IPv6 ファースト ホップ セキュリティの設定

この章では、Cisco NX-OS デバイスで First Hop Security（FHS）機能を設定する方法を説明します。

この章は、次の項で構成されています。

ファーストホップ セキュリティについて

レイヤ 2 およびレイヤ 3 スイッチは、サーバ仮想化、オーバーレイトランスポート仮想化（OTV）、レイヤ 2 モビリティなどのテクノロジーを使用して、レイヤ 2 ドメインで動作します。これらのデバイスは、特にエンドノードに面している場合に、「ファーストホップ」と呼ばれることがあります。ファーストホップセキュリティ機能は、エンドノードを保護し、IPv6 またはデュアルスタック ネットワークでのリンク操作を最適化します。

ファーストホップ セキュリティ（FHS）は、IPv6 リンクの動作を最適化し、大規模な L2 ドメインの拡張に役立つ一連の機能です。これらの機能は、さまざまな不正ユーザや設定ミスのユーザから保護します。拡張 FHS 機能は、さまざまな展開シナリオまたは攻撃ベクトルに使用できます。

次の FHS 機能がサポートされています。

- IPv6 RA ガード

- DHCPv6 ガード
- IPv6 スヌーピング

（注） この機能のイネーブル化の詳細については、ファーストホップセキュリティの注意事項と制約事項 （3 ページ）を参照してください。

（注） FHS 機能をイネーブルにするには、**feature dhcp** コマンドを使用します。

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 スヌーピング、DHCPv6 ガード、および IPv6 RA ガードは、IPv6 グローバル ポリシーの機能です。IPv6 スヌーピング、DHCPv6 ガード、および IPv6 RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

すべてのポート レベルの FHS ポリシーは ifacl リージョンでプログラミングされますが、VLAN レベルのポリシーは FHS リージョンでプログラミングされます。ハードウェア プロファイルを設定するには、**tcam regionfhs tcam_size** コマンドを使用します。TCAM サイズの範囲は 0 ー 4096 です。

- Cisco Nexus 9200、9300-EX、および9300-FX/FX2プラットフォームスイッチでは、FHS パケットはソフトウェア処理のために copp-s-dhcpreq キューを使用します。
- Cisco Nexus 9300、9500 プラットフォーム スイッチ、Cisco Nexus 3164Q スイッチ、N9K-X9432C-S ライン カード、および Cisco Nexus 3232C および 3264Q スイッチは、クラス デフォルトを使用します。

（注） In-Service Software Upgrades（ISSU）を使用して Cisco Nexus シリーズスイッチを Cisco NX-OS Release 7.0(3)I7(1) にアップグレードする場合は、ポート レベルの FHS ポリシーを設定する前に Cisco NX-OS ボックスをリロードする必要があります。

IPv6 ファーストホップ セキュリティ バインディング テーブル

デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、IPv6 スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv6 アドレス、

およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

ファーストホップ セキュリティの注意事項と制約事項

ファーストホップ セキュリティの一般的な注意事項と制限事項は次のとおりです。

- インターフェイスで FHS を有効にする前に、Cisco Nexus 9300 および 9500 プラットフォーム スイッチで TCAM リージョンをカービングすることを推奨します。FHS を正しく有効にするには、次の手順を実行します。
  - インターフェイスでは、**ifacl** TCAMリージョンをカービングする必要があります。
  - VLAN では、必要なリダイレクト TCAM リージョンをカービングする必要があります。
  - FEX インターフェイスでは、**fex-ipv6-ifacl** TCAMリージョンをカービングする必要があります。
- Cisco Nexus 9200、9300-EX、および 9300-FX/FX2 プラットフォーム スイッチでは、FHS を有効にする前に、**ing-redirect** TCAM リージョンをカービングすることを推奨します。
- Cisco NX-OS リリース 9.3(5) 以降、FHS は Cisco Nexus 9300-GX スイッチでサポートされます。

vPC ファーストホップ セキュリティ設定について

IPv6 ファーストホップ セキュリティ vPC はさまざまな方法で導入できます。次のベストプラクティス展開シナリオを推奨します。

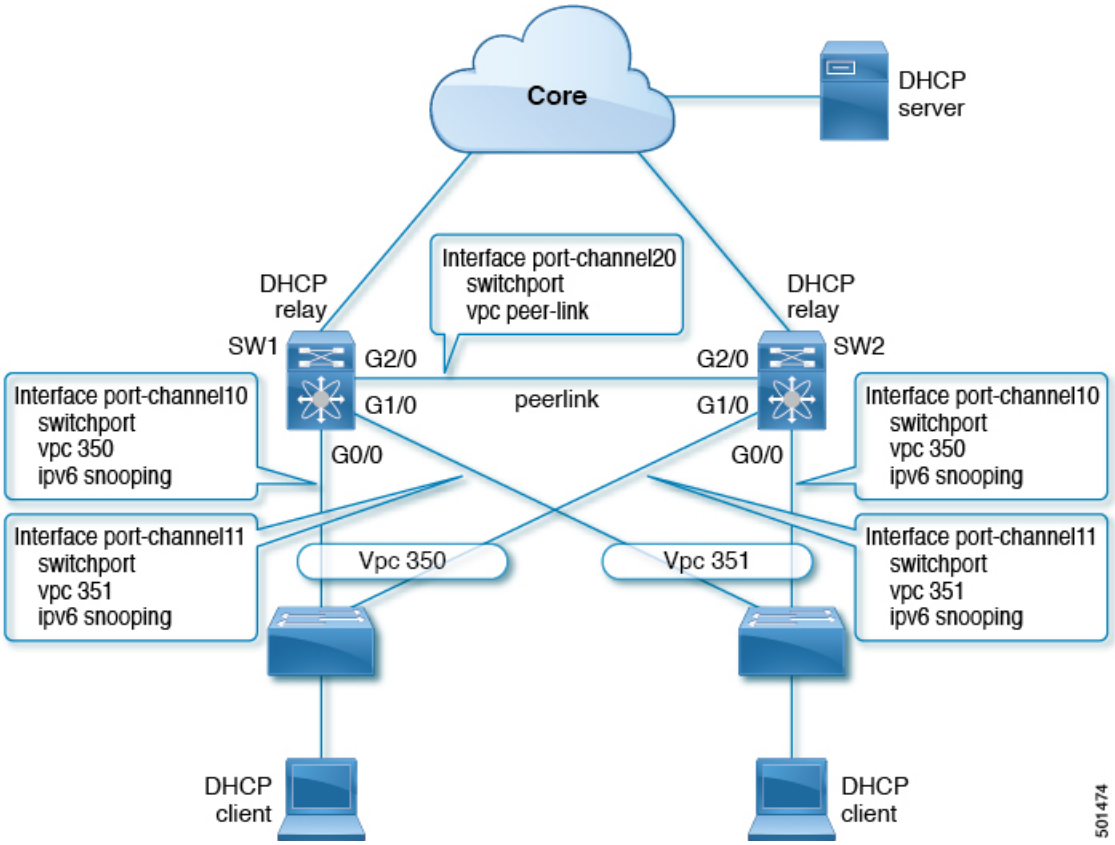
- DHCP リレー オンスタック
- vPC レッグの DHCP リレー
- 孤立ポートの DHCP クライアントとリレー

DHCP リレー オンスタック

この導入シナリオでは、vPC リンクの背後にあるクライアント、または Nexus スイッチで実行されている DHCP リレーを使用する中間スイッチの背後にあるクライアントを、直接接続できます。Nexus スイッチで実行されている DHCP リレーを使用する中間スイッチの背後にあるクライアントに接続することは、理想的な手段です。VLAN レベルではなく、vPC インターフェイス リンク上の IPv6 スヌーピング機能を直接設定できるからです。インターフェイス レベルでの設定は、次の理由で効率的です。

- 制御トラフィック（DHCP/ND）は、ピア リンクを経由する場合、CPU にリダイレクトされて両方の vPC ピアで処理されることはありません。
- ピアリンク経由でスイッチングされたパケットに、2 回目の処理は行われません。

Figure 1: DHCP* リレー オンスタックでの *FHS



図では、スヌーピング ポリシーは両方の vPC リンクで有効になっています。このシナリオでは、2 つの vPC ピアが vPC リンクの背後にあるすべてのホスト IP/MAC バインディングを学習し、それらを相互に同期します。2 つの vPC ピアは、IPv6 ND と IPv6 DHCP 制御プロトコルの両方を使用してバインディングを学習します。

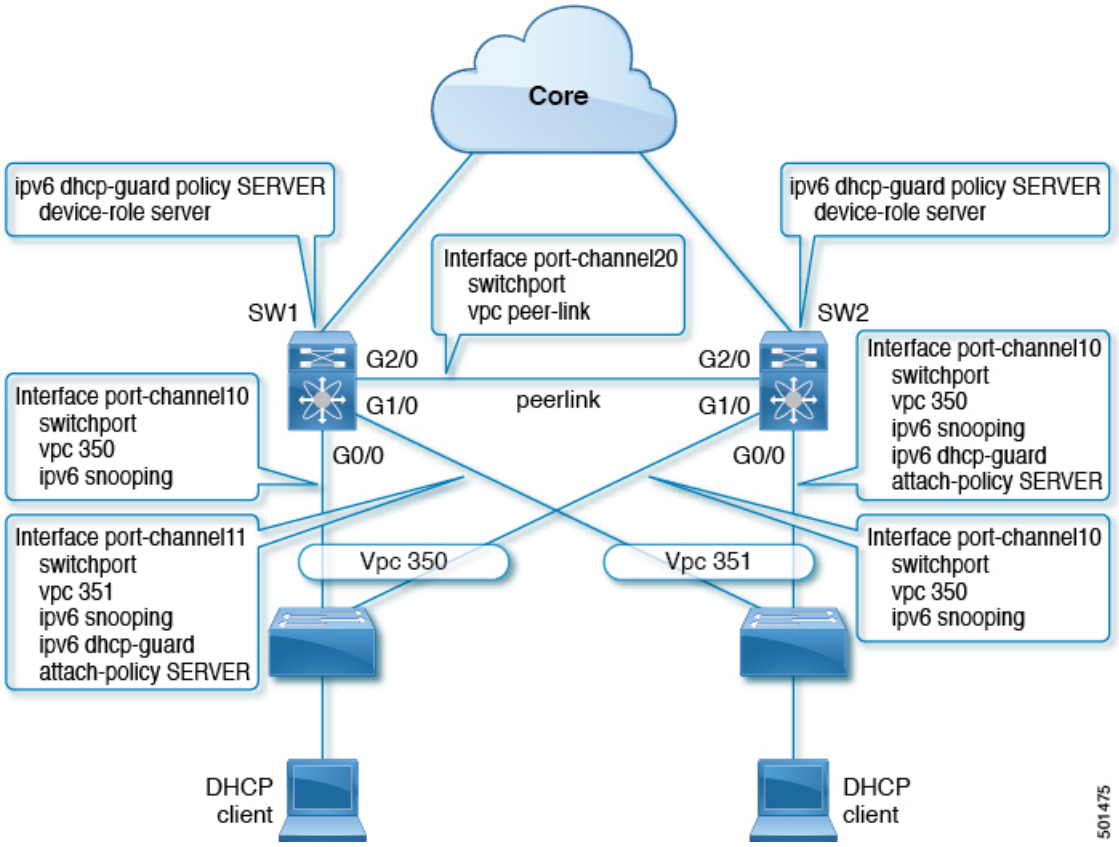
VPC レッグでの DHCP リレー

この設定では、リレー エージェントは vPC ピアで実行されません。代わりに、DHCP リレー エージェント（または DHCP サーバ）が vPC リンクの背後で実行されます（アクセスできる場所に置くことも、さらにはコアのどこかに配置することもできます）。このような導入シナリオでは、IPv6 スヌーピング機能は DHCP サーバメッセージを暗黙的に信頼せず、デフォルトでDHCP サーバ メッセージをドロップします。IPv6 ポリシーをカスタマイズして、次を実装できます。

- セキュリティ レベルに関する補足情報。

- デバイス ロール サーバを使用した IPv6 DHCP ガード ポリシー。この設定では、IPv6 スヌーピングは vPC リンクに接続された DHCP サーバ メッセージを信頼します。

Figure 2: 外部 ***DHCP*** リレーを使用した ***FHS*** 設定



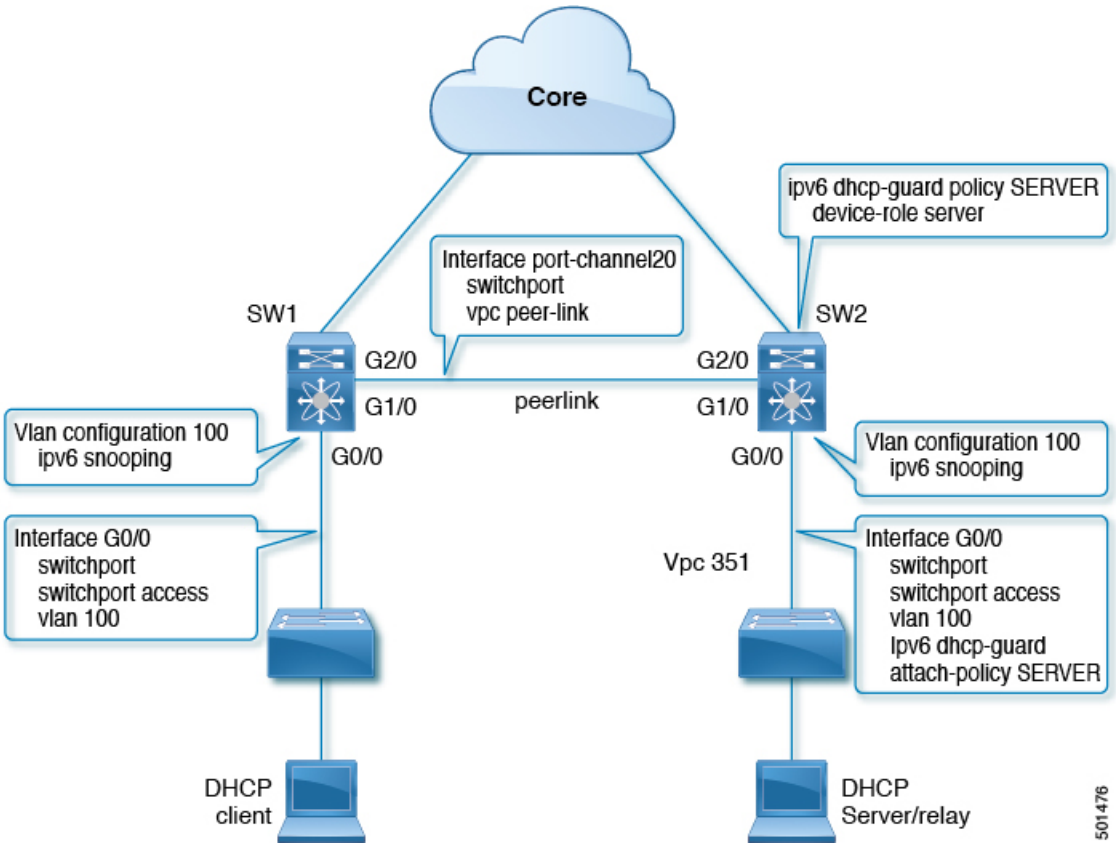
図では、クライアントはデフォルトの IPv6 スヌーピング ポリシーを持つ vPC リンクの背後に配置されています。DHCP サーバトラフィックが到達するリンクに、ipv6 スヌーピングと、ipv6 dhcp-guard attach-policy SERVER ポリシーの両方をアタッチできます。DHCP 制御トラフィックを介してクライアントバインディングエントリを作成するには、サーバまたはリレー側とクライアント側の両方の IPv6 スヌーピング ポリシーが必要です。これは、IPv6 スヌーピングがバインディングを作成するためにはクライアントとサーバの両方のパケットを確認する必要があるためです。また、IPv6 DHCP ガード ポリシーを設定して、IPv6 スヌーピング ポリシーによる DHCP サーバ トラフィックを許可する必要があります。vPC ピアは vPC ポートで学習されたすべての新しく学習されたクライアントエントリを同期するため、両方のピアに同じ設定が必要です。

孤立ポートでの DHCP クライアント リレー

この設定では、孤立ポートを介してクライアントを接続できます。IPv6 スヌーピング機能は、vPC ポートのクライアント バインディングのみを同期します。孤立ポートは両方の vPC ピアに直接接続されていないため、同期されません。このような設定では、IPv6 スヌーピング機能は両方のスイッチで独立して実行されます。この図は、次のことを示しています。

- 最初のスイッチで、クライアント側インターフェイスに IPv6 スヌーピング ポリシーをアタッチする必要があります。ただし、vPC ピアの背後にある孤立ポート上のサーバからの DHCP サーバパケットに対応するには、VLAN レベルでポリシーを付加する必要があります。のこのような場合、VLAN に適用されるポリシーは、クライアント トラフィック インターフェイスと DHCP サーバ トラフィックの両方を検査します。インターフェイスごとに個別の IPv6 スヌーピング ポリシーは必要ありません。vPC ピア経由で着信する DHCP トラフィックも暗黙的に信頼され、ポリシングが必要な場合は、vPC ピアによって自動的にドロップされます。
- また、2 番目のスイッチで VLAN レベルで IPv6 を設定する必要があります。また、孤立ポートに面するサーバで「デバイス ロール サーバ」を使用して IPv6 DHCP ガード ポリシーを設定する必要があります。これにより、IPv6 スヌーピング機能による DHCP サーバ パケットのドロップが防止されます。両方のスイッチはクライアント バインディング エントリを個別に学習し、クライアントが vPC リンク上にないため、それらを同期しません。

Figure 3: 孤立ポート上のクライアントおよび ***DHCP*** リレーによる ***FHS*** 設定



RA ガード

IPv6 RA ガードの概要

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正なRAガードメッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2（L2）デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

IPv6 RA ルータ アドバタイズメントとフラグ

ルータ アドバタイズメントは、リンク上で通信するためのグローバル ユニキャスト アドレスおよびその他のアドレス指定情報を作成または取得する方法をデバイスに提案します。RA メッセージは 4 つのフラグを使用して、これがどのように行われるかをデバイスに通知します。

1. アドレス自動構成フラグ（A フラグ）：A フラグはデフォルトで有効になっています。このフラグは、指定したプレフィックスが IPv6 自動構成に使用できることをローカル リンク上のホストに知らせます。
2. その他の構成フラグ（O フラグ）：O フラグはデフォルトで無効になっています。このフラグは、ステートレス DHCPv6 サーバーからグローバル ユニキャスト アドレス以外のアドレス指定情報を取得するようにホストに指示します。この情報には、DNS サーバーのアドレスとドメイン名が含まれる場合があります。
3. 管理対象アドレス構成フラグ（M フラグ）：M フラグはデフォルトで無効になっています。このフラグは、グローバル ユニキャスト アドレスおよびその他すべてのアドレス指定情報にステートフル DHCPv6 サーバーを使用するようにホストに指示します。ステートフル DHCPv6 が必要な場合は、**ipv6 managed-config-flag** コマンドを使用して M フラグを有効にします。

（注） M フラグが有効な場合、A フラグは通常無効にする必要があります。M フラグを手動で有効にしても、A フラグは自動的に無効になりません。A フラグを無効にするには、**ipv6 nd prefix** *ipv6-prefix/prefix-length* **no-autoconfig** コマンドを使用します。

4. オンリンク フラグ（L フラグ）：L フラグもデフォルトで有効になっています。L フラグは、特定のプレフィックスがこのリンクまたはサブネット上にあることを識別します。IPv6

は、接続先IPアドレスがリンクに対してローカルであるかどうかを判断するために、IPv4のように論理 AND ハッシュを実行しません。L フラグが無効になっている場合、すべてのパケットはデフォルト ゲートウェイに送信されます。A フラグと L フラグは、デフォルトで ICMPv6 ルーター アドバタイズメント（RA）を介してアドバタイズされます。

IPv6 RA ガードの注意事項と制約事項

IPv6 RA ガードの注意事項と制約事項は次のとおりです。

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- Cisco NX-OS リリース 10.1(1) から、Cisco Nexus 9300-GX プラットフォーム スイッチで IPV6 RA ガードはサポートされます。
- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、補助VLANおよびプライベートVLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。

DHCPv6 ガード

DHCPの概要：DHCPv6 ガード

DHCPv6 ガード機能は、サーバからクライアントにDHCPパケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメント メッセージをブロックします。クライアントメッセージまたはリレーエージェントによってクライアントからサーバに送信されるメッセージはブロックされません。フィルタリングの決定は、受信側スイッチポート、トランク、またはVLANに割り当てられたデバイスロールによって決定されます。この機能は、トラフィックリダイレクションまたはサービス妨害（DoS）を防止するのに役立ちます。

パケットは、3つのDHCPタイプメッセージのいずれかに分類されます。すべてのクライアントメッセージは、デバイスロールに関係なく常にスイッチングされます。DHCPサーバメッセージは、デバイスロールがserverに設定されている場合にのみ、さらに処理されます。DHCP サーバ アドバタイズメントの追加処理は、サーバ プリファレンス チェックのために行われます。

デバイスがDHCPサーバとして設定されている場合は、デバイスロールの設定に関係なく、すべてのメッセージを切り替える必要があります。

DHCPv6 ガードの制限事項

DHCPv6 ガードの注意事項と制約事項は次のとおりです。

- DHCP サーバから到着するパケットがリレー転送またはリレー応答である場合、デバイスロールのみがチェックされます。さらに、IPv6 DHCP ガードは、スイッチで実行されているローカル リレー エージェントによって送信されたパケットにポリシーを適用しません。

IPv6 スヌーピング

IGMP スヌーピングの概要

IPv6 の「スヌーピング」機能は、レイヤ 2 IPv6 のファーストホップ機能をいくつか組み合わせたもので、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディング テーブルを構築するためにスヌーピング メッセージを分析します。有効なバインディングのない IPv6 スヌーピング メッセージはドロップされます。IPv6 スヌーピング メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックのスヌーピング プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。スヌーピング トラフィックの場合、Neighbor Discovery Protocol（NDP）メッセージは SISF に送信されます。DHCPv6の場合、dhcvp6_client および dhcvp_server ポートから送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピング エントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 スヌーピングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

加えて、IPv6 スヌーピングは、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上のスヌーピングおよびDHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

IPv6 スヌーピングに関する注意事項と制限事項

IPv6スヌーピングの注意事項と制限事項は次のとおりです。

- 両方の vPC ピアで同じ設定を実行する必要があります。IPv6 スヌーピングの自動整合性チェッカはサポートされていません。
- IPv6 スヌーピング機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスまたは VLAN のみで設定できます。
- IPv6 スヌーピングが DHCP バインディングを学習するには、サーバとクライアントの両方の応答を確認する必要があります。IPv6 スヌーピング ポリシーは、インターフェイス（またはVLAN）に面したクライアントと、インターフェイス（またはVLAN）に面したDHCP サーバの両方にアタッチする必要があります。DHCP リレーの場合、サーバの応答を確認するために、IPv6 スヌーピングポリシーを VLAN レベルでアタッチする必要があります。

IPv6 FHS の設定方法

デバイスでの IPv6 RA ガード ポリシーの設定

（注） **ipv6 nd raguard** コマンドがポートで設定されている場合、ルータ送信要求メッセージはこれらのポートに複製されません。ルータ要請メッセージを複製するには、ルータ側のすべてのポートをルータ ロールに設定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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 2	**ipv6 nd raguard policy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy policy1`	RA ガード ポリシー名を定義して、RA ガード ポリシー 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	**device-role** {**host** | **router** | **monitor** | **switch**} 例： `Device(config-ra-guard)# device-role router`	ポートに接続されているデバイスの役割を指定します。 • device-role host：通常のノードまたはホストを接続するインターフェイスまたはVLAN。これは、IPV6 RA ガード ポリシーを適用します。device-role ホストは、着信 RS パケットを許可し、着信 RA または RR パケットをブロックします。別のインターフェイスで受信された RS パケットは、デバイスロール ホストにリダイレクトされません。RA および RR パケット（許可されている）のみがデバイスロール ホストにリダイレクトされます。 • device-role switch：device-role スイッチは device-role ホストと同様に動作します。たとえば、トランク ポートのラベルとして使用できます。 • device-role monitor：このデバイスはネットワーク トラフィックをモニタします。これは、RS パケットもこのインターフェイスに送信されることを除き、device-role ホストと同様に動作します。これは、トラフィックのキャプチャに役立ちます。 • device-role router：ルータに接続するインターフェイス。このインターフェイスは、着信RS、RA、または RR パケットを許可します。

	コマンドまたはアクション	目的
ステップ 4	**hop-limit** {**maximum** | **minimum** *limit*} 例： `Device(config-ra-guard)# hop-limit minimum 3`	（任意）アドバタイズされたホップ カウント制限の検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 5	**managed-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# managed-config-flag on`	（任意）アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。 （注） M フラグを有効にする場合は、A フラグを無効にすることをお勧めします。 • 設定されていない場合、このチェックは回避されます。
ステップ 6	**other-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# other-config-flag on`	（任意）アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。
ステップ 7	**router-preference maximum** {**high** | **low** | **medium**} 例： `Device(config-ra-guard)# router-preference maximum high`	（任意）アドバタイズされたデフォルト ルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。
ステップ 8	**trusted-port** 例： `Device(config-ra-guard)# trusted-port`	（任意）このポリシーが信頼できるポートに適用されることを指定します。 • すべての RA ガード ポリシングが無効になります。
ステップ 9	**exit** 例： `Device(config-ra-guard)# exit`	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

インターフェイスの IPv6 RA ガードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**interface** *type number*
	例：
	`Device(config)# interface ethernet 1/1`
	例：
	`Device(config)# vlan configuration 10`
		インターフェイスのタイプと番号を指定し、デバイスをインターフェイス モードにするか、VLAN 設定モードにします。

ステップ 3	**ipv6 nd raguard attach-policy** [*policy-name*] 例： `Device(config-if)# ipv6 nd raguard attach-policy`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	**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 モードを終了します。

ステップ 5	**show ipv6 nd raguard policy** [*policy-name*]
	例：
	`switch# show ipv6 nd raguard policy host`
	`Policy host configuration:`
	`  device-role host`
	
	`Policy applied on the following interfaces:`
	
	`  Et0/0  vlan all`
	`  Et1/0  vlan all`
		RA ガードを使用して設定されているすべてのインターフェイスで RA ガード ポリシーを表示します。

ステップ 6	**debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*] 例： `Device# debug ipv6 snooping raguard`	IPv6 RA ガード スヌーピング情報のデバッグを有効にします。

DHCP の設定：DHCPv6 ガード

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**ipv6 dhcp guard policy** *policy-name* 例： `Device(config)# ipv6 dhcp guard policy pol1`	DHCPv6 ガード ポリシー名を定義して、DHCP ガード 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	**device-role** {**client** | **server**} 例： `Device(config-dhcp-guard)# device-role server`	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのデバイス ロールを指定します。 • device-role client：通常の DHCPv6 クライアントが接続されているインターフェイス。着信サーバ パケットをブロックします。 • device-role server：通常の DHCPv6 サーバが接続されているインターフェイス。このインターフェイスから発信されるすべての DHCPv6 パケットを許可します。
ステップ 4	**preference min** 制限 例： `Device(config-dhcp-guard)# preference min 0`	（オプション）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証を有効にします。設定されていない場合、このチェックは回避されます。
ステップ 5	**preference max** 制限 例： `Device(config-dhcp-guard)# preference max 255`	（オプション）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証を有効にします。設定されていない場合、このチェックは回避されます。

	コマンドまたはアクション	目的
ステップ 6	**trusted-port** 例： `Device(config-dhcp-guard)# trusted-port`	（任意）このポリシーが信頼できるポートに適用されることを指定します。すべての DHCP ガード ポリシングが無効になります。
ステップ 7	**exit** 例： `Device(config-dhcp-guard)# exit`	DHCP ガード 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 8	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/2/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport** 例： `Device(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 モードにします。
ステップ 10	**ipv6 dhcp guard** [**attach-policy** *policy-name*] 例： `Device(config-if)# ipv6 dhcp guard attach-policy pol1`	DHCPv6ガードポリシーをインターフェイスに適用します。
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。
ステップ 12	**vlan configuration** *vlan-id* 例： `Device(config)# vlan configuration 1`	VLAN を指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 13	**ipv6 dhcp guard** [**attach-policy** *policy-name*] 例： `Device(config-vlan-config)# ipv6 dhcp guard attach-policy pol1`	DHCPv6ガードポリシーをVLANに適用します。

	コマンドまたはアクション	目的
ステップ 14	**exit** 例： `Device(config-vlan-config)# exit`	VLAN 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 15	**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 16	**show ipv6 dhcp guard policy** [*policy-name*] 例： `Device# show ipv6 dhcp policy guard pol1`	（オプション）ポリシー設定と、そのポリシーが適用されるインターフェイスを表示します。

IPv6 スヌーピングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**ipv6 snooping policy** *policy-name* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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	**device-role** { **node** | **switch** } 例： `Device(config-snoop-policy)# device-node switch`	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのロールを指定します。 • node - がデフォルトです。バインディングが作成され、エントリがプローブされます。 • スイッチ：エントリはプローブされず、信頼できるポートが有効になっている場合、バインディングは作成されません。

	コマンドまたはアクション	目的
ステップ 4	**[no] limit address-count** 例： `Device(config-snoop-policy)# limit address-count 500`	バインディングエントリの数を制限します。no limit address-count は制限なしを意味します。

ステップ 5	**[no] protocol** *dhcp* | *ndp*
	例：
	`Device(config-snoop-policy)# protocol dhcp`
	`Device(config-snoop-policy)# protocol ndp`
		DHCP または NDP グリーニングのいずれかをオンまたはオフにします。

ステップ 6	**trusted-port** 例： `Device(config-snoop-policy)# trusted-port`	ポリシーを信頼できるポートに適用することを指定します。エントリが信頼できるポートである場合、そのトラフィックはブロックまたはドロップされません。
ステップ 7	**security-level** *glean* | *guard* | *inspect* 例： `Device(config-snoop-policy)# security-level guard`	ポリシーに適用するセキュリティのタイプ（グリーニング、ガード、または検査）を指定します。各セキュリティレベルの意味は次のとおりです。 • glean：バインディングを学習しますが、パケットはドロップしません。 • inspect：アドレス盗難などの問題を検出した場合に、バインディングを学習し、パケットをドロップします。 • guard：inspect と同様に機能しますが、さらに脅威の場合に IPv6、ND、RA、および IPv6 DHCP サーバ パケットをドロップします。
ステップ 8	**tracking** 例： `Device(config-snoop-policy)# tracking enable`	トラッキングをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-snoop-policy)# exit`	IPv6 スヌーピング 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 10	**interface** *type-number* 例： `Device(config-if)# interface ethernet 1/25`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**[no] switchport** 例： `Device(config-if)# switchport`	レイヤ 2 モードとレイヤ 3 モードを切り替えます。
ステップ 12	**ipv6 snooping attach-policy** *policy-name* 例： `Device(config-if)# ipv6 snooping attach-policy policy1`	インターフェイスに IPv6 スヌーピング ポリシーを適用します。
ステップ 13	**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 14	**vlan configuration** *vlan-id* 例： `Device(config)# vlan configuration 333`	VLAN を指定し、VLAN コンフィギュレーション モードを開始します。
ステップ 15	**ipv6 snooping attach-policy** *policy-name* 例： `Device(config-vlan-config)# ipv6 snooping attach-policy policy1`	IPv6 スヌーピング ポリシーを VLAN に適用します。
ステップ 16	**exit** 例： `Device(config-vlan-config)# exit`	VLAN 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 17	**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 18	**show ipv6 snooping policy** *policy-name* 例： `Device(config)# show ipv6 snooping policy policy1`	ポリシー設定と、そのポリシーが適用されるインターフェイスを表示します。

IPv6 スヌーピングの確認とトラブルシューティング

手順

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 snooping capture-policy** [**interface** *type number*] 例： `Device# show ipv6 snooping capture-policy interface ethernet 0/0`	スヌーピング ND メッセージ キャプチャ ポリシーを表示します。
ステップ 2	**show ipv6 snooping counter** [**interface** *type number*] 例： `Device# show ipv6 snooping counter interface FastEthernet 4/12`	インターフェイス カウンタによってカウントされたパケットに関する情報を表示します。
ステップ 3	**show ipv6 snooping features** 例： `Device# show ipv6 snooping features`	デバイスに設定されているスヌーピング機能に関する情報を表示します。
ステップ 4	**show ipv6 snooping policies** [**interface** *type number*] 例： `Device# show ipv6 snooping policies`	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 5	**debug ipv6 snooping** 例： `Device# debug ipv6 snooping`	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

設定例

例：IPv6 RA ガードの設定

```
Device(config)# interface ethernet 1/1

Device(config-if)# ipv6 nd raguard attach-policy
```

```
Device# show running-config interface ethernet 1/1

Building configuration...
Current configuration : 129 bytes
!
interface ethernet1/1
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

例：DHCP—DHCPv6 ガードの設定

次の例は、DHCPv6 ガードの設定例を示しています。

```
configure terminal
ipv6 dhcp guard policy pol1
 device-role server
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1
 vlan configuration 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

例：IPv6 ファーストホップ セキュリティ バインディング テーブルの設定

```
config terminal
 ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0
 ipv6 neighbor binding max-entries 100
 ipv6 neighbor binding logging
 ipv6 neighbor binding retry-interval 8
 exit
show ipv6 neighbor binding
```

例：IPv6 スヌーピングの設定

```
switch (config)# ipv6 snooping policy policy1
switch(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
switch(config-ipv6-snooping)# exit
.
.
.
Device# show ipv6 snooping policies policy1
Policy policy1 configuration:
```

```
  trusted-port
  device-role node
Policy applied on the following interfaces:
   Et0/0       vlan all
   Et1/0       vlan all
Policy applied on the following vlans:
   vlan 1-100,200,300-400
```

IPv6 ファーストホップ セキュリティに関する追加情報

ここでは、IPv6 ファーストホップ セキュリティに関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS* ライセンス ガイド』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

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。