



# Configuring IPv6 First Hop Security

- [Finding Feature Information, on page 1](#)
- [Prerequisites for First Hop Security in IPv6, on page 1](#)
- [Restrictions for First Hop Security in IPv6, on page 2](#)
- [Information about First Hop Security in IPv6, on page 2](#)
- [How to Configure an IPv6 Snooping Policy, on page 3](#)
- [How to Configure the IPv6 Binding Table Content , on page 7](#)
- [How to Configure an IPv6 Neighbor Discovery Inspection Policy, on page 9](#)
- [How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device, on page 13](#)
- [How to Configure an IPv6 Router Advertisement Guard Policy, on page 16](#)
- [How to Configure an IPv6 DHCP Guard Policy , on page 20](#)
- [How to Configure IPv6 Source Guard, on page 24](#)
- [How to Configure IPv6 Prefix Guard, on page 27](#)
- [Configuration Examples for IPv6 First Hop Security, on page 30](#)
- [Additional References, on page 31](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfngn.cisco.com/>. An account on Cisco.com is not required.

## Prerequisites for First Hop Security in IPv6

- You have configured the necessary IPv6 enabled SDM template.
- QoS should be enabled on the switch before configuring CoPP policies using **mls qos** command.

## Restrictions for First Hop Security in IPv6

- The following restrictions apply when applying FHS policies to EtherChannel interfaces (Port Channels):
  - A physical port with an FHS policy attached cannot join an EtherChannel group.
  - An FHS policy cannot be attached to a physical port when it is a member of an EtherChannel group.
- By default, a snooping policy has a security-level of guard. When such a snooping policy is configured on an access switch, external IPv6 Router Advertisement (RA) or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server packets are blocked, even though the uplink port facing the router or DHCP server/relay is configured as a trusted port. To allow IPv6 RA or DHCPv6 server messages, do the following:
  - Apply an IPv6 RA-guard policy (for RA) or IPv6 DHCP-guard policy (for DHCP server messages) on the uplink port.
  - Configure a snooping policy with a lower security-level, for example glean or inspect. However; configuring a lower security level is not recommended with such a snooping policy, because benefits of First Hop security features are not effective.
- The following restrictions apply for CoPP policies with IPv6 SISF-based device tracking policies due to limitation reported in [CSCvk32439](#):
  - CoPP policies are required to limit IPv6 NDP traffic when IPv6 SISF policies are configured on the switch.
  - After NDP CoPP policies are configured, limited traffic hits CPU. To accommodate the total end points connected, the number of NDP CoPP policies should be slightly more than the number of users connected to each switch in a stack. If you configure NDP CoPP policies less than the number of end points connected to the switch, the IP allocation to the end point is delayed but is not ignored completely.



---

**Note** For example, if a stack of 5 switches has approximately 300 users, the NDP CoPP policies should be more than 300.

---

- The DHCPv6 (server-to-client and client-to-server) CoPP policies are required only if Lightweight DHCPv6 Relay Agent (LDRA) is configured under IPv6 SISF-based device tracking policies on the switch.

## Information about First Hop Security in IPv6

First Hop Security in IPv6 (FHS IPv6) is a set of IPv6 security features, the policies of which can be attached to a physical interface, or a VLAN. An IPv6 software policy database service stores and accesses these policies. When a policy is configured or modified, the attributes of the policy are stored or updated in the software policy database, then applied as was specified. The following IPv6 policies are currently supported:

- IPv6 Snooping Policy—IPv6 Snooping Policy acts as a container policy that enables most of the features available with FHS in IPv6.
- IPv6 FHS Binding Table Content—A database table of IPv6 neighbors connected to the switch is created from information sources such as Neighbor Discovery (ND) protocol snooping. This database, or binding, table is used by various IPv6 guard features (such as IPv6 ND Inspection) to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.
- IPv6 Neighbor Discovery Inspection—IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database and IPv6 neighbor discovery messages that do not conform are dropped. An ND message is considered trustworthy if its IPv6-to-Media Access Control (MAC) mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities of the ND mechanism, such as attacks on DAD, address resolution, router discovery, and the neighbor cache.

- IPv6 Router Advertisement Guard—The IPv6 Router Advertisement (RA) guard feature enables the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network switch platform. RAs are used by routers to announce themselves on the link. The RA Guard feature analyzes the RAs and filters out bogus RAs sent by unauthorized routers. In host mode, all router advertisement and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 device with the information found in the received RA frame. Once the Layer 2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.
- IPv6 DHCP Guard—The IPv6 DHCP Guard feature blocks reply and advertisement messages that come from unauthorized DHCPv6 servers and relay agents. IPv6 DHCP guard can prevent forged messages from being entered in the binding table and block DHCPv6 server messages when they are received on ports that are not explicitly configured as facing a DHCPv6 server or DHCP relay. To use this feature, configure a policy and attach it to an interface or a VLAN. To debug DHCP guard packets, use the **debug ipv6 snooping dhcp-guard** privileged EXEC command.

## How to Configure an IPv6 Snooping Policy

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Snooping Policy :

### SUMMARY STEPS

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*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>ipv6 snooping policy <i>policy-name</i></b> <b>Example:</b> Device(config)# <b>ipv6 snooping policy example_policy</b>	Creates a snooping policy and enters IPv6 Snooping Policy Configuration mode.
<b>Step 3</b>	<pre>{[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 ] }</pre> <b>Example:</b> Device (config-ipv6-snooping) # <b>security-level inspect</b> <b>Example:</b> Device (config-ipv6-snooping) # <b>trusted-port</b>	Enables data address gleaning, validates messages against various criteria, specifies the security level for messages. <ul style="list-style-type: none"> <li>• (Optional) <b>default</b>—Sets all to default options.</li> <li>• (Optional) <b>device-role {node}   switch</b>—Specifies the role of the device attached to the port. Default is <b>node</b>.</li> <li>• (Optional) <b>limit address-count <i>value</i></b>—Limits the number of addresses allowed per target.</li> <li>• (Optional) <b>no</b>—Negates a command or sets it to defaults.</li> <li>• (Optional) <b>protocol {dhcp   ndp}</b>—Specifies which protocol should be redirected to the snooping feature for analysis. The default, is <b>dhcp</b> and <b>ndp</b>. To change the default, use the <b>no protocol</b> command.</li> <li>• (Optional) <b>security-level {glean guard inspect}</b>—Specifies the level of security enforced by the feature. Default is <b>guard</b>.               <ul style="list-style-type: none"> <li><b>glean</b>—Gleans addresses from messages and populates the binding table without any verification.</li> <li><b>guard</b>—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.</li> <li><b>inspect</b>—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.</li> </ul> </li> <li>• (Optional) <b>tracking {disable   enable}</b>—Overrides the default tracking behavior and specifies a tracking option.</li> <li>• (Optional) <b>trusted-port</b>—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over</li> </ul>

	Command or Action	Purpose
		bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Device(config-ipv6-snooping)# <b>exit</b>	Exits configuration modes to Privileged EXEC mode.
<b>Step 5</b>	<b>show ipv6 snooping policy <i>policy-name</i></b>  <b>Example:</b> Device# <b>show ipv6 snooping policy example_policy</b>	Displays the snooping policy configuration.

**What to do next**

Attach an IPv6 Snooping policy to interfaces or VLANs.

## How to Attach an IPv6 Snooping Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an interface or VLAN:

**SUMMARY STEPS**

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**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>interface</b> Interface_type <i>stack/module/port</i>  <b>Example:</b> Device(config)# <b>interface gigabitethernet 1/1/4</b>	Specifies an interface type and identifier; enters the interface configuration mode.
<b>Step 3</b>	<b>switchport</b>  <b>Example:</b>	Enters the Switchport mode.

	Command or Action	Purpose
	Device(config-if) # <b>switchport</b>	<b>Note</b> To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the switchport interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration. The command prompt displays as (config-if)# in Switchport configuration mode.
<b>Step 4</b>	<p><b>ipv6 snooping</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> {<i>vlan_id</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b><i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>} ]   <b>vlan</b> {<i>vlan_id</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b><i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ]</p> <p><b>Example:</b></p> <pre>Device(config-if) # ipv6 snooping</pre> <p>or</p> <pre>Device(config-if) # ipv6 snooping attach-policy example_policy</pre> <p>or</p> <pre>Device(config-if) # ipv6 snooping vlan 111,112</pre> <p>or</p> <pre>Device(config-if) # ipv6 snooping attach-policy example_policy vlan 111,112</pre>	Attaches a custom ipv6 snooping policy to the interface or the specified VLANs on the interface. To attach the default policy to the interface, use the <b>ipv6 snooping</b> command without the <b>attach-policy</b> keyword. To attach the default policy to VLANs on the interface, use the <b>ipv6 snooping vlan</b> command. The default policy is, security-level <b>guard</b> , device-role <b>node</b> , protocol <b>ndp</b> and <b>dhcp</b> .
<b>Step 5</b>	<p><b>do show running-config</b></p> <p><b>Example:</b></p> <pre>Device#(config-if) # do show running-config</pre>	Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.

## How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an EtherChannel interface or VLAN:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>interface range</b> <i>Interface_name</i> <b>Example:</b> Device(config)# <b>interface range Po11</b>	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.  <b>Tip</b> Enter the <b>do show interfaces summary</b> command for quick reference to interface names and types.
<b>Step 3</b>	<b>ipv6 snooping</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>Example:</b> Device(config-if-range)# <b>ipv6 snooping attach-policy example_policy</b>  or  Device(config-if-range)# <b>ipv6 snooping attach-policy example_policy vlan 222,223,224</b>  or  Device(config-if-range)# <b>ipv6 snooping vlan 222,223,224</b>	Attaches the IPv6 Snooping policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.
<b>Step 4</b>	<b>do show running-config interface</b> <i>portchannel_interface_name</i> <b>Example:</b> Device#(config-if-range)# <b>do show running-config int po11</b>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Configure the IPv6 Binding Table Content

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content :

### SUMMARY STEPS

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-limitnumber] ] ] ]`
4. `ipv6 neighbor binding logging`
5. `exit`
6. `show ipv6 neighbor binding`

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters the global configuration mode.
<b>Step 2</b>	<code>[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] } ] ] ]</code>  <b>Example:</b> Device(config)# <code>ipv6 neighbor binding</code>	Adds a static entry to the binding table database.
<b>Step 3</b>	<code>[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-limitnumber] ] ] ]</code>  <b>Example:</b> Device(config)# <code>ipv6 neighbor binding max-entries 30000</code>	Specifies the maximum number of entries that are allowed to be inserted in the binding table cache.
<b>Step 4</b>	<b>ipv6 neighbor binding logging</b>  <b>Example:</b> Device(config)# <code>ipv6 neighbor binding logging</code>	Enables the logging of binding table main events.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config)# <code>exit</code>	Exits global configuration mode, and places the router in privileged EXEC mode.
<b>Step 6</b>	<b>show ipv6 neighbor binding</b>  <b>Example:</b> Device# <code>show ipv6 neighbor binding</code>	Displays contents of a binding table.



# How to Configure an IPv6 Neighbor Discovery Inspection Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 ND Inspection Policy:

## SUMMARY STEPS

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***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
Step 2	<b>[no]ipv6 nd inspection policy <i>policy-name</i></b>  <b>Example:</b> Device(config)# <b>ipv6 nd inspection policy example_policy</b>	Specifies the ND inspection policy name and enters ND Inspection Policy configuration mode.
Step 3	<b>device-role {host   monitor   router   switch}</b>  <b>Example:</b> Device(config-nd-inspection)# <b>device-role switch</b>	Specifies the role of the device attached to the port. The default is <b>host</b> .
Step 4	<b>drop-unsecure</b>  <b>Example:</b> Device(config-nd-inspection)# <b>drop-unsecure</b>	Drops messages with no or invalid options or an invalid signature.
Step 5	<b>limit address-count <i>value</i></b>  <b>Example:</b> Device(config-nd-inspection)# <b>limit address-count 1000</b>	Enter 1–10,000.

	Command or Action	Purpose
<b>Step 6</b>	<b>sec-level minimum</b> <i>value</i> <b>Example:</b> Device(config-nd-inspection)# <b>limit address-count</b> 1000	Specifies the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used.
<b>Step 7</b>	<b>tracking</b> { <b>enable</b> [ <b>reachable-lifetime</b> { <i>value</i>   <b>infinite</b> }]   <b>disable</b> [ <b>stale-lifetime</b> { <i>value</i>   <b>infinite</b> }]} <b>Example:</b> Device(config-nd-inspection)# <b>tracking disable</b> <b>stale-lifetime infinite</b>	Overrides the default tracking policy on a port.
<b>Step 8</b>	<b>trusted-port</b> <b>Example:</b> Device(config-nd-inspection)# <b>trusted-port</b>	Configures a port to become a trusted port.
<b>Step 9</b>	<b>validate source-mac</b> <b>Example:</b> Device(config-nd-inspection)# <b>validate source-mac</b>	Checks the source media access control (MAC) address against the link-layer address.
<b>Step 10</b>	<b>no</b> { <b>device-role</b>   <b>drop-unsecure</b>   <b>limit address-count</b>   <b>sec-level minimum</b>   <b>tracking</b>   <b>trusted-port</b>   <b>validate source-mac</b> } <b>Example:</b> Device(config-nd-inspection)# <b>no validate</b> <b>source-mac</b>	Remove the current configuration of a parameter with the <b>no</b> form of the command.
<b>Step 11</b>	<b>default</b> { <b>device-role</b>   <b>drop-unsecure</b>   <b>limit address-count</b>   <b>sec-level minimum</b>   <b>tracking</b>   <b>trusted-port</b>   <b>validate source-mac</b> } <b>Example:</b> Device(config-nd-inspection)# <b>default limit</b> <b>address-count</b>	Restores configuration to the default values.
<b>Step 12</b>	<b>do show ipv6 nd inspection policy</b> <i>policy_name</i> <b>Example:</b> Device(config-nd-inspection)# <b>do show ipv6 nd</b> <b>inspection policy example_policy</b>	Verifies the ND Inspection Configuration without exiting ND inspection configuration mode.

## How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface

Starting with Cisco IOS XE Amsterdam 17.1.1 the IPv6 ND Inspection feature is deprecated and the SISF-based device tracking feature replaces it. For the corresponding replacement task, see *Attaching a Device Tracking Policy to an Interface* under the *Configuring SISF-Based Device Tracking* chapter in this document.

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 ND Inspection policy to an interface or VLANs on an interface :

## SUMMARY STEPS

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**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
Step 2	<b>interface</b> <i>Interface_type stack/module/port</i> <b>Example:</b> Device(config)# <b>interface gigabitethernet 1/1/4</b>	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	<b>ipv6 nd inspection</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>Example:</b> Device(config-if)# <b>ipv6 nd inspection attach-policy example_policy</b> or Device(config-if)# <b>ipv6 nd inspection attach-policy example_policy vlan 222,223,224</b> or Device(config-if)# <b>ipv6 nd inspection vlan 222,223,224</b>	Attaches the Neighbor Discovery Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.
Step 4	<b>do show running-config</b> <b>Example:</b> Device#(config-if)# <b>do show running-config</b>	Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.

## How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface

Starting with Cisco IOS XE Amsterdam 17.1.1 the IPv6 ND Inspection feature is deprecated and the SISF-based device tracking feature replaces it. For the corresponding replacement task, see *Attaching a Device Tracking Policy to an Interface* under the *Configuring SISF-Based Device Tracking* chapter in this document.

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Neighbor Discovery Inspection policy on an EtherChannel interface or VLAN:

### SUMMARY STEPS

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 interface** *portchannel\_interface\_name*

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>interface range</b> <i>Interface_name</i> <b>Example:</b> Device(config)# <b>interface Po11</b>	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.  <b>Tip</b> Enter the <b>do show interfaces summary</b> command for quick reference to interface names and types.
<b>Step 3</b>	<b>ipv6 nd inspection</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>Example:</b> Device(config-if-range)# <b>ipv6 nd inspection attach-policy example_policy</b> or Device(config-if-range)# <b>ipv6 nd inspection attach-policy example_policy vlan 222,223,224</b> or Device(config-if-range)# <b>ipv6 nd inspection vlan 222, 223,224</b>	Attaches the ND Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.

	Command or Action	Purpose
<b>Step 4</b>	<b>do show running-config</b> <b>interface</b> <i>portchannel_interface_name</i>  <b>Example:</b> Device# (config-if-range)# <b>do show running-config</b> <b>int poll</b>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device

To attach an IPV6 Neighbor Discovery Multicast Suppress policy on a device, complete the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy** *policy-name*
4. **mode dad-proxy**
5. **mode full-proxy**
6. **mode mc-proxy**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>ipv6 nd suppress policy</b> <i>policy-name</i>	Defines the Neighbor Discovery suppress policy name and enters Neighbor Discovery suppress policy configuration mode.
<b>Step 4</b>	<b>mode dad-proxy</b>	Enables Neighbor Discovery suppress in IPv6 DAD proxy mode.
<b>Step 5</b>	<b>mode full-proxy</b>	Enables Neighbor Discovery suppress to proxy multicast and unicast Neighbor Solicitation messages.
<b>Step 6</b>	<b>mode mc-proxy</b>	Enables Neighbor Discovery suppress to proxy multicast Neighbor Solicitation messages.

# How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on an Interface

To attach an IPv6 Neighbor Discovery Multicast Suppress policy on an interface, complete the following steps:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Perform one of the following tasks:
  - **interface** *type number*
  - **ipv6 nd inspection** [**attach-policy** *policy\_name* [ **vlan** { **add** | **except** | **none** | **remove** | **all** } *vlan* [ *vlan1, vlan2, vlan3...* ] ] ]
  - OR
  - **vlan configuration** *vlan-id*
  - **ipv6 nd inspection** [**attach-policy** *policy\_name* [ **vlan** { **add** | **except** | **none** | **remove** | **all** } *vlan* [ *vlan1, vlan2, vlan3...* ] ] ]
4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	Perform one of the following tasks: <ul style="list-style-type: none"> <li>• <b>interface</b> <i>type number</i></li> <li>• <b>ipv6 nd inspection</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b>   <b>all</b> } <i>vlan</i> [ <i>vlan1, vlan2, vlan3...</i> ] ] ]</li> <li>OR</li> <li>• <b>vlan configuration</b> <i>vlan-id</i></li> <li>• <b>ipv6 nd inspection</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b>   <b>all</b> } <i>vlan</i> [ <i>vlan1, vlan2, vlan3...</i> ] ] ]</li> </ul>	Specifies an interface type and number, and places the device in interface configuration mode.  Attaches the IPv6 Neighbor Discovery Multicast Policy to an interface or a VLAN.
<b>Step 4</b>	<b>exit</b>	Exists the interface configuration mode.

# How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy to a Layer 2 EtherChannel Interface

To attach an IPv6 Neighbor Discovery Multicast Suppress policy on an EtherChannel interface, complete the following steps:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Perform one of the following tasks:
  - **interface port-channel** *port-channel-number*
  - **ipv6 nd inspection** [**attach-policy** *policy\_name* [ **vlan** { **add** | **except** | **none** | **remove** | **all** } *vlan* [ *vlan1*, *vlan2*, *vlan3*... ]]]
  - OR
  - **vlan configuration** *vlan-id*
  - **ipv6 nd inspection** [**attach-policy** *policy\_name* [ **vlan** { **add** | **except** | **none** | **remove** | **all** } *vlan* [ *vlan1*, *vlan2*, *vlan3*... ]]]
4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters the global configuration mode.
Step 3	Perform one of the following tasks: <ul style="list-style-type: none"> <li>• <b>interface port-channel</b> <i>port-channel-number</i></li> <li>• <b>ipv6 nd inspection</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b>   <b>all</b> } <i>vlan</i> [ <i>vlan1</i>, <i>vlan2</i>, <i>vlan3</i>... ]]]</li> <li>OR</li> <li>• <b>vlan configuration</b> <i>vlan-id</i></li> <li>• <b>ipv6 nd inspection</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b>   <b>all</b> } <i>vlan</i> [ <i>vlan1</i>, <i>vlan2</i>, <i>vlan3</i>... ]]]</li> </ul>	Specifies an interface type and port number and places the switch in the port channel configuration mode.  Attaches the IPv6 Neighbor Discovery Multicast Policy to an interface or a VLAN.
Step 4	<b>exit</b>	Exists the interface configuration mode.

# How to Configure an IPv6 Router Advertisement Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 Router Advertisement policy :

## SUMMARY STEPS

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***

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>[no]ipv6 nd rguard policy <i>policy-name</i></b> <b>Example:</b> Device(config)# <b>ipv6 nd rguard policy example_policy</b>	Specifies the RA Guard policy name and enters RA Guard Policy configuration mode.
<b>Step 3</b>	<b>[no]device-role {host   monitor   router   switch}</b> <b>Example:</b> Device(config-nd-rguard)# <b>device-role switch</b>	Specifies the role of the device attached to the port. The default is <b>host</b> .
<b>Step 4</b>	<b>[no]hop-limit {maximum   minimum} <i>value</i></b> <b>Example:</b> Device(config-nd-rguard)# <b>hop-limit maximum 33</b>	(1–255) Range for Maximum and Minimum Hop Limit values.  Enables filtering of Router Advertisement messages by the Hop Limit value. A rogue RA message may have a low Hop Limit value (equivalent to the IPv4 Time to Live) that when accepted by the host, prevents the host from generating traffic to destinations beyond the rogue RA message generator. An RA message with an unspecified Hop Limit value is blocked.  If not configured, this filter is disabled. Configure <b>minimum</b> to block RA messages with Hop Limit values



	Command or Action	Purpose
		lower than the value you specify. Configure <b>maximum</b> to block RA messages with Hop Limit values greater than the value you specify.
<b>Step 5</b>	<p><b>[no]managed-config-flag {off   on}</b></p> <p><b>Example:</b></p> <pre>Device(config-nd-raguard)# managed-config-flag on</pre>	<p>Enables filtering of Router Advertisement messages by the Managed Address Configuration, or "M" flag field. A rogue RA message with an M field of 1 can cause a host to use a rogue DHCPv6 server. If not configured, this filter is disabled.</p> <p><b>On</b>—Accepts and forwards RA messages with an M value of 1, blocks those with 0.</p> <p><b>Off</b>—Accepts and forwards RA messages with an M value of 0, blocks those with 1.</p>
<b>Step 6</b>	<p><b>[no]match {ipv6 access-list list   ra prefix-list list}</b></p> <p><b>Example:</b></p> <pre>Device(config-nd-raguard)# match ipv6 access-list example_list</pre>	Matches a specified prefix list or access list.
<b>Step 7</b>	<p><b>[no]other-config-flag {on   off}</b></p> <p><b>Example:</b></p> <pre>Device(config-nd-raguard)# other-config-flag on</pre>	<p>Enables filtering of Router Advertisement messages by the Other Configuration, or "O" flag field. A rogue RA message with an O field of 1 can cause a host to use a rogue DHCPv6 server. If not configured, this filter is disabled.</p> <p><b>On</b>—Accepts and forwards RA messages with an O value of 1, blocks those with 0.</p> <p><b>Off</b>—Accepts and forwards RA messages with an O value of 0, blocks those with 1.</p>
<b>Step 8</b>	<p><b>[no]router-preference maximum {high   medium   low}</b></p> <p><b>Example:</b></p> <pre>Device(config-nd-raguard)# router-preference maximum high</pre>	<p>Enables filtering of Router Advertisement messages by the Router Preference flag. If not configured, this filter is disabled.</p> <ul style="list-style-type: none"> <li>• <b>high</b>—Accepts RA messages with the Router Preference set to high, medium, or low.</li> <li>• <b>medium</b>—Blocks RA messages with the Router Preference set to high.</li> <li>• <b>low</b>—Blocks RA messages with the Router Preference set to medium and high.</li> </ul>
<b>Step 9</b>	<p><b>[no]trusted-port</b></p> <p><b>Example:</b></p> <pre>Device(config-nd-raguard)# trusted-port</pre>	When configured as a trusted port, all attached devices are trusted, and no further message verification is performed.
<b>Step 10</b>	<p><b>default {device-role   hop-limit {maximum   minimum}   managed-config-flag   match {ipv6 access-list   ra</b></p>	Restores a command to its default value.

	Command or Action	Purpose
	<b>prefix-list }   other-config-flag   router-preference maximum   trusted-port}</b> <b>Example:</b> Device (config-nd-raguard) # <b>default hop-limit</b>	
<b>Step 11</b>	<b>do show ipv6 nd raguard policy <i>policy_name</i></b> <b>Example:</b> Device (config-nd-raguard) # <b>do show ipv6 nd raguard policy example_policy</b>	(Optional)—Displays the ND Guard Policy configuration without exiting the RA Guard policy configuration mode.

## How to Attach an IPv6 Router Advertisement Guard Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement policy to an interface or to VLANs on the interface :

### SUMMARY STEPS

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**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>Interface_type stack/module/port</i> <b>Example:</b> Device (config) # <b>interface gigabitethernet 1/1/4</b>	Specifies an interface type and identifier; enters the interface configuration mode.
<b>Step 3</b>	<b>ipv6 nd raguard [attach-policy <i>policy_name</i> [ <b>vlan</b> {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ]   <b>vlan</b> [ {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ] ]</b> <b>Example:</b> Device (config-if) # <b>ipv6 nd raguard attach-policy example_policy</b>  or	Attaches the Neighbor Discovery Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.

	Command or Action	Purpose
	<pre>Device(config-if)# ipv6 nd rguard attach-policy example_policy vlan 222,223,224  or  Device(config-if)# ipv6 nd rguard vlan 222, 223,224</pre>	
<b>Step 4</b>	<p><b>do show running-config</b></p> <p><b>Example:</b></p> <pre>Device#(config-if)# do show running-config</pre>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement Guard Policy on an EtherChannel interface or VLAN:

### SUMMARY STEPS

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 interfaceportchannel\_interface\_name**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters the global configuration mode.
<b>Step 2</b>	<p><b>interface range</b> <i>Interface_name</i></p> <p><b>Example:</b></p> <pre>Device(config)# interface Po11</pre>	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.  <b>Tip</b> Enter the <b>do show interfaces summary</b> command for quick reference to interface names and types.
<b>Step 3</b>	<p><b>ipv6 nd rguard</b> [<b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ]   <b>vlan</b> [ {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ]</p>	Attaches the RA Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-if-range)# ipv6 nd rguard attach-policy example_policy</pre> <p>or</p> <pre>Device(config-if-range)# ipv6 nd rguard attach-policy example_policy vlan 222,223,224</pre> <p>or</p> <pre>Device(config-if-range)#ipv6 nd rguard vlan 222, 223,224</pre>	
<b>Step 4</b>	<p><b>do show running-config</b> <i>interfaceportchannel_interface_name</i></p> <p><b>Example:</b></p> <pre>Device#(config-if-range)# do show running-config int po11</pre>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Configure an IPv6 DHCP Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 DHCP (DHCPv6) Guard policy:

### SUMMARY STEPS

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*

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters the global configuration mode.
<b>Step 2</b>	<p><b>[no]ipv6 dhcp guard policy</b> <i>policy-name</i></p> <p><b>Example:</b></p>	Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.

	Command or Action	Purpose
	Device(config)# <b>ipv6 dhcp guard policy example_policy</b>	
<b>Step 3</b>	<p><b>[no]device-role {client   server}</b></p> <p><b>Example:</b></p> <pre>Device(config-dhcp-guard)# <b>device-role server</b></pre>	<p>(Optional) Filters out DHCPv6 replies and DHCPv6 advertisements on the port that are not from a device of the specified role. Default is <b>client</b>.</p> <ul style="list-style-type: none"> <li>• <b>client</b>—Default value, specifies that the attached device is a client. Server messages are dropped on this port.</li> <li>• <b>server</b>—Specifies that the attached device is a DHCPv6 server. Server messages are allowed on this port.</li> </ul>
<b>Step 4</b>	<p><b>[no] match server access-list ipv6-access-list-name</b></p> <p><b>Example:</b></p> <pre>;;Assume a preconfigured IPv6 Access List as follows: Device(config)# <b>ipv6 access-list my_acls</b> Device(config-ipv6-acl)# <b>permit host FE80::A8BB:CCFF:FE01:F700 any</b>  ;;configure DHCPv6 Guard to match approved access list. Device(config-dhcp-guard)# <b>match server access-list my_acls</b></pre>	<p>(Optional). Enables verification that the advertised DHCPv6 server or relay address is from an authorized server access list (The destination address in the access list is 'any'). If not configured, this check will be bypassed. An empty access list is treated as a permit all.</p>
<b>Step 5</b>	<p><b>[no] match reply prefix-list ipv6-prefix-list-name</b></p> <p><b>Example:</b></p> <pre>;;Assume a preconfigured IPv6 prefix list as follows: Device(config)# <b>ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128</b>  ;; Configure DHCPv6 Guard to match prefix Device(config-dhcp-guard)# <b>match reply prefix-list my_prefix</b></pre>	<p>(Optional) Enables verification of the advertised prefixes in DHCPv6 reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.</p>
<b>Step 6</b>	<p><b>[no]preference{ max limit   min limit }</b></p> <p><b>Example:</b></p> <pre>Device(config-dhcp-guard)# <b>preference max 250</b> Device(config-dhcp-guard)#<b>preference min 150</b></pre>	<p>Configure <b>max</b> and <b>min</b> when <b>device-role</b> is <b>server</b> to filter DHCPv6 server advertisements by the server preference value. The defaults permit all advertisements.</p> <p><b>max limit</b>—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. Default is 255. If not specified, this check will be bypassed.</p> <p><b>min limit</b>—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. Default is 0. If not specified, this check will be bypassed.</p>

	Command or Action	Purpose
<b>Step 7</b>	<b>[no] trusted-port</b> <b>Example:</b> Device(config-dhcp-guard) # <b>trusted-port</b>	(Optional) <b>trusted-port</b> —Sets the port to a trusted mode. No further policing takes place on the port. <b>Note</b> If you configure a trusted port then the device-role option is not available.
<b>Step 8</b>	<b>default {device-role   trusted-port}</b> <b>Example:</b> Device(config-dhcp-guard) # <b>default device-role</b>	(Optional) <b>default</b> —Sets a command to its defaults.
<b>Step 9</b>	<b>do show ipv6 dhcp guard policy policy_name</b> <b>Example:</b> Device(config-dhcp-guard) # <b>do show ipv6 dhcp guard policy example_policy</b>	(Optional) Displays the configuration of the IPv6 DHCP guard policy without leaving the configuration submode. Omitting the <i>policy_name</i> variable displays all DHCPv6 policies.

### Example of DHCPv6 Guard Configuration

```
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
```

## How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content :

### SUMMARY STEPS

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\_ids | add vlan\_ids | exceptvlan\_ids | none | remove vlan\_ids | all} ]**
4. **do show running-config interface** Interface\_type stack/module/port

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
Step 2	<b>interface</b> Interface_type <i>stack/module/port</i> <b>Example:</b> Device(config)# <b>interface gigabitethernet 1/1/4</b>	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	<b>ipv6 dhcp guard</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>Example:</b> Device(config-if)# <b>ipv6 dhcp guard attach-policy example_policy</b>  or Device(config-if)# <b>ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</b>  or Device(config-if)# <b>ipv6 dhcp guard vlan 222,223,224</b>	Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.
Step 4	<b>do show running-config interface</b> Interface_type <i>stack/module/port</i> <b>Example:</b> Device#(config-if)# <b>do show running-config gig 1/1/4</b>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 DHCP Guard policy on an EtherChannel interface or VLAN:

## SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>interface range</b> <i>Interface_name</i> <b>Example:</b> Device(config)# <b>interface Po11</b>	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.  <b>Tip</b> Enter the <b>do show interfaces summary</b> command for quick reference to interface names and types.
<b>Step 3</b>	<b>ipv6 dhcp guard</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>Example:</b> Device(config-if-range)# <b>ipv6 dhcp guard attach-policy example_policy</b>  or  Device(config-if-range)# <b>ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</b>  or  Device(config-if-range)# <b>ipv6 dhcp guard vlan 222, 223,224</b>	Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the <b>attach-policy</b> option is not used.
<b>Step 4</b>	<b>do show running-config interfaceportchannel_interface_name</b> <b>Example:</b> Device#(config-if-range)# <b>do show running-config int po11</b>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

## How to Configure IPv6 Source Guard

### SUMMARY STEPS

1. enable
2. configure terminal



3. `[no] ipv6 source-guard policy policy_name`
4. `[deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]`
5. `end`
6. `show ipv6 source-guard policy policy_name`

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters the global configuration mode.
<b>Step 3</b>	<b>[no] ipv6 source-guard policy policy_name</b> <b>Example:</b> <pre>Device(config)# ipv6 source-guard policy example_policy</pre>	Specifies the IPv6 Source Guard policy name and enters IPv6 Source Guard policy configuration mode.
<b>Step 4</b>	<b>[deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]</b> <b>Example:</b> <pre>Device(config-sisf-sourceguard)# deny global-autoconf</pre>	(Optional) Defines the IPv6 Source Guard policy. <ul style="list-style-type: none"> <li>• <b>deny global-autoconf</b>—Denies data traffic from auto-configured global addresses. This is useful when all global addresses on a link are DHCP-assigned and the administrator wants to block hosts with self-configured addresses to send traffic.</li> <li>• <b>permit link-local</b>—Allows all data traffic that is sourced by a link-local address.</li> </ul> <p><b>Note</b> Trusted option under source guard policy is not supported.</p>
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config-sisf-sourceguard)# end</pre>	Exits out of IPv6 Source Guard policy configuration mode.
<b>Step 6</b>	<b>show ipv6 source-guard policy policy_name</b> <b>Example:</b> <pre>Device# show ipv6 source-guard policy example_policy</pre>	Shows the policy configuration and all the interfaces where the policy is applied.

### What to do next

Apply the IPv6 Source Guard policy to an interface.

## How to Attach an IPv6 Source Guard Policy to an Interface

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters the global configuration mode.
<b>Step 3</b>	<b>interface Interface_type stack/module/port</b> <b>Example:</b> Device(config)# <code>interface gigabitethernet 1/1/4</code>	Specifies an interface type and identifier; enters the interface configuration mode.
<b>Step 4</b>	<b>ipv6 source-guard [attach-policy &lt;policy_name&gt; ]</b> <b>Example:</b> Device(config-if)# <code>ipv6 source-guard attach-policy example_policy</code>	Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <b>attach-policy</b> option is not used.
<b>Step 5</b>	<b>show ipv6 source-guard policy policy_name</b> <b>Example:</b> Device#(config-if)# <code>show ipv6 source-guard policy example_policy</code>	Shows the policy configuration and all the interfaces where the policy is applied.

## How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface port-channel port-channel-number`

4. `ipv6 source-guard [attach-policy <policy_name> ]`
5. `show ipv6 source-guard policy policy_name`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters the global configuration mode.
Step 3	<b>interface port-channel</b> <i>port-channel-number</i> <b>Example:</b> Device (config)# <code>interface Po4</code>	Specifies an interface type and port number and places the switch in the port channel configuration mode.
Step 4	<b>ipv6 source-guard</b> [attach-policy <policy_name> ] <b>Example:</b> Device(config-if) # <code>ipv6 source-guard attach-policy example_policy</code>	Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <b>attach-policy</b> option is not used.
Step 5	<b>show ipv6 source-guard policy</b> <i>policy_name</i> <b>Example:</b> Device(config-if) # <code>show ipv6 source-guard policy example_policy</code>	Shows the policy configuration and all the interfaces where the policy is applied.

## How to Configure IPv6 Prefix Guard



**Note** To allow routing protocol control packets sourced by a link-local address when prefix guard is applied, enable the `permit link-local` command in the source-guard policy configuration mode.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `[no] ipv6 source-guard policy source-guard-policy`
4. `[ no ] validate address`
5. `validate prefix`
6. `exit`

## 7. show ipv6 source-guard policy [*source-guard-policy*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>[no] ipv6 source-guard policy <i>source-guard-policy</i></b> <b>Example:</b> Device(config)# <b>ipv6 source-guard policy my_snooping_policy</b>	Defines an IPv6 source-guard policy name and enters switch integrated security features source-guard policy configuration mode.
<b>Step 4</b>	<b>[ no ] validate address</b> <b>Example:</b> Device(config-sisf-sourceguard)# <b>no validate address</b>	Disables the validate address feature and enables the IPv6 prefix guard feature to be configured.
<b>Step 5</b>	<b>validate prefix</b> <b>Example:</b> Device(config-sisf-sourceguard)# <b>validate prefix</b>	Enables IPv6 source guard to perform the IPv6 prefix-guard operation.
<b>Step 6</b>	<b>exit</b> <b>Example:</b> Device(config-sisf-sourceguard)# <b>exit</b>	Exits switch integrated security features source-guard policy configuration mode and returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ipv6 source-guard policy [<i>source-guard-policy</i>]</b> <b>Example:</b> Device# <b>show ipv6 source-guard policy policy1</b>	Displays the IPv6 source-guard policy configuration.

## How to Attach an IPv6 Prefix Guard Policy to an Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *Interface\_type stack/module/port*
4. **ipv6 source-guard attach-policy** *policy\_name*

5. `show ipv6 source-guard policy policy_name`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters the global configuration mode.
Step 3	<b>interface</b> <i>Interface_type stack/module/port</i> <b>Example:</b> Device(config)# <code>interface gigabitethernet 1/1/4</code>	Specifies an interface type and identifier; enters the interface configuration mode.
Step 4	<b>ipv6 source-guard attach-policy policy_name</b> <b>Example:</b> Device(config-if)# <code>ipv6 source-guard attach-policy example_policy</code>	Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <b>attach-policy</b> option is not used.
Step 5	<b>show ipv6 source-guard policy policy_name</b> <b>Example:</b> Device(config-if)# <code>show ipv6 source-guard policy example_policy</code>	Shows the policy configuration and all the interfaces where the policy is applied.

## How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
	Device> <b>enable</b>	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>interface port-channel</b> <i>port-channel-number</i> <b>Example:</b> Device (config)# <b>interface Po4</b>	Specifies an interface type and port number and places the switch in the port channel configuration mode.
<b>Step 4</b>	<b>ipv6 source-guard</b> [ <b>attach-policy</b> < <i>policy_name</i> > ] <b>Example:</b> Device(config-if)# <b>ipv6 source-guard attach-policy example_policy</b>	Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <b>attach-policy</b> option is not used.
<b>Step 5</b>	<b>show ipv6 source-guard policy</b> <i>policy_name</i> <b>Example:</b> Device(config-if)# <b>show ipv6 source-guard policy example_policy</b>	Shows the policy configuration and all the interfaces where the policy is applied.

## Configuration Examples for IPv6 First Hop Security

### Examples: How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface:

```
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)#
```

### Examples: How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface:

```
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
```

## Additional References

### Related Documents

Related Topic	Document Title
Implementing IPv6 Addressing and Basic Connectivity	<a href="http://www.cisco.com/.../ipconfig/3y6ad.html">http://www.cisco.com/.../ipconfig/3y6ad.html</a>
IPv6 network management and security topics	IPv6 Configuration Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) <a href="http://www.cisco.com/.../ipconfig/3850e38.html">http://www.cisco.com/.../ipconfig/3850e38.html</a>
IPv6 Command Reference	IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) <a href="http://www.cisco.com/.../ipconfig/3850e38.html">http://www.cisco.com/.../ipconfig/3850e38.html</a>

### Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

