。グローバルおよびインターフェイス レベルの両方が設定されている場合は、インターフェイス レベルの設定がグローバル設定を上書きします。
ステップ 3	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Lightweight DHCPv6 リレー エージェントの設定

インターフェイスの Lightweight DHCPv6 リレー エージェントの設定

次のタスクを実行してインターフェイスの Lightweight DHCPv6 リレー エージェント（LDRA）を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# 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 2	**[no] ipv6 dhcp ldra** 例： `switch(config)# ipv6 dhcp ldra`	LDRA 機能をグローバルにイネーブルにします。
ステップ 3	**interface***slot*/*port* 例： `switch(config)# interface ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、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 4	**switchport** 例： `switch(config-if)# switchport`	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードに切り替えます。
ステップ 5	**[no] ipv6 dhcp-ldra{client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}**	指定されたインターフェイスまたはポートの LDRA 機能をイネーブルにします。**no** オプションを指定すると、LDRA 機能が無効になります。

	コマンドまたはアクション	目的
	例： `switch(config-if)# ipv6 dhcp-ldra server-facing`	（注） **client-facing-trusted** は、クライアント側のインターフェイスまたはポートを信頼できるとして指定します。信頼できるポートは DHCPv6 パケットを許可し、これらは LDRA オプションによってカプセル化されます。 **client-facing-untrusted** は、クライアント側のインターフェイスまたはポートを信頼できないとして指定します。信頼できないポートは LDRA 機能を実行しますが、受信したリレー転送パケットのみドロップします。 **client-facing-disable** キーワードは、インターフェイスまたはポートの LDRA 機能を無効にします。無効ポートは、DHCPv6 パケットのレイヤ 2 フォワーディングを実行します。 **server-facing** キーワードは、インターフェイスまたはポートをサーバ側として指定します。サーバ側ポートは、サーバからの応答パケットを許可します。

VLAN の Lightweight DHCPv6 リレー エージェントの設定

次のタスクを実行して VLAN の Lightweight DHCPv6 リレー エージェント（LDRA）を設定します。

はじめる前に

VLAN に IP アドレスが割り当てられていないことを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# 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 2	**[no] ipv6 dhcp ldra** 例： `switch(config)# ipv6 dhcp ldra`	LDRA 機能をグローバルにイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**[no] ipv6 dhcp-ldra attach–policyvlan***vlan-id*{**client-facing-trusted | client-facing-untrusted}** 例： `switch(config)# ipv6 dhcp-ldra attach-policy vlan 25 client-facing-trusted`	指定した VLAN で LDRA 機能をイネーブルにします。**no** オプションを指定すると、LDRA 機能が無効になります。 （注） **client-facing-trusted** キーワードは、VLAN に関連するすべてのポートまたはインターフェイスをクライアント側の信頼できるポートとして設定します。**client-facing-untrusted** キーワードは、VLAN に関連するすべてのポートまたはインターフェイスをクライアント側の信頼できないポートとして設定します。

VIP アドレスを使用する DHCP リレー エージェントの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **[no] ip dhcp relay source-address hsrp**	VIP をグローバルで使用するために DHCP リレー エージェントを有効または無効にします。
ステップ 3	switch(config)# **interface***type number*	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	switch(config-if)# **[no] ip dhcp relay source-address hsrp**	VIP を L3 インターフェイス レベルで使用するために DHCP リレー エージェントを有効または無効にします。
ステップ 5	switch(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 6	（オプション）switch# **show ip dhcp relay**	DHCP リレーの設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	（オプション）switch# **show hsrp brief**	Hot Standby Router Protocol（HSRP）情報の概要を表示します。

次の例では、VIP アドレスを使用して DHCP リレー エージェントを有効化します。

```
interface vlan 500
ip address 5.5.5.5/24
ip dhcp relay source-address hsrp
ip dhcp relay address 100.100.100.100
hsrp 10
ip 17.17.17.17/28
ip 15.15.15.20/28 secondary
```

DHCP スヌーピング設定の確認

DHCP スヌーピングの設定情報を表示するには、次のいずれかの作業を行います。これらのコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『System Management Configuration Guide』を参照してください。

コマンド	目的
show running-config dhcp	DHCP スヌーピング設定を表示します。
show ip dhcp relay	DHCP リレーの設定を表示します。
show ipv6 dhcp relay [**interface***interface*]	DHCPv6 リレーのグローバルまたはインターフェイス レベルの設定を表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。

DHCP バインディングの表示

DHCP スタティックおよびダイナミック バインディング テーブルを表示するには、**show ip dhcp snooping binding** コマンドを使用します。DHCP ダイナミック バインディング テーブルを表示するには、**show ip dhcp snooping binding dynamic** を使用します。

このコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『*System Management Configuration Guide*』を参照してください。

次に、スタティック DHCP バインディングを作成してから、**show ip dhcp snooping binding** コマンドを使用してバインディングを確認する例を示します。

```
switch# configuration terminal
switch(config)# ip source binding 10.20.30.40 0000.1111.2222 vlan 400 interface port-channel
 500

switch(config)# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  --------------
00:00:11:11:22:22   10.20.30.40      infinite  static       400   port-channel500
```

LDRA 情報の表示とクリア

Lightweight DHCPv6 リレー エージェント（LDRA）の情報を表示するには、この表のいずれかのコマンドを使用します。

コマンド	目的
show ipv6 dhcp-ldra	LDRA 設定の詳細を表示します。
show ipv6 dhcp-ldra statistics	DHCP セッションを開始する前後の LDRA 設定統計情報を表示します。
show ipv6 dhcp-ldra statistics vlan*vlan-id*	指定した VLAN の LDRA 設定統計情報を表示します。
show ipv6 dhcp-ldra statistics interface*interface-id*	指定したインターフェイスの LDRA 設定統計情報を表示します。

DHCPv6 LDRA の固有の統計情報をクリアするには、**clear ipv6 dhcp-ldra statistics** コマンドを使用します。

LDRA 設定の詳細の表示

次の例では、スイッチの LDRA 設定の詳細を示します。

```
switch(config)# show ipv6 dhcp-ldra

DHCPv6 LDRA is Enabled.


DHCPv6 LDRA policy: client-facing-trusted
Target: Ethernet1/1

DHCPv6 LDRA policy: client-facing-untrusted
Target: vlan 102 vlan 103

DHCPv6 LDRA policy: server-facing
Target: port-channel101
```

LDRA 統計情報の表示

次の例は、LDRA の統計情報を表示します。

```
switch(config)# show ipv6 dhcp-ldra statistics

PACKET STATS:
------------------------------------------------------------
Message Type                    Rx         Tx      Drops  |
------------------------------------------------------------
SOLICIT                          0          0          0  |
ADVERTISE                        0          0          0  |
REQUEST                          0          0          0  |
CONFIRM                          0          0          0  |
RENEW                            0          0          0  |
REBIND                           0          0          0  |
REPLY                            0          0          0  |
RELEASE                          0          0          0  |
DECLINE                          0          0          0  |
RECONFIGURE                      0          0          0  |
INFORMATION_REQUEST              0          0          0  |
RELAY_FORWARD                    0          0          0  |
RELAY_REPLY                      0          0          0  |
------------------------------------------------------------
Total                            0          0          0  |
------------------------------------------------------------

CFS STATS:
------------------------------------------------------------
Message Type                    Rx         Tx      Drops  |
------------------------------------------------------------
SOLICIT                          0          0          0  |
ADVERTISE                        0          0          0  |
REQUEST                          0          0          0  |
CONFIRM                          0          0          0  |
RENEW                            0          0          0  |
REBIND                           0          0          0  |
REPLY                            0          0          0  |
RELEASE                          0          0          0  |
DECLINE                          0          0          0  |
RECONFIGURE                      0          0          0  |
INFORMATION_REQUEST              0          0          0  |
RELAY_FORWARD                    0          0          0  |
RELAY_REPLY                      0          0          0  |
------------------------------------------------------------
Total                            0          0          0  |
------------------------------------------------------------
Non-DHCPv6 LDRA Packets:
------------------------------------------------------------
Total Packets Received:                                  0
Total Packets Forwarded:                                 0
Total Packets Dropped:                                   0

------------------------------------------------------------
DHCPv6 LDRA DROPS
------------------------------------------------------------
Invalid Message Type:                                    0
Max hops exceeded:                                       0
Relay Forward Received on Untrusted port:                0
Packet received over MCT:                                0
Invalid Message Type on Client facing port:              0
No Server Port Present:                                  0
```

次の例では、Ethernet1/1 インターフェイスの LDRA の統計情報を表示します。

```
SWITCH(config)# show ipv6 dhcp-ldra statistics interface e1/1
INTERFACE: Ethernet1/1

PACKET STATS:
------------------------------------------------------------
Message Type                    Rx         Tx      Drops  |
------------------------------------------------------------
SOLICIT                          0          0          0  |
```

```
ADVERTISE                      0          0          0  |
REQUEST                        0          0          0  |
CONFIRM                        0          0          0  |
RENEW                          0          0          0  |
REBIND                         0          0          0  |
REPLY                          0          0          0  |
RELEASE                        0          0          0  |
DECLINE                        0          0          0  |
RECONFIGURE                    0          0          0  |
INFORMATION_REQUEST            0          0          0  |
RELAY_FORWARD                  0          0          0  |
RELAY_REPLY                    0          0          0  |
------------------------------------------------------------
Total                          0          0          0  |
------------------------------------------------------------

CFS STATS:
------------------------------------------------------------
Message Type                 Rx         Tx      Drops  |
------------------------------------------------------------
SOLICIT                        0          0          0  |
ADVERTISE                      0          0          0  |
REQUEST                        0          0          0  |
CONFIRM                        0          0          0  |
RENEW                          0          0          0  |
REBIND                         0          0          0  |
REPLY                          0          0          0  |
RELEASE                        0          0          0  |
DECLINE                        0          0          0  |
RECONFIGURE                    0          0          0  |
INFORMATION_REQUEST            0          0          0  |
RELAY_FORWARD                  0          0          0  |
RELAY_REPLY                    0          0          0  |
------------------------------------------------------------
Total                          0          0          0  |
------------------------------------------------------------
Non-DHCPv6 LDRA Packets:
------------------------------------------------------------
Total Packets Received:                                 0
Total Packets Forwarded:                                0
Total Packets Dropped:                                  0

------------------------------------------------------------
DHCPv6 LDRA DROPS
------------------------------------------------------------
Invalid Message Type:                                   0
Max hops exceeded:                                      0
Relay Forward Received on Untrusted port:               0
Packet received over MCT:                               0
Invalid Message Type on Client facing port:             0
No Server Port Present:                                 0
```

次の例では、VLAN 101 の LDRA の統計情報を表示します。

```
SWITCH(config)# show ipv6 dhcp-ldra statistics vlan 101
VLAN: 101

PACKET STATS:
------------------------------------------------------------
Message Type                 Rx         Tx      Drops  |
------------------------------------------------------------
SOLICIT                        0          0          0  |
ADVERTISE                      0          0          0  |
REQUEST                        0          0          0  |
CONFIRM                        0          0          0  |
RENEW                          0          0          0  |
REBIND                         0          0          0  |
REPLY                          0          0          0  |
RELEASE                        0          0          0  |
DECLINE                        0          0          0  |
RECONFIGURE                    0          0          0  |
INFORMATION_REQUEST            0          0          0  |
RELAY_FORWARD                  0          0          0  |
RELAY_REPLY                    0          0          0  |
```

```
-------------------------------------------------------------
Total                          0          0          0  |
-------------------------------------------------------------

CFS STATS:
-------------------------------------------------------------
Message Type                 Rx         Tx      Drops  |
-------------------------------------------------------------
SOLICIT                        0          0          0  |
ADVERTISE                      0          0          0  |
REQUEST                        0          0          0  |
CONFIRM                        0          0          0  |
RENEW                          0          0          0  |
REBIND                         0          0          0  |
REPLY                          0          0          0  |
RELEASE                        0          0          0  |
DECLINE                        0          0          0  |
RECONFIGURE                    0          0          0  |
INFORMATION_REQUEST            0          0          0  |
RELAY_FORWARD                  0          0          0  |
RELAY_REPLY                    0          0          0  |
-------------------------------------------------------------
Total                          0          0          0  |
-------------------------------------------------------------
Non-DHCPv6 LDRA Packets:
-------------------------------------------------------------
Total Packets Received:                                  0
Total Packets Forwarded:                                 0
Total Packets Dropped:                                   0

-------------------------------------------------------------
DHCPv6 LDRA DROPS
-------------------------------------------------------------
Invalid Message Type:                                    0
Max hops exceeded:                                       0
Relay Forward Received on Untrusted port:                0
Packet received over MCT:                                0
Invalid Message Type on Client facing port:              0
No Server Port Present:                                  0
```

DHCP スヌーピング バインディング データベースのクリア

DHCP スヌーピング バインディング データベースからエントリを削除できます。1 つのエントリ、インターフェイスに関連するすべてのエントリ、データベース内のすべてのエントリなどを削除することが可能です。

はじめる前に

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ip dhcp snooping binding** 例： `switch# clear ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	**clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] 例： `switch# clear ip dhcp snooping binding interface ethernet 1/4`	（任意） DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	**clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*] 例： `switch# clear ip dhcp snooping binding interface port-channel 72`	（任意） DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。
ステップ 4	**clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot*/*port*[.*subinterface-number* | **port-channel** *channel-number*[.*subchannel-number*] } 例： `switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11`	（任意） DHCP スヌーピング バインディング データベースから、特定のエントリをクリアします。
ステップ 5	**show ip dhcp snooping binding** 例： `switch# show ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースを表示します。

DHCP リレー統計情報のクリア

グローバル DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics** コマンドを使用します。

特定のインターフェイスの DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics interface** *interface* コマンドを使用します。

clear ip dhcp relay statistics interface *interface* **serverip** *ip-address* [**use-vrf** *vrf-name*] コマンドを使用して、特定のインターフェイスのサーバ レベルでの DHCP リレー統計情報をクリアします。

DHCPv6 リレー統計情報のクリア

グローバル DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics** コマンドを使用します。

特定のインターフェイスの DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics interface***interface* コマンドを使用します。

clear ipv6 dhcp relay statistics interface*interface***server-ip***ip-address* [**use-vrf***vrf-name*] コマンドを使用して、特定のインターフェイスのサーバ レベルでの DHCPv6 リレー統計情報をクリアします。

DHCP のモニタリング

DHCP スヌーピングをモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp relay statistics[**interface***interface* [**serverip***ip-address* [**use-vrf***vrf-name*]]] コマンドを使用して、グローバル、サーバ、またはインターフェイス レベルでの DHCP リレー統計情報をモニタします。

show ip dhcp snooping statisticsvlan [*vlan-id*] **interface**[**ethernet**|*port-channel*][*id*] コマンド（オプション）を使用して、VLAN より下位のインターフェイス別のスヌーピング統計情報に関する正確な統計情報を確認します。

show ipv6 dhcp relay statistics[**interface***interface* [**server-ip***ip-address* [**use-vrf***vrf-name*]]] コマンドを使用して、グローバル、サーバ、またはインターフェイス レベルでの DHCPv6 リレー統計情報をモニタします。

DHCP スヌーピングの設定例

次に、2 つの VLAN 上で DHCP スヌーピングをイネーブルにして、Option 82 サポートをイネーブルにし、さらに DHCP サーバがイーサネット インターフェイス 2/5 に接続されているためにそのインターフェイスを信頼できるインターフェイスとして設定する例を示します。

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

LDRA の設定例

インターフェイスの LDRA の設定

次の例では、LDRA を有効にして、インターフェイス Ethernet 1/1 をクライアント側の信頼できるインターフェイスとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# ipv6 dhcp ldra
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# ipv6 dhcp-ldra client-facing-trusted
switch(config-if)# exit
switch(config)# interface ethernet 1/0
switch(config-if)# switchport
switch(config-if)# ipv6 dhcp-ldra attach-policy server-facing
switch(config-if)# exit
```

VLAN の LDRA の設定

次の例では、LDRA を有効にして、VLAN を VLAN ID 25 でクライアント側の信頼できる VLAN として設定する方法を示しています。

```
switch# configure terminal
switch(config)# ipv6 dhcp ldra
switch(config)# ipv6 dhcp-ldra attach-policy vlan 25 client-facing-trusted
```