



IPv6 ファースト ホップ セキュリティの設定

- [IPv6 でのファースト ホップ セキュリティの前提条件 \(1 ページ\)](#)
- [IPv6 でのファースト ホップ セキュリティの制約事項 \(1 ページ\)](#)
- [IPv6 でのファースト ホップ セキュリティに関する情報 \(2 ページ\)](#)
- [IPv6 スヌーピング ポリシーの設定方法 \(4 ページ\)](#)
- [IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 \(6 ページ\)](#)
- [IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 \(8 ページ\)](#)
- [IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法 \(9 ページ\)](#)
- [IPv6 バインディング テーブルの内容を設定する方法 \(9 ページ\)](#)
- [IPv6 ネイバー探索検査ポリシーの設定方法 \(11 ページ\)](#)
- [IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 \(16 ページ\)](#)
- [IPv6 DHCP ガード ポリシーの設定方法 \(22 ページ\)](#)
- [IPv6 ソース ガードの設定方法 \(27 ページ\)](#)
- [IPv6 プレフィックス ガードの設定方法 \(30 ページ\)](#)
- [IPv6 ファースト ホップ セキュリティの設定例 \(32 ページ\)](#)

IPv6 でのファースト ホップ セキュリティの前提条件

必要な、IPv6 が有効になっている SDM テンプレートが設定されていること。

IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します (ポート チャンネル)。
 - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。

- FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピング ポリシーがアクセス スイッチに設定されると、ルータまたは DHCP サーバリレーに対応するアップリンク ポートが信頼できるポートとして設定されていても、IPv6 (DHCPv6) サーバ パケットに対する外部 IPv6 ルータ アドバタイズメント(RA)または Dynamic Host Configuration Protocol はブロックされます。IPv6 RA または DHCPv6 サーバ メッセージを許可するには、次の手順を実行します。
 - IPv6 RA ガード ポリシー (RA の場合) または IPv6 DHCP ガード ポリシー (DHCP サーバ メッセージの場合) をアップリンク ポートに適用します。
 - 低いセキュリティ レベルでスヌーピング ポリシーを設定します (たとえば、`glean` や `inspect` など)。しかし、ファースト ホップ セキュリティ機能の利点が有効でないため、このようなスヌーピング ポリシーでは、低いセキュリティ レベルを設定することはお勧めしません。
- 同じノードにおけるホストとガードの設定はサポートされていません。
- DHCPv6 ガードを機能させるには、同じスイッチ上の対応する VLAN で SVI を設定する必要があります。

IPv6 でのファースト ホップ セキュリティに関する情報

IPv6 のファーストホップセキュリティ (FHS IPv6) は、ポリシーを物理インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシー データベースに保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能を有効にできるコンテナ ポリシーとして機能します。



(注) 以降、IPv6 スヌーピングポリシー機能は廃止され、Switch Integrated Security Features (SISF) ベースのデバイス追跡に置き換わります。IPv6 スヌーピングポリシー コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代替の機能の詳細については、このガイドの「SISF ベースのデバイス追跡の設定」を参照してください。

- IPv6 FHS バインディング テーブルの内容：スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索 (ND) プロトコル スヌーピングなどの情報ソースから作

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、リンク層アドレス (LLA)、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するために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 (IPv6 ND 検査など) によって使用されます。



(注) 以降、IPv6 FHS バインディングテーブルコンテンツ機能は、SISF ベースのデバイス追跡によってサポートされます。詳細については、このガイドの「SISF ベースのデバイス追跡の設定」を参照してください。

- IPv6 ネイバー探索検査 : IPv6 ND 検査は、レイヤ 2 ネイバー テーブル内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、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージは破棄されます。ND メッセージは、その IPv6 からメディアアクセスコントロール (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。

この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。



(注) Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。IPv6 ND 検査コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代替の機能の詳細については、このガイドの「SISF ベースのデバイス追跡の設定」を参照してください。

- IPv6 ルータ アドバタイズメント ガード : IPv6 ルータ アドバタイズメント (RA) ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ 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ブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメント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 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。レイヤ 2 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 は破棄されます。
- IPv6 DHCP ガード : IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバおよびリレーエージェントからの返信およびアドバタイズメントメッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバまたは DHCP リレーからデータを受信することが明示的に設定されていない

いポートで受信された DHCPv6 サーバメッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピングポリシー機能は廃止されました。コマンドは CLI に表示され、設定できますが、代わりにスイッチ統合セキュリティ機能 (SISF) ベースのデバイス追跡機能を使用することを推奨します。

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6 snooping policy *policy-name***
3. **{[default] |[device-role {node | switch}] |[limit address-count *value*] |[no] |[protocol {dhcp | ndp}] |[security-level {glean | guard | inspect}] |[tracking {disable [stale-lifetime [*seconds* | infinite]] | enable [reachable-lifetime [*seconds* | infinite]]] |[trusted-port] }**
4. **end**
5. **show ipv6 snooping policy *policy-name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 <i>policy-name</i> 例： <code>(config)# ipv6 snooping policy example_policy</code>	スヌーピングポリシーを作成し、IPv6 スヌーピングポリシー コンフィギュレーション モードに移行します。
ステップ 3	{[default] [device-role {node switch}] [limit address-count <i>value</i>] [no] [protocol {dhcp ndp}] [security-level {glean guard inspect}] [tracking {disable [stale-lifetime [<i>seconds</i> infinite]] enable [reachable-lifetime [<i>seconds</i> infinite]]] [trusted-port] } 例： <code>(config-ipv6-snooping)# security-level inspect</code> 例：	データ アドレス グリーニングを有効にし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 <ul style="list-style-type: none"> • (任意) default : すべてをデフォルトオプションに設定します。 • (任意) device-role {node switch} : ポートに接続されたデバイスの役割を指定します。デフォルトは node です。

	コマンドまたはアクション	目的
	<code>(config-ipv6-snooping)# trusted-port</code>	<ul style="list-style-type: none"> • (任意) limit address-count value : ターゲットごとに許可されるアドレス数を制限します。 • (任意) no : コマンドを無効にするか、またはそのデフォルトに設定します。 • (任意) protocol{dhcp ndp} : 分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、dhcp および ndp です。デフォルトを変更するには、no protocol コマンドを使用します。 • (任意) security-level{glean guard inspect} : この機能によって適用されるセキュリティのレベルを指定します。デフォルトは guard です。 <ul style="list-style-type: none"> glean : メッセージからアドレスを収集し、何も確認せずにバインディングテーブルに入力します。 guard : アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバメッセージを拒否します。これがデフォルトのオプションです。 inspect : アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。 • (任意) tracking {disable enable} : デフォルトの追跡動作を上書きし、追跡オプションを指定します。 • (任意) trusted-port : 信頼できるポートを設定します。これにより、該当するターゲットに対するガードが無効になります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 4	end 例 : <code>(config-ipv6-snooping)# exit</code>	コンフィギュレーションモードから特権 EXEC モードに戻ります。
ステップ 5	show ipv6 snooping policy policy-name 例 :	スヌーピング ポリシー設定を表示します。

	コマンドまたはアクション	目的
	<code>#show ipv6 snooping policy example_policy</code>	

次のタスク

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type stack/module/port
3. **switchport**
4. **ipv6 snooping** [**attach-policy** policy_name [**vlan** {vlan_id | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids}] | **vlan** {vlan_id | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids | **all**]
5. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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_type stack/module/port 例： (config)# <code>interface gigabitethernet 1/1/4</code>	インターフェイスのタイプおよび ID 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 3	switchport 例：	switchport モードを開始します。

	コマンドまたはアクション	目的
	<pre>(config-if)# switchport</pre>	<p>(注) インターフェイスがレイヤ3モードの場合に、レイヤ2パラメータを設定するには、パラメータを指定せずに switchport 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、インターフェイスをレイヤ2モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度有効になり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ3モードのインターフェイスをレイヤ2モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。switchport コンフィギュレーション モードではコマンドプロンプトは (config-if) # と表示されます。</p>
<p>ステップ 4</p>	<pre>ipv6 snooping [attach-policy <i>policy_name</i> [vlan {<i>vlan_id</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i>}] vlan {<i>vlan_id</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all}]</pre> <p>例 :</p> <pre>(config-if)# ipv6 snooping</pre> <p>or</p> <pre>(config-if)# ipv6 snooping attach-policy example_policy</pre> <p>or</p> <pre>(config-if)# ipv6 snooping vlan 111,112</pre> <p>or</p> <pre>(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112</pre>	<p>インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピング ポリシーをアタッチします。デフォルトポリシーをインターフェイスにアタッチするには、attach-policy キーワードを指定せずに ipv6 snooping コマンドを使用します。デフォルト ポリシーをインターフェイス上の VLAN にアタッチするには、ipv6 snooping vlan コマンドを使用します。デフォルトポリシーは、セキュリティ レベル guard、デバイス ロール node、プロトコル ndp および dhcp です。</p>
<p>ステップ 5</p>	<pre>do show running-config</pre> <p>例 :</p> <pre>#(config-if)# do show running-config</pre>	<p>インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。</p>

IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 range <i>Interface_name</i> 例： <code>(config)# interface range Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。
ステップ 3	ipv6 snooping [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] 例： <code>(config-if-range)# ipv6 snooping attach-policy example_policy</code> or <code>(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224</code> or <code>(config-if-range)#ipv6 snooping vlan 222, 223,224</code>	IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	do show running-config interface <i>portchannel_interface_name</i> 例： <code>#(config-if-range)# do show running-config int po11</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6スヌーピングポリシーをVLANにグローバルにアタッチする方法

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. `configure terminal`
2. `vlan configuration vlan_list`
3. `ipv6 snooping [attach-policy policy_name]`
4. `do show running-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： <code># configure terminal</code>	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	<code>vlan configuration vlan_list</code> 例： <code>(config)# vlan configuration 333</code>	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	<code>ipv6 snooping [attach-policy policy_name]</code> 例： <code>(config-vlan-config)#ipv6 snooping attach-policy example_policy</code>	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポリシーを指定した VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルトポリシーがアタッチされます。デフォルトポリシーは、セキュリティ レベル guard 、デバイス ロール node 、プロトコル ndp および dhcp です。
ステップ 4	<code>do show running-config</code> 例： <code>#(config-if)# do show running-config</code>	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンドまたはアクション	目的
	<code>(config)# exit</code>	
ステップ 6	show ipv6 neighbor binding 例： <code># show ipv6 neighbor binding</code>	バインディング テーブルの内容を表示します。

IPv6 ネイバー探索検査ポリシーの設定方法

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「SISF ベースのデバイス追跡の設定」の章の「カスタム設定を使用したカスタムデバイス追跡ポリシーの作成」を参照してください。

特権 EXEC モードから、IPv6 ND 検査ポリシーを設定するには、次の手順に従ってください。

手順の概要

1. **configure terminal**
2. **[no]ipv6 nd inspection policy *policy-name***
3. **device-role {host | switch}**
4. **limit address-count *value***
5. **tracking {enable [reachable-lifetime {*value* | infinite}] | disable [stale-lifetime {*value* | infinite}]}**
6. **trusted-port**
7. **validate source-mac**
8. **no {device-role | limit address-count | tracking | trusted-port | validate source-mac}**
9. **default {device-role | limit address-count | tracking | trusted-port | validate source-mac}**
10. **do show ipv6 nd inspection policy *policy_name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 nd inspection policy <i>policy-name</i> 例： <code>(config)# ipv6 nd inspection policy example_policy</code>	ND 検査ポリシー名を指定し、ND 検査ポリシー 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 switch} 例： <code>(config-nd-inspection)# device-role switch</code>	ポートに接続されているデバイスの役割を指定します。デフォルトは host です。

	コマンドまたはアクション	目的
ステップ 4	limit address-count <i>value</i> 例： <code>(config-nd-inspection)# limit address-count 1000</code>	1 ~ 10,000 を入力します。
ステップ 5	tracking {enable [reachable-lifetime {value infinite}] disable [stale-lifetime {value infinite}]} 例： <code>(config-nd-inspection)# tracking disable stale-lifetime infinite</code>	ポートのデフォルトのデバイス追跡ポリシーを上書きします。
ステップ 6	trusted-port 例： <code>(config-nd-inspection)# trusted-port</code>	信頼できるポートにするポートを設定します。
ステップ 7	validate source-mac 例： <code>(config-nd-inspection)# validate source-mac</code>	送信元 Media Access Control (MAC) アドレスをリンク層アドレスと照合します。
ステップ 8	no {device-role limit address-count tracking trusted-port validate source-mac} 例： <code>(config-nd-inspection)# no validate source-mac</code>	このコマンドの no 形式を使用してパラメータの現在の設定を削除します。
ステップ 9	default {device-role limit address-count tracking trusted-port validate source-mac} 例： <code>(config-nd-inspection)# default limit address-count</code>	設定をデフォルト値に戻します。
ステップ 10	do show ipv6 nd inspection policy <i>policy_name</i> 例： <code>(config-nd-inspection)# do show ipv6 nd inspection policy example_policy</code>	ND 検査コンフィギュレーションモードを終了しないで ND 検査の設定を確認します。

IPv6 ネイバー探索検査ポリシーをインターフェイスにアタッチする方法

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「SISF ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type stack/module/port
3. **ipv6 nd inspection** [**attach-policy** policy_name [**vlan** {vlan_ids | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids | **all**}] | **vlan** [{vlan_ids | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： # 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 Interface_type stack/module/port 例： (config)# interface gigabitethernet 1/1/4	インターフェイスのタイプおよび ID 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 3	ipv6 nd inspection [attach-policy policy_name [vlan {vlan_ids add vlan_ids except vlan_ids none remove vlan_ids all }] vlan [{vlan_ids add vlan_ids except vlan_ids none remove vlan_ids all }] 例： (config-if)# ipv6 nd inspection attach-policy example_policy or (config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224 or (config-if)# ipv6 nd inspection vlan 222, 223,224	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	do show running-config 例： #(config-if)# do show running-config	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ネイバー探索検査ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。対応する置き換えタスクについては、このドキュメントの「SISF ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interfaceportchannel_interface_name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 range <i>Interface_name</i> 例： <code>(config)# interface Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。
ステップ 3	ipv6 nd inspection [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] 例： <code>(config-if-range)# ipv6 nd inspection attach-policy example_policy</code> or <code>(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224</code>	ND 検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
	<pre>or (config-if-range)#ipv6 nd inspection vlan 222, 223,224</pre>	
ステップ 4	<p>do show running-config interfaceportchannel_interface_name</p> <p>例 :</p> <pre> #(config-if-range)# do show running-config int poll</pre>	<p>コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。</p>

IPv6 ネイバー探索検査ポリシーを全体的に VLAN にアタッチする方法

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「SISF ベースのデバイス追跡の設定」の「デバイス追跡ポリシーの VLAN への適用」を参照してください。

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 nd inspection** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <pre># configure terminal</pre>	<p>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。</p>
ステップ 2	<p>vlan configuration <i>vlan_list</i></p> <p>例 :</p> <pre>(config)# vlan configuration 334</pre>	<p>VLAN インターフェイスのコンフィギュレーションモードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。</p>
ステップ 3	<p>ipv6 nd inspection [attach-policy <i>policy_name</i>]</p> <p>例 :</p> <pre>(config-vlan-config)#ipv6 nd inspection attach-policy example_policy</pre>	<p>すべてのスイッチおよびスタックインターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。</p>

	コマンドまたはアクション	目的
		デフォルトのポリシーは、device-role host 、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。
ステップ 4	do show running-config 例： <pre>(config-if)# do show running-config</pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no]ipv6 nd rguard policy *policy-name***
3. **[no]device-role {host | monitor | router | switch}**
4. **[no]hop-limit {maximum | minimum} *value***
5. **[no]managed-config-flag {off | on}**
6. **[no]match {ipv6 access-list *list* | ra prefix-list *list*}**
7. **[no]other-config-flag {on | off}**
8. **[no]router-preference maximum {high | medium | low}**
9. **[no]trusted-port**
10. **default {device-role | hop-limit {maximum | minimum} | managed-config-flag | match {ipv6 access-list | ra prefix-list } | other-config-flag | router-preference maximum | trusted-port}**
11. **do show ipv6 nd rguard policy *policy_name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre># configure terminal</pre>	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 nd rguard policy <i>policy-name</i> 例： <pre>(config)# ipv6 nd rguard policy example_policy</pre>	RA ガード ポリシー名を指定し、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。

	コマンドまたはアクション	目的
ステップ 3	<p>[no]device-role {host monitor router switch}</p> <p>例 :</p> <pre>(config-nd-raguard)# device-role switch</pre>	<p>ポートに接続されているデバイスの役割を指定します。デフォルトは host です。</p> <p>(注) ホスト側ポートとルータ側ポートの両方を備えたネットワークでは、ホスト側ポートまたは VLAN で device-role host を設定した RA ガードポリシーとともに、RA ガード機能が適切に動作できるように、ルータ側のポートで device-role router を設定した RA ガードポリシーを設定することが必須です。</p>
ステップ 4	<p>[no]hop-limit {maximum minimum} value</p> <p>例 :</p> <pre>(config-nd-raguard)# hop-limit maximum 33</pre>	<p>(1~255) 最大および最小のホップ制限値の範囲。</p> <p>ホップ制限値によるルータアドバタイズメントメッセージのフィルタリングを有効にします。不正 RA メッセージは低いホップ制限値 (IPv4 の Time to Live と同じ) を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。</p> <p>設定されていない場合、このフィルタは無効になります。「minimum」を設定して、指定する値より低いホップ制限値を持つ RA メッセージをブロックします。「maximum」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。</p>
ステップ 5	<p>[no]managed-config-flag {off on}</p> <p>例 :</p> <pre>(config-nd-raguard)# managed-config-flag on</pre>	<p>管理アドレス設定 (「M」フラグ) フィールドに基づいてルータアドバタイズメントメッセージのフィルタリングを有効にします。「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。設定されていない場合、このフィルタは無効になります。</p> <p>On : 「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。</p> <p>Off : 「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。</p>
ステップ 6	<p>[no]match {ipv6 access-list list ra prefix-list list}</p> <p>例 :</p>	<p>指定したプレフィックスリストまたはアクセスリストと照合します。</p>

	コマンドまたはアクション	目的
	<code>(config-nd-raguard)# match ipv6 access-list example_list</code>	
ステップ 7	<p><code>[no]other-config-flag {on off}</code></p> <p>例 :</p> <p><code>(config-nd-raguard)# other-config-flag on</code></p>	<p>その他の設定（「O」フラグ）フィールドに基づくルータ アドバタイズメントメッセージのフィルタリングを有効にします。「O」フィールドが1の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバを使用する場合があります。設定されていない場合、このフィルタは無効になります。</p> <p>On : 「O」値が1の RA メッセージを受け入れて転送し、0 のものをブロックします。</p> <p>Off : 「O」値が0の RA メッセージを受け入れて転送し、1 のものをブロックします。</p>
ステップ 8	<p><code>[no]router-preference maximum {high medium low}</code></p> <p>例 :</p> <p><code>(config-nd-raguard)# router-preference maximum high</code></p>	<p>「Router Preference」フラグを使用したルータ アドバタイズメントメッセージのフィルタリングを有効にします。設定されていない場合、このフィルタは無効になります。</p> <ul style="list-style-type: none"> • high : 「Router Preference」が「high」、 「medium」、または「low」に設定された RA メッセージを受け入れます。 • medium : 「Router Preference」が「high」に設定された RA メッセージをブロックします。 • low : 「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。
ステップ 9	<p><code>[no]trusted-port</code></p> <p>例 :</p> <p><code>(config-nd-raguard)# trusted-port</code></p>	<p>信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。</p>
ステップ 10	<p><code>default {device-role hop-limit {maximum minimum} managed-config-flag match {ipv6 access-list ra prefix-list } other-config-flag router-preference maximum trusted-port}</code></p> <p>例 :</p> <p><code>(config-nd-raguard)# default hop-limit</code></p>	<p>コマンドをデフォルト値に戻します。</p>
ステップ 11	<p><code>do show ipv6 nd raguard policy policy_name</code></p> <p>例 :</p> <p><code>(config-nd-raguard)# do show ipv6 nd raguard policy example_policy</code></p>	<p>(任意) : 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ないで ND ガードポリシー設定を表示します。</p>

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface** Interface_type stack/module/port
3. **ipv6 nd rguard** [**attach-policy** policy_name [**vlan** {vlan_ids | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids | **all**}] | **vlan** [{vlan_ids | **add** vlan_ids | **except** vlan_ids | **none** | **remove** vlan_ids | **all**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： # 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 Interface_type stack/module/port 例： (config)# interface gigabitethernet 1/1/4	インターフェイスのタイプおよび ID 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 3	ipv6 nd rguard [attach-policy policy_name [vlan {vlan_ids add vlan_ids except vlan_ids none remove vlan_ids all }] vlan [{vlan_ids add vlan_ids except vlan_ids none remove vlan_ids all }] 例： (config-if)# ipv6 nd rguard attach-policy example_policy or (config-if)# ipv6 nd rguard attach-policy example_policy vlan 222,223,224 or (config-if)# ipv6 nd rguard vlan 222, 223,224	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	do show running-config 例： #(config-if)# do show running-config	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 nd rguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interface** *portchannel_interface_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 range <i>Interface_name</i> 例： <code>(config)# interface Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。 ヒント インターフェイス名やタイプを簡単に参照するには <code>do show interfaces summary</code> コマンドを使用します。
ステップ 3	ipv6 nd rguard [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] 例： <code>(config-if-range)# ipv6 nd rguard attach-policy example_policy</code> or <code>(config-if-range)# ipv6 nd rguard attach-policy example_policy vlan 222,223,224</code> or <code>(config-if-range)# ipv6 nd rguard vlan 222,223,224</code>	RA ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
ステップ 4	do show running-config interfaceportchannel_interface_name 例 : <pre> #(config-if-range)# do show running-config int poll </pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre> # configure terminal </pre>	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	vlan configuration <i>vlan_list</i> 例 : <pre> (config)# vlan configuration 335 </pre>	VLAN インターフェイスのコンフィギュレーションモードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。
ステップ 3	ipv6 dhcp guard [attach-policy <i>policy_name</i>] 例 : <pre> (config-vlan-config)#ipv6 nd rguard attach-policy example_policy </pre>	すべてのスイッチおよびスタック インターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルトポリシーがアタッチされます。
ステップ 4	do show running-config 例 : <pre> #(config-if)# do show running-config </pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーの設定方法

IPv6 DHCP (DHCPv6) ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no]ipv6 dhcp guard policy *policy-name***
3. **[no]device-role {*client* | *server*}**
4. **[no] match server access-list *ipv6-access-list-name***
5. **[no] match reply prefix-list *ipv6-prefix-list-name***
6. **[no]preference { *max limit* | *min limit* }**
7. **[no] trusted-port**
8. **default {*device-role* | *trusted-port*}**
9. **do show ipv6 dhcp guard policy *policy_name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 guard policy <i>policy-name</i> 例： <code>(config)# ipv6 dhcp guard policy example_policy</code>	DHCPv6 ガード ポリシー名を指定し、DHCPv6 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	[no]device-role {<i>client</i> <i>server</i>} 例： <code>(config-dhcp-guard)# device-role server</code>	(任意) 特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは client です。 <ul style="list-style-type: none"> • client : デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバメッセージにはこのポートで破棄されます。 • server : 適用されたデバイスが DHCPv6 サーバであることを指定します。このポートでは、サーバメッセージが許可されます。
ステップ 4	[no] match server access-list <i>ipv6-access-list-name</i> 例： <code>;;Assume a preconfigured IPv6 Access List as</code>	(任意)。アドバタイズされた DHCPv6 サーバまたはリレー アドレスが認証されたサーバのアクセスリストからのものであることの確認を有効にします (アクセスリストの宛先アドレスは「any」です)。

	コマンドまたはアクション	目的
	<pre>follows: (config)# ipv6 access-list my_acls (config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any ;;configure DHCPv6 Guard to match approved access list. (config-dhcp-guard)# match server access-list my_acls</pre>	<p>設定されていない場合、このチェックは回避されます。空のアクセスリストは、permit allとして処理されます。</p>
ステップ 5	<p>[no] match reply prefix-list <i>ipv6-prefix-list-name</i></p> <p>例 :</p> <pre>;;Assume a preconfigured IPv6 prefix list as follows: (config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128 ;; Configure DHCPv6 Guard to match prefix (config-dhcp-guard)# match reply prefix-list my_prefix</pre>	<p>(任意) DHCPv6 応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクスリストからのものであることの確認を有効にします。設定されていない場合、このチェックは回避されます。空のプレフィクスリストは、permitとして処理されます。</p>
ステップ 6	<p>[no] preference { <i>max limit</i> <i>min limit</i> }</p> <p>例 :</p> <pre>(config-dhcp-guard)# preference max 250 (config-dhcp-guard)# preference min 150</pre>	<p>device-role が server である場合に max および min を設定して、DHCPv6 サーバアドバタイズメント値をサーバ優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。</p> <p>max limit : (0 ~ 255) (任意) 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。デフォルトは 255 です。設定されていない場合、このチェックは回避されます。</p> <p>min limit : (0 ~ 255) (任意) 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。デフォルトは 0 です。設定されていない場合、このチェックは回避されます。</p>
ステップ 7	<p>[no] trusted-port</p> <p>例 :</p> <pre>(config-dhcp-guard)# trusted-port</pre>	<p>(任意) trusted-port : ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。</p> <p>(注) 信頼できるポートを設定した場合、device-role オプションは使用できません。</p>
ステップ 8	<p>default { <i>device-role</i> <i>trusted-port</i> }</p> <p>例 :</p> <pre>(config-dhcp-guard)# default device-role</pre>	<p>(任意) default : コマンドをデフォルトに設定します。</p>

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

	コマンドまたはアクション	目的
ステップ 9	do show ipv6 dhcp guard policy <i>policy_name</i> 例 : <pre>(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy</pre>	(任意) コンフィギュレーションサブモードを終了せずに IPv6 DHCP のガード ポリシーの設定を表示します。 <i>policy_name</i> 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
  permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy poll
  device-role server
  match server access-list acl1
  match reply prefix-list abc
  preference min 0
  preference max 255
  trusted-port
interface GigabitEthernet 0/2/0
  switchport
  ipv6 dhcp guard attach-policy poll vlan add 1
  vlan 1
  ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll
```

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration *vlan_list***
3. **ipv6 dhcp guard [attach-policy *policy_name*]**
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre># configure terminal</pre>	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 2	vlan configuration <i>vlan_list</i> 例： <code>(config)# vlan configuration 334</code>	VLAN インターフェイスのコンフィギュレーションモードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	ipv6 dhcp guard [attach-policy <i>policy_name</i>] 例： <code>(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy</code>	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、 device-role client 、 no trusted-port です。
ステップ 4	do show running-config 例： <code>#(config-if) # do show running-config</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interfaceportchannel_interface_name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 range <i>Interface_name</i> 例： <code>(config)# interface Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

	コマンドまたはアクション	目的
		ヒント インターフェイス名やタイプを簡単に参照するには do show interfaces summary コマンドを使用します。
ステップ 3	ipv6 dhcp guard [attach-policy <i>policy_name</i> [vlan {<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all}] vlan [{<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all}] 例 : <pre>(config-if-range)# ipv6 dhcp guard attach-policy example_policy</pre> or <pre>(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</pre> or <pre>(config-if-range)# ipv6 dhcp guard vlan 222,223,224</pre>	DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	do show running-config interfaceportchannel <i>interface_name</i> 例 : <pre>#(config-if-range)# do show running-config int po11</pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガードポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順の概要

1. **configure terminal**
2. **vlan configuration *vlan_list***
3. **ipv6 dhcp guard [attach-policy *policy_name*]**
4. **do show running-config**

手順の詳細

	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
	<code># configure terminal</code>	
ステップ 2	vlan configuration <i>vlan_list</i> 例： <code>(config)# vlan configuration 334</code>	VLAN インターフェイスのコンフィギュレーションモードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	ipv6 dhcp guard [attach-policy <i>policy_name</i>] 例： <code>(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy</code>	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、 device-role client 、 no trusted-port です。
ステップ 4	do show running-config 例： <code>#(config-if)# do show running-config</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

IPv6 ソース ガードの設定方法

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 source-guard policy** *policy_name*
3. [**deny global-autoconf**] [**permit link-local**] [**default**{...}] [**exit**] [**no**{...}]
4. **end**
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code># configure terminal</code>	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 source-guard policy <i>policy_name</i> 例： <code>(config)# ipv6 source-guard policy example_policy</code>	IPv6 ソース ガード ポリシー名を指定し、IPv6 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 3	[deny global-autoconf] [permit link-local] [default {...}] [exit] [no {...}] 例：	(任意) IPv6 ソース ガード ポリシーを定義します。 <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
	<code>(config-sisf-sourceguard)# deny global-autoconf</code>	<p>します。これは、リンク上のすべてのグローバルアドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。</p> <ul style="list-style-type: none"> • permit link-local : リンクローカルアドレスから送信されたすべてのデータトラフィックを許可します。 <p>(注) ソース ガード ポリシーでは <code>trusted</code> オプションはサポートされません。</p>
ステップ 4	end 例 : <code>(config-sisf-sourceguard)# end</code>	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 5	show ipv6 source-guard policy <i>policy_name</i> 例 : <code># show ipv6 source-guard policy example_policy</code>	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次のタスク

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **configure terminal**
2. **interface** *Interface_type stack/module/port*
3. **ipv6 source-guard** [**attach-policy** *<policy_name>*]
4. **show ipv6 source-guard policy *policy_name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code># configure terminal</code>	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 2	interface <i>Interface_type stack/module/port</i> 例： (config)# interface gigabitethernet 1/1/4	インターフェイスのタイプおよび ID 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 3	ipv6 source-guard [attach-policy < <i>policy_name</i> >] 例： (config-if)# ipv6 source-guard attach-policy example_policy	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	show ipv6 source-guard policy <i>policy_name</i> 例： #(config-if)# show ipv6 source-guard policy example_policy	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. **configure terminal**
2. **interface port-channel** *port-channel-number*
3. **ipv6 source-guard** [**attach-policy** <*policy_name*>]
4. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： # 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 port-channel <i>port-channel-number</i> 例： (config)# interface Po4	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 3	ipv6 source-guard [attach-policy < <i>policy_name</i> >] 例： (config-if) # ipv6 source-guard attach-policy example_policy	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

	コマンドまたはアクション	目的
ステップ 4	show ipv6 source-guard policy <i>policy_name</i> 例 : <pre>(config-if) #show ipv6 source-guard policy example_policy</pre>	ポリシー設定と、そのポリシーが適用され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 ガードの設定方法



- (注) プレフィックスガードが適用されている場合にリンクローカルアドレスから送信されたルーティングプロトコル制御パケットを許可するには、ソースガードポリシー コンフィギュレーション モードで `permit link-local` コマンドを有効にします。

手順の概要

1. `[no] ipv6 source-guard policy source-guard-policy`
2. `[no] validate address`
3. `validate prefix`
4. `exit`
5. `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	[no] ipv6 source-guard policy <i>source-guard-policy</i> 例 : <pre>(config)# ipv6 source-guard policy my_snooping_policy</pre>	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 2	[no] validate address 例 : <pre>(config-sisf-sourceguard) # no validate address</pre>	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 3	validate prefix 例 : <pre>(config-sisf-sourceguard) # validate prefix</pre>	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 4	exit 例 : <pre>(config-sisf-sourceguard) # exit</pre>	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。

	コマンドまたはアクション	目的
ステップ 5	show ipv6 source-guard policy [<i>source-guard-policy</i>] 例 : # 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 プレフィックスガードポリシーをインターフェイスにアタッチする方法

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 source-guard attach-policy** policy_name
4. **show ipv6 source-guard policy** policy_name

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : # 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 Interface_type <i>stack/module/port</i> 例 : (config)# interface gigabitethernet 1/1/4	インターフェイスのタイプおよび ID 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 3	ipv6 source-guard attach-policy policy_name 例 : (config-if)# ipv6 source-guard attach-policy example_policy	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	show ipv6 source-guard policy policy_name 例 : (config-if)# show ipv6 source-guard policy example_policy	ポリシー設定と、そのポリシーが適用され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 ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

手順の概要

1. `configure terminal`
2. `interface port-channel port-channel-number`
3. `ipv6 source-guard [attach-policy <policy_name>]`
4. `show ipv6 source-guard policy policy_name`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： <code># configure terminal</code>	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	<code>interface port-channel port-channel-number</code> 例： <code>(config)# interface Po4</code>	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 3	<code>ipv6 source-guard [attach-policy <policy_name>]</code> 例： <code>(config-if)# ipv6 source-guard attach-policy example_policy</code>	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 <code>attach-policy</code> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<code>show ipv6 source-guard policy policy_name</code> 例： <code>(config-if)# show ipv6 source-guard policy example_policy</code>	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 ファースト ホップ セキュリティの設定例

例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard) # validate address
switch(config-sisf-sourceguard) # exit
```



```
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法