IPv6 ソース ガードとプレフィックス ガード

IPv6 ソース ガードと IPv6 プレフィックス ガードは、IPv6 トラフィックの送信元を検証するレイヤ 2 スヌーピング機能です。IPv6 ソース ガードは、不明な送信元からのデータ トラフィックをブロックします。たとえば、バインディング テーブルにまだ入力されていないトラフィックや、ネイバー探索（ND）または Dynamic Host Configuration Protocol（DHCP）グリーニングを介して学習されていないトラフィックをブロックします。IPv6 プレフィックス ガードは、承認および委任されたトラフィック以外のホームノードが送信元のトラフィックを阻止します。

IPv6 ソース ガードとプレフィックス ガードに関する情報

IPv6 ソース ガードの概要

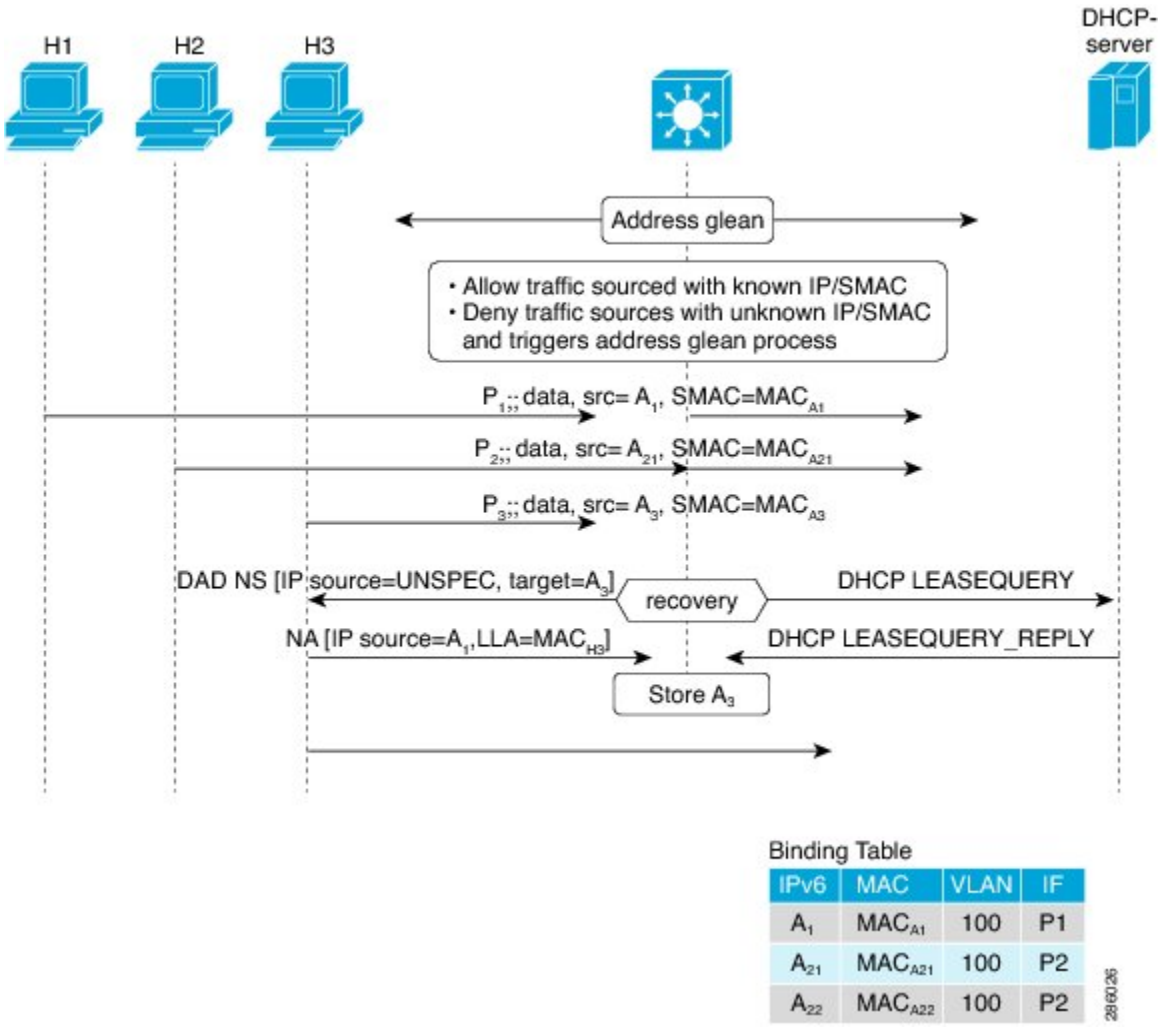
IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイス機能です。この機能により、デバイスは、バインディング テーブルに保存されていないアドレスから送信されたトラフィックを拒否できます。IPv6 ソース ガードは ND や DHCPパケットを検査せず、むしろ、IPv6 ネイバー探索（ND）インスペクションや IPv6 アドレス収集（どちらもリンク上の既存アドレスを検出して、バインディング テーブルに保存する機能）と連動して機能します。IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイスであり、IPv6 ソース ガードが機能するためには、バインディング テーブルに IPv6 プレフィックスが入力されている必要があります。

IPv6 ソース ガードは、DHCP サーバによって割り当てられていない送信元からのトラフィックなど、不明な発信元や未割り当てのアドレスからのトラフィックを拒否できます。トラフィッ

クが拒否されると、IPv6アドレス収集機能に通知されるため、DHCPサーバをクエリして、またはIPv6 NDを使用して、トラフィックのリカバリを試みることができます。データ収集機能は、有効なアドレスをバインディング テーブルに保存できず、復旧パスがなく、エンド ユーザが接続できなくなるとすぐに、デバイスとエンド ユーザがデッドロックになるのを防ぎます。

次の図は、IPv6 ソース ガードと IPv6 アドレス収集の仕組みの概要を示しています。

図 *1 : IPv6* ソース ガードとアドレス収集の概要



IPv6 プレフィックス ガードの概要

IPv6 プレフィックス ガード機能は、IPv6 ソース ガード機能内で動作し、トポロジ面で正しくないアドレスから発信されたトラフィックをデバイスが拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンク

に割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

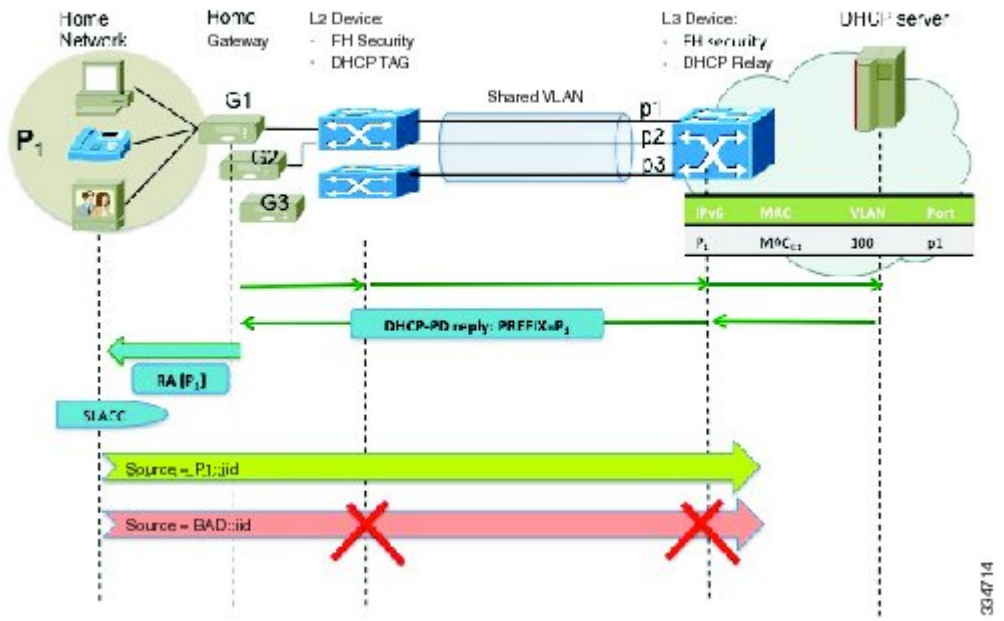
許可するプレフィックスとブロックするプレフィックスを決めるために、IPv6プレフィックスガードは以下の情報を使用します。

- ルータ アドバタイズメント（RA）でのプレフィックス収集
- DHCP プレフィックス委任でのプレフィックス収集
- 静的設定

IPv6 プレフィックス ガードでは、許可されるプレフィックスは常にハードウェア テーブルにダウンロードされます。ハードウェアは、パケットのスイッチングが行われるたびに、パケットの送信元をこのテーブルで照合し、一致するものがない場合そのパケットをドロップします。

次の図は、プレフィックスがDHCP-PDメッセージで収集されるサービスプロバイダー（SP）のシナリオを示しています。

図 *2:* プレフィックスが収集される *DHCP-PD* メッセージのシナリオ



IPv6 ソース ガードとプレフィックス ガードの設定方法

IPv6 ソース ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **permit link-local**
5. **deny global-autoconf**
6. **trusted**
7. **exit**
8. **show ipv6 source-guard policy** ［*snooping-policy*］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_sourceguard_policy`	IPv6 ソースガードポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード 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 4	**permit link-local** 例： `Device(config-sisf-sourceguard)# permit link-local`	リンクローカル アドレスから発信されるすべてのデータ トラフィックに対するハードウェア ブリッジングを許可します。
ステップ 5	**deny global-autoconf** 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。

	コマンドまたはアクション	目的
ステップ 6	**trusted** 例： `Device(config-sisf-sourceguard)# trusted`	ポリシーが適用されるターゲットのすべてのデータトラフィックに対するハードウェア ブリッジングを許可します。
ステップ 7	**exit** 例： `Device(config-sisf-sourceguard)# exit`	ソース 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、特権 EXEC モードに戻ります。
ステップ 8	**show ipv6 source-guard policy** ［*snooping-policy*］ 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

インターフェイスの IPv6 ソース ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 source-guard attach-policy** *source-guard-policy*
5. **exit**
6. **show ipv6 source-guard policy** *source-guard-policy*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface fastethernet 3/13`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 source-guard attach-policy** *source-guard-policy* 例： `Device(config-if)# ipv6 source-guard attach-policy my_source_guard_policy`	インターフェイスに IPv6 ソース ガードを適用します。
ステップ 5	**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 モードを終了して、デバイスを特権 EXEC モードにします。
ステップ 6	**show ipv6 source-guard policy** *source-guard-policy* 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソース ガードが適用されているすべてのインターフェイスを表示します。

IPv6 プレフィックス ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy** ［*source-guard-policy*］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**validate address** 例： `Device(config-sisf-sourceguard)# no validate address`	アドレス検証機能を無効にし、IPv6 プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： `Device(config-sisf-sourceguard)# validate prefix`	IPv6 プレフィックスガード動作を実行するよう、IPv6 ソースガードを有効にします。
ステップ 6	**exit** 例： `Device(config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy** ［*source-guard-policy*］ 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

IPv6 ソース ガードとプレフィックス ガードの設定例

例：IPv6 ソース ガードとプレフィックス ガードの設定

```
Device# ipv6 source-guard policy policy1

Policy guard configuration:
  validate prefix
  validate address
```

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

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。