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

- 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。

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。

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、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 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 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、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。
  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。

- 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 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

  ソース ガード パケットをデバッグするには、debug ipv6 snooping source-guard 特権 EXEC コマンドを使用します。

  次の制約事項が適用されます。

  - 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 ソース ガードがスイッチ ポートでイネーブルになっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングをイネーブルにする必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。

- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。
- インターフェイスで IPv4 および IPv6 のソース ガードを一緒に設定する場合は、**ip verify source** の代わりに **ip verify source mac-check** の使用を推奨します。2 つの異なるフィルタリング ルール（IPv4（IP フィルタ）用と IPv6（IP-MAC フィルタ）用）が設定されているため、特定のポートの IPv4 接続が切断される可能性があります。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを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。

  IPv6 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

  IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

SISF ベースの IPv4 および IPv6 デバイス トラッキングに関する情報

スイッチ統合セキュリティ機能ベース（SISF ベース）の IP デバイス トラッキングは、IP に依存しない CLI コマンドを使用して、IPv4 と IPv6 の両方で FHS が使用可能なスヌーピングおよびデバイス トラッキング機能を有効にするコンテナ ポリシーとして機能します。

SISF ベースの IP デバイス トラッキングおよびスヌーピング ポリシーを作成する方法

デバイス トラッキング 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

	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	**device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_policy`	デバイス トラッキング 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**}] | [**limit address-count** *value*] | [**no**] | [**destination-glean**{**recovery**|**log-only**[**dhcp**]] | [**data-glean**{**recovery**|**log-only**{**dhcp** | **ndp**}] | **prefix-glean**] | [**security-level** {**glean** | **guard** | **inspect**}] | [**tracking** {**disable** [**stale-lifetime** [*seconds* | **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] } 例： Device(config-device-tracking)# security-level inspect 例： Device(config-device-tracking)# trusted-port	IPv4 と IPv6 の両方で次のオプションを有効にします。 • （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）**destination-glean**{**recovery**| **log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。 • （任意）**data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。 • （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

	コマンドまたはアクション	目的
		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、ルータアドバタイズメント（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**}：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。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： `Device(config-device-tracking)# exit`	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 device-tracking policy** *policy-name* 例： `Device#show device-tracking policy example_policy`	デバイス トラッキング ポリシー設定を表示します。

デバイス トラッキング ポリシーをインターフェイスにアタッチする方法

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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***interface* 例： `Device(config)# interface gigabitethernet 1/1/4`	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 3	**device-trackingattach-policy** *policy name* 例： `Device(config-if)# device-tracking attach-policy example_policy`	デバイストラッキング 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で指定された VLAN にアタッチします。
ステップ 4	**show device-tracking policies** [**interface***interface*] 例： `Device#(config-if)# do show running-config`	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーを VLAN にアタッチする方法

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	デバイス トラッキング ポリシーをアタッチする VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	**device-tracking** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#device-tracking attach-policy example_policy`	すべてのスイッチ インターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。
ステップ 4	**do show running-config** 例： `Device#(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。

デバイス全体のエントリをバインディング テーブルに追加する方法

バインディング テーブルの内容を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	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	[**no**] **device-trackingDefault**| [**down-lifetime** *value*] | [**logging**] | [**max entries***value*] | [**reachable-lifetime** *seconds* | **retry-interval** *seconds*] | [**stale-lifetime**[*seconds*]	デバイス全体のデフォルト デバイス トラッキング ポリシーを作成し、エントリを次のオプションと共にバインディング テーブルに追加します。 • **down-lifetime**：エントリが削除される前に DOWN 状態で保持されるデフォルトの最長時間を設定します。

	コマンドまたはアクション	目的
	例： `Device(config)# device-tracking Default`	• **logging**：バインディング テーブル イベントを記録する syslog ロギングを有効にします。 • **max-entries**：バインディング テーブル内の最大エントリ数を定義します。 • **reachable-lifetime**：到達可能なエントリが到達可能性の証拠なしに直接的または間接的に到達可能であると見なされる最長時間を定義します。 • **retry-interval**：2 つのプローブの間隔を定義します。 • **stale-lifetime**：エントリが削除される前に Slate 状態で保持される最長時間を定義します。
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。

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

	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 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*	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。

	コマンドまたはアクション	目的
	| **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] } 例： Device(config-ipv6-snooping)# security-level inspect 例： Device(config-ipv6-snooping)# trusted-port	• （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。 • （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。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(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： `Device#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

	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** Interface_type *stack/module/port* 例： `Device(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： `Device(config-if)# switchport`	switchport モードを開始します。

	コマンドまたはアクション	目的
		（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：
	`Device(config-if)# ipv6 snooping`
	
	`or`
	
	`Device(config-if)# ipv6 snooping attach-policy example_policy`
	
	`or`
	`Device(config-if)# ipv6 snooping vlan 111,112`
	
	`or`
	
	`Device(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。

ステップ 5	**do show running-config** 例： `Device#(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

	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 range** *Interface_name* 例： `Device(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	**ipv6snooping** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	
	例：
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy`
	
	`or`
	
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(config-if-range)#ipv6 snooping vlan 222, 223,224`
		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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-configinterface***portchannel_interface_name* 例： `Device#(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

	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	**vlan configuration** *vlan_list* 例： `Device(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： `Device(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： `Device#(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

	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	[] [*vlan-id* {*ipv6-address* interface_type *stack/module/port hw_address* [[*seconds*		]	[{ [default	disable] [[*seconds*		]	[[[*seconds*		]	[{*seconds*| [[*seconds*		] }]**noipv6 neighbor bindingvlaninterfacereachable-lifetimevalue defaultinfinitetrackingreachable-lifetimevalue defaultinfiniteenablereachable-lifetimevalue defaultinfiniteretry-intervaldefaultreachable-lifetimevalue defaultinfinite** 例： `Device(config)# ipv6 neighbor binding`	バインディング テーブル データベースにスタティック エントリを追加します。
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： `Device(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 bindinglogging** 例： `Device(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： `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： `Device# 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

	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	[**no**]**ipv6 nd inspectionpolicy** *policy-name* 例： `Device(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： `Device(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： `Device(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： `Device(config-nd-inspection)# limit address-count 1000`	1 ～ 10,000 を入力します。
ステップ 6	**sec-level minimum** *value* 例： `Device(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： `Device(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。

	コマンドまたはアクション	目的
ステップ 8	**trusted-port** 例： `Device(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： `Device(config-nd-inspection)# validate source-mac`	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 10	**no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `Device(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： `Device(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： `Device(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

	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** Interface_type *stack/module/port* 例： `Device(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** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	
	例：
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy`
	
	or
	
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(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： `Device#(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

	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 range** *Interface_name* 例： `Device(config)# interface 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	**ipv6ndinspection** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	
	例：
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	
	or
	
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(config-if-range)#ipv6 nd inspection vlan 222, 223,224`
		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-configinterface***portchannel_interface_name* 例： `Device#(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

	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	**vlan configuration** *vlan_list* 例： `Device(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： `Device(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： `Device#(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

	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	[**no**]**ipv6 nd raguardpolicy** *policy-name* 例： `Device(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： `Device(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： `Device(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： `Device(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。

	コマンドまたはアクション	目的
		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： `Device(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： `Device(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： `Device(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。
ステップ 9	[**no**]**trusted-port** 例： `Device(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** }	コマンドをデフォルト値に戻します。

	コマンドまたはアクション	目的
	| **other-config-flag** | **router-preference maximum**| **trusted-port**} 例： `Device(config-nd-raguard)# default hop-limit`	
ステップ 11	**do show ipv6 nd raguard policy** *policy_name* 例： `Device(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

	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** Interface_type *stack/module/port* 例： `Device(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** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all** 例： `Device(config-if)# ipv6 nd raguard attach-policy example_policy`	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

	or
	
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(config-if)# ipv6 nd raguard vlan 222, 223,224`	

ステップ 4	**do show running-config** 例： `Device#(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

	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 range** *Interface_name* 例： `Device(config)# interface 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	**ipv6ndraguard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan**	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。

	コマンドまたはアクション	目的

	addexceptnoneremove allvlan addexceptnoneremove all
	
	例：
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	
	or
	
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(config-if-range)#ipv6 nd raguard vlan 222, 223,224`
		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-configinterface***portchannel_interface_name* 例： `Device#(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

	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	**vlan configuration** *vlan_list* 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6dhcp guard** [**attach-policy** *policy_name*] 例： `Device(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。
ステップ 4	**do show running-config** 例： `Device#(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

	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	[**no**]**ipv6 dhcp guardpolicy** *policy-name* 例： `Device(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： `Device(config-dhcp-guard)# device-role server`	（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。 • **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

	コマンドまたはアクション	目的
		トでは、サーバ メッセージが許可されます。

ステップ 4	[**no**] **matchserveraccess-list** *ipv6-access-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`Device(config)# ipv6 access-list my_acls`
	`Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	
	`;;configure DCHPv6 Guard to match approved access list.`
	`Device(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**] **matchreplyprefix-list** *ipv6-prefix-list-name*
	
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`Device(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	
	`;; Configure DCHPv6 Guard to match prefix`
	`Device(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：
	`Device(config-dhcp-guard)# preference max 250`
	`Device(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

	コマンドまたはアクション	目的
		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。
ステップ 7	[no] trusted-port 例： Device(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： Device(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： Device(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

	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** Interface_type *stack/module/port* 例： `Device(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** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	
	例：
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy`
	
	`or`
	
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	or
	
	`Device(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： `Device#(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

	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 range** *Interface_name* 例： `Device(config)# interface 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	**ipv6dhcpguard** [*policy_name* [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }] | [{*vlan_ids* | *vlan_ids* | *vlan_ids* | | *vlan_ids* | }]**attach-policyvlan addexceptnoneremove allvlan addexceptnoneremove all**
	
	例：
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	
	`or`
	
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	
	`or`
	
	`Device(config-if-range)#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-configinterface***portchannel_interface_name* 例： `Device#(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

	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	**vlan configuration** *vlan_list* 例： `Device(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： `Device(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。
ステップ 4	**do show running-config** 例： `Device#(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 ソース ガードの設定方法

手順

	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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
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	[**no**] **ipv6 source-guard policy** *policy_name* 例： `Device(config)# ipv6 source-guard policy example_policy`	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 4	[**deny global-autoconf**] [**permit link-local**] [**default**{...}] [**exit**] [**no**{...}] 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **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。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。 • **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。 （注） ソース ガード ポリシーに基づく信頼できるオプションはサポートされません。
ステップ 5	**end** 例： `Device(config-sisf-sourceguard)# end`	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 6	**show ipv6 source-guard policy** *policy_name* 例： `Device# 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。

次の作業

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

	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モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
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** Interface_type *stack/module/port* 例： `Device(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 4	**ipv6 source-guard**[**attach-policy** <*policy_name*>] 例： `Device(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 5	**show ipv6 source-guard policy** *policy_name* 例： `Device#(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

	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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
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 port-channel** *port-channel-number* 例： `Device (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 4	**ipv6 source-guard**[**attach-policy** <*policy_name*>] 例： `Device(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 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(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 コマンドをイネーブルにします。

手順

	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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**[no]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。
ステップ 4	**[no]validate address** 例： `Device (config-sisf-sourceguard)# no validate address`	アドレス検証機能をディセーブルにし、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 ソース ガードをイネーブルにし、IPv6 プレフィックスガード動作を実行します。
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。

	コマンドまたはアクション	目的
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

	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モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
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** Interface_type *stack/module/port* 例： `Device(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 4	**ipv6 source-guard attach-policy** *policy_name* 例： `Device(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 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(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

	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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
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 port-channel** *port-channel-number* 例： `Device (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 4	**ipv6 source-guard**[**attach-policy** <*policy_name*>] 例： `Device(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 5	**show ipv6 source-guard policy** *policy_name* 例： `Device(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 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
```

IPv6 ファースト ホップ セキュリティの機能情報

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 リリースのみを示しています。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 Cisco 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*：*IPv6* ファースト ホップ セキュリティの機能情報

機能名	リリース	機能情報
IPv6 ファースト ホップ セキュリティ	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ