IPv6 ファーストホップセキュリティの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

IPv6 でのファーストホップセキュリティの前提条件

- IPv6 がイネーブルになった必要な SDM テンプレートが設定されていること。

- IPv6 ネイバー探索機能についての知識が必要です。 詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

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 チャネル）。

- FHS ポリシーは、レイヤ 2 EtherChannel インターフェイスまたは EtherChannel グループ内の VLAN に対してアタッチできます。
- FHS ポリシーはレイヤ 3 EtherChannel にアタッチすることはできません。
- 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。

IPv6 でファースト ホップ セキュリティに関する情報

First Hop Security in IPv6（FHS IPv6）は、ポリシーを物理インターフェイス、EtherChannel 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イネーブルにできるコンテナ ポリシーとして機能します。
- IPv6 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 インスペクションなど）によって使用されます。
- IPv6 ネイバー探索インスペクション：IPv6 ND インスペクションは、L2 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ドロップされます。 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。

- 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、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 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： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 snooping policy***policy-name* 例： `ControllerDevice(config)# ipv6 snooping policy example_policy`	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** *value*] | [**no**] | [**protocol** {**dhcp** | **ndp**}] | [**security-level** {**glean** | **guard** | **inspect**}] | [**tracking** {**disable** [**stale-lifetime** [*seconds* | **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] } 例： ControllerDevice(config-ipv6-snooping)# security-level inspect 例： ControllerDevice(config-ipv6-snooping)# trusted-port	データ アドレス グリーニングをイネーブルにし、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。 • （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ロールを指定します。 デフォルトは **node** です。 • （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。 **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**}：デフォルトのトラッキング動作を上書きし、トラッキング 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ディセーブルになります。 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

	コマンドまたはアクション	目的
		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： `ControllerDevice(config-ipv6-snooping)# exit`	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： `ControllerDevice#show ipv6 snooping policy example_policy`	スヌーピング ポリシー設定を表示します。

次の作業

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 ルータスヌーピング 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： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** Interface_type *stack/module/port* 例： `ControllerDevice(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	**switchport** 例： `ControllerDevice(config-if)# switchport`	switchport モードを開始します。 （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イネーブルになり、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。

ステップ 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**}]
	
	例：
	`ControllerDevice(config-if)# ipv6 snooping`
	
	or
	
	`ControllerDevice(config-if)# ipv6 snooping attach-policy example_policy`
	
	or
	`ControllerDevice(config-if)# ipv6 snooping vlan 111,112`
	
	or
	
	`ControllerDevice(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112`
		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。

	コマンドまたはアクション	目的
ステップ 5	**do show running-config** 例： `ControllerDevice#(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 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。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 snooping** [**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： `ControllerDevice# 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 range** *Interface_name* 例： `ControllerDevice(config)# interface range Po11`	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** *policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove** *vlan_ids*	**all**}]	**vlan** [{*vlan_ids*	**add**	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

	コマンドまたはアクション	目的

	vlan_ids | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`ControllerDevice(config-if-range)# ipv6 snooping attach-policy example_policy`
	
	`or`
	
	`ControllerDevice(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	
	`or`
	
	`ControllerDevice(config-if-range)#ipv6 snooping vlan 222, 223,224`
		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***portchannel_interface_name* 例： `ControllerDevice#(config-if-range)# do show running-config int po11`	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 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	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**vlan configuration** *vlan_list* 例： `ControllerDevice(config)# vlan configuration 333`	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 snooping** [**attach-policy** *policy_name*] 例： `ControllerDevice(config-vlan-config)#ipv6 snooping attach-policy example_policy`	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	**do show running-config** 例： `ControllerDevice#(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 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。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address* [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**tracking**{ [default | disable] [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] }]
3. [**no**] **ipv6 neighbor binding max-entries** *number* [**mac-limit** *number* | **port-limit** *number* [**mac-limit** *number*] | **vlan-limit** *number* [[**mac-limit** *number*] | [**port-limit** *number* [**mac-limit***number*]]]]
4. **ipv6 neighbor binding logging**
5. **exit**
6. **show ipv6 neighbor binding**

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： `ControllerDevice# 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 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address* [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**tracking**{ [default | disable] [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] }] 例： `ControllerDevice(config)# ipv6 neighbor binding`	
ステップ 3	[**no**] **ipv6 neighbor binding max-entries** *number* [**mac-limit** *number* | **port-limit** *number* [**mac-limit** *number*] | **vlan-limit** *number* [[**mac-limit** *number*] | [**port-limit** *number* [**mac-limit***number*]]]] 例： `ControllerDevice(config)# ipv6 neighbor binding max-entries 30000`	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。
ステップ 4	**ipv6 neighbor binding logging** 例： `ControllerDevice(config)# ipv6 neighbor binding logging`	バインディング テーブル メイン イベントのロギングをイネーブルにします。
ステップ 5	**exit** 例： `ControllerDevice(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権EXEC モードにします。
ステップ 6	**show ipv6 neighbor binding** 例： `ControllerDevice# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

IPv6 ネイバー探索インスペクション ポリシーの設定方法

特権 EXEC モードから、IPv6 ND インスペクション 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** | **monitor** | **router** | **switch**}
4. **drop-unsecure**
5. **limit address-count** *value*
6. **sec-level minimum** *value*
7. **tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}
8. **trusted-port**
9. **validate source-mac**
10. **no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
11. **default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
12. **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： `ControllerDevice# 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 nd inspection policy** *policy-name* 例： `ControllerDevice(config)# ipv6 nd inspection policy example_policy`	ND インスペクション ポリシー名を指定し、ND インスペクション 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**	**monitor**	**router**	**switch**} 例： `ControllerDevice(config-nd-inspection)# device-role switch`	ポートに接続されているデバイスのロールを指定します。 デフォルトは **host** です。
ステップ 4	**drop-unsecure** 例： `ControllerDevice(config-nd-inspection)# drop-unsecure`	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ステップ 5	**limit address-count** *value* 例： `ControllerDevice(config-nd-inspection)# limit address-count 1000`	1 ～ 10,000 を入力します。

	コマンドまたはアクション	目的
ステップ 6	**sec-level minimum** *value* 例： `ControllerDevice(config-nd-inspection)# limit address-count 1000`	暗号化生成アドレス（CGA）オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
ステップ 7	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： `ControllerDevice(config-nd-inspection)# tracking disable stale-lifetime infinite`	ポートでデフォルトのトラッキング ポリシーを上書きします。
ステップ 8	**trusted-port** 例： `ControllerDevice(config-nd-inspection)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 9	**validate source-mac** 例： `ControllerDevice(config-nd-inspection)# validate source-mac`	
ステップ 10	**no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `ControllerDevice(config-nd-inspection)# no validate source-mac`	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 11	**default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `ControllerDevice(config-nd-inspection)# default limit address-count`	設定をデフォルト値に戻します。
ステップ 12	**do show ipv6 nd inspection policy** *policy_name* 例： `ControllerDevice(config-nd-inspection)# do show ipv6 nd inspection policy example_policy`	ND インスペクション コンフィギュレーション モードを終了しないで ND インスペクションの設定を確認します。

IPv6 ネイバー探索インスペクション 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ース上の 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_id*s | **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： `ControllerDevice# 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： `ControllerDevice(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_id*s	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove** *vlan_ids*	**all**}] 例： `ControllerDevice(config-if)# ipv6 nd inspection attach-policy example_policy` or `ControllerDevice(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224` **or** `ControllerDevice(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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： `ControllerDevice#(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 ネイバー探索インスペクション 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 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_id*s | **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： `ControllerDevice# 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 range** *Interface_name* 例： `ControllerDevice(config)# interface range Po11`	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** *policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove** *vlan_ids*	**all**}]	**vlan** [{*vlan_id*s	**add**	ND インスペクション 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

	コマンドまたはアクション	目的

	vlan_ids | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`ControllerDevice(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	
	`or`
	
	`ControllerDevice(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	
	`or`
	
	`ControllerDevice(config-if-range)#ipv6 nd inspection vlan 222, 223,224`
		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***portchannel_interface_name* 例： `ControllerDevice#(config-if-range)# do show running-config int po11`	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ネイバー探索インスペクション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 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	**configure terminal** 例： `ControllerDevice# 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	**vlan configuration** *vlan_list* 例： `ControllerDevice(config)# vlan configuration 334`	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 nd inspection** [**attach-policy** *policy_name*] 例： `ControllerDevice(config-vlan-config)#ipv6 nd inspection attach-policy example_policy`	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： `ControllerDevice#(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 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 raguard 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 raguard 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： `ControllerDevice# 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 nd raguard policy** *policy-name* 例： `ControllerDevice(config)# ipv6 nd raguard policy example_policy`	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。
ステップ 3	[**no**]**device-role** {**host**	**monitor**	**router**	**switch**} 例： `ControllerDevice(config-nd-raguard)# device-role switch`	ポートに接続されているデバイスのロールを指定します。デフォルトは **host** です。
ステップ 4	[**no**]**hop-limit** {**maximum**	**minimum**} *value* 例： `ControllerDevice(config-nd-raguard)# hop-limit maximum 33`	（1 ～ 255）最大および最小のホップ制限値の範囲。 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イネーブルにします。 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。 設定されていない場合、このフィルタはディセーブルになります。 「**minimum**」を設定して、指定する値より低いホップ制限

	コマンドまたはアクション	目的
		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。
ステップ 5	[**no**]**managed-config-flag** {**off** | **on**} 例： `ControllerDevice(config-nd-raguard)# managed-config-flag on`	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イネーブルにします。「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、このフィルタはディセーブルになります。 **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。 **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。
ステップ 6	[**no**]**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} 例： `ControllerDevice(config-nd-raguard)# match ipv6 access-list example_list`	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。
ステップ 7	[**no**]**other-config-flag** {**on** | **off**} 例： `ControllerDevice(config-nd-raguard)# other-config-flag on`	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イネーブルにします。「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、このフィルタはディセーブルになります。 **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。 **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。
ステップ 8	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： `ControllerDevice(config-nd-raguard)# router-preference maximum high`	「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イネーブルにします。 設定されていない場合、このフィルタはディセーブルになります。 • **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。

	コマンドまたはアクション	目的
ステップ 9	**[no]trusted-port** 例： `ControllerDevice(config-nd-raguard)# trusted-port`	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。
ステップ 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**} 例： `ControllerDevice(config-nd-raguard)# default hop-limit`	コマンドをデフォルト値に戻します。
ステップ 11	**do show ipv6 nd raguard policy** *policy_name* 例： `ControllerDevice(config-nd-raguard)# do show ipv6 nd raguard policy example_policy`	（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。

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ース上の 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 raguard** [**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： `ControllerDevice# 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： `ControllerDevice(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 raguard** [**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：
	`ControllerDevice(config-if)# ipv6 nd raguard attach-policy example_policy`
	
	`or`
	
	`ControllerDevice(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	
	`or`
	
	`ControllerDevice(config-if)# ipv6 nd raguard 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： `ControllerDevice#(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2EtherChannel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 raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **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： `ControllerDevice# 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 range** *Interface_name* 例： `ControllerDevice(config)# interface range Po11`	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 raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids*	**add** *vlan_ids*	**except** *vlan_ids*	**none**	**remove** *vlan_ids*	**all**}]	**vlan** [{*vlan_id*s	**add** *vlan_ids*	**except***vlan_ids*	**none**	**remove** *vlan_ids*	**all**}] 例： `ControllerDevice(config-if-range)# ipv6 nd raguard attach-policy example_policy` `or` `ControllerDevice(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224` `or` `ControllerDevice(config-if-range)#ipv6 nd raguard vlan 222, 223,224`	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 interface***portchannel_interface_name* 例： `ControllerDevice#(config-if-range)# do show running-config int po11`	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： `ControllerDevice# 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	**vlan configuration** *vlan_list* 例： `ControllerDevice(config)# vlan configuration 335`	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** *policy_name*] 例： `ControllerDevice(config-vlan-config)#ipv6 nd raguard attach-policy example_policy`	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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： `ControllerDevice#(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 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： `ControllerDevice# 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 guard policy** *policy-name* 例： `ControllerDevice(config)# ipv6 dhcp guard policy example_policy`	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** {**client**	**server**} 例： `ControllerDevice(config-dhcp-guard)# device-role server`	（任意）特定のロール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。

	コマンドまたはアクション	目的
		• **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ドロップされます。 • **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** *ipv6-access-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`ControllerDevice(config)# ipv6 access-list my_acls`
	`ControllerDevice(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	
	`;;configure DCHPv6 Guard to match approved access list.`
	`ControllerDevice(config-dhcp-guard)# match server access-list my_acls`
		（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イネーブルにします（アクセスリストの宛先アドレスは「any」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。 空のアクセス リストは、permit all として処理されます。

ステップ 5	[**no**] **match reply prefix-list** *ipv6-prefix-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`ControllerDevice(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	
	`;; Configure DCHPv6 Guard to match prefix`
	`ControllerDevice(config-dhcp-guard)# match reply prefix-list my_prefix`
		（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。 空のプレフィクス リストは、permit として処理されます。

ステップ 6	[**no**]**preference**{ **max** *limit* | **min** *limit* }
	
	例：
	`ControllerDevice(config-dhcp-guard)# preference max 250`
	`ControllerDevice(config-dhcp-guard)#preference min 150`
		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。
		
		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イネーブルにします。 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。
		
		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イネーブルにします。 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。

	コマンドまたはアクション	目的
ステップ 7	**[no] trusted-port** 例： `ControllerDevice(config-dhcp-guard)# trusted-port`	（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。 （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。
ステップ 8	**default** {**device-role** | **trusted-port**} 例： `ControllerDevice(config-dhcp-guard)# default device-role`	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 9	**do show ipv6 dhcp guard policy** *policy_name* 例： `ControllerDevice(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy`	（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。*policy_name* 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 pol1
 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 pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

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。

手順の概要

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

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： `ControllerDevice# 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： `ControllerDevice(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 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_id*s | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	
	例：
	`ControllerDevice(config-if)# ipv6 dhcp guard attach-policy example_policy`
	
	or
	
	`ControllerDevice(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`ControllerDevice(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		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 interface** Interface_type *stack/module/port* 例： `ControllerDevice#(config-if)# do show running-config gig 1/1/4`	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 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： `ControllerDevice# 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 range** *Interface_name* 例： `ControllerDevice(config)# interface range Po11`	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 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**}]
	
	例：
	`ControllerDevice(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	
	or
	
	`ControllerDevice(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
		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。

	コマンドまたはアクション	目的
	`ControllerDevice(config-if-range)#ipv6 dhcp guard vlan 222, 223,224`	
ステップ 4	**do show running-config interface***portchannel_interface_name* 例： `ControllerDevice#(config-if-range)# do show running-config int po11`	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： `ControllerDevice# 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	**vlan configuration** *vlan_list* 例： `ControllerDevice(config)# vlan configuration 334`	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** *policy_name*] 例： `ControllerDevice(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy`	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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： `ControllerDevice#(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 VLAN にアタッチされていることを確認します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 ネットワーク管理とセキュリティのトピック	『IPv6 Configuration Library, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html
IPv6 コマンド リファレンス	『IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ)』 http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

セキュリティ コンフィギュレーション ガイド、Cisco IOS XE リリース 3E（Cisco WLC 5700 シリーズ）