



IPv6 RA Guard

Last Updated: August 27, 2012

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform.

- [Finding Feature Information, page 1](#)
- [Restrictions for IPv6 RA Guard, page 1](#)
- [Information About IPv6 RA Guard, page 2](#)
- [How to Configure IPv6 RA Guard, page 2](#)
- [Configuration Examples for IPv6 RA Guard, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for IPv6 RA Guard, page 8](#)

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 RA Guard

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is supported on EtherChannel, but not on EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- This feature is supported on auxiliary VLANs and private VLANs (PVLANS). In the case of PVLANS, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
- If the **platform ipv6 acl icmp optimize neighbor-discovery command** is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

Information About IPv6 RA Guard

- [IPv6 Global Policies, page 2](#)
- [IPv6 RA Guard, page 2](#)

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 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.

How to Configure IPv6 RA Guard

- [Configuring the IPv6 RA Guard Policy on the Device, page 3](#)
- [Configuring IPv6 RA Guard on an Interface, page 5](#)

Configuring the IPv6 RA Guard Policy on the Device

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 nd rguard policy *policy-name*
4. device-role {host | router}
5. hop-limit {maximum | minimum *limit*}
6. managed-config-flag {on | off}
7. match ipv6 access-list *ipv6-access-list-name*
8. match ra prefix-list *ipv6-prefix-list-name*
9. other-config-flag {on | off}
10. router-preference maximum {high | low | medium}
11. trusted-port
12. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>ipv6 nd rguard policy <i>policy-name</i></p> <p>Example:</p> <pre>Device(config)# ipv6 nd rguard policy policy1</pre>	<p>Defines the RA guard policy name and enters RA guard policy configuration mode.</p>
Step 4	<p>device-role {host router}</p> <p>Example:</p> <pre>Device(config-ra-guard)# device-role router</pre>	<p>Specifies the role of the device attached to the port.</p>

Command or Action	Purpose
Step 5 hop-limit { maximum minimum <i>limit</i> } Example: Device(config-ra-guard)# hop-limit minimum 3	(Optional) Enables verification of the advertised hop count limit. <ul style="list-style-type: none"> If not configured, this check will be bypassed.
Step 6 managed-config-flag { on off } Example: Device(config-ra-guard)# managed-config-flag on	(Optional) Enables verification that the advertised managed address configuration flag is on. <ul style="list-style-type: none"> If not configured, this check will be bypassed.
Step 7 match ipv6 access-list <i>ipv6-access-list-name</i> Example: Device(config-ra-guard)# match ipv6 access-list list1	(Optional) Enables verification of the sender's IPv6 address in inspected messages from the configured authorized device source access list. <ul style="list-style-type: none"> If not configured, this check will be bypassed.
Step 8 match ra prefix-list <i>ipv6-prefix-list-name</i> Example: Device(config-ra-guard)# match ra prefix-list listname1	(Optional) Enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. <ul style="list-style-type: none"> If not configured, this check will be bypassed.
Step 9 other-config-flag { on off } Example: Device(config-ra-guard)# other-config-flag on	(Optional) Enables verification of the advertised “other” configuration parameter.
Step 10 router-preference maximum { high low medium } Example: Device(config-ra-guard)# router-preference maximum high	(Optional) Enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit.
Step 11 trusted-port Example: Device(config-ra-guard)# trusted-port	(Optional) Specifies that this policy is being applied to trusted ports. <ul style="list-style-type: none"> All RA guard policing will be disabled.
Step 12 exit Example: Device(config-ra-guard)# exit	Exits RA guard policy configuration mode and returns to global configuration mode.

Configuring IPv6 RA Guard on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd rguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1*, *vlan2*, *vlan3*...]]]
5. **exit**
6. **show ipv6 nd rguard policy** [*policy-name*]
7. **debug ipv6 snooping rguard** [*filter* | *interface* | *vlanid*]

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 interface <i>type number</i></p> <p>Example:</p> <pre>Device(config)# interface fastethernet 3/13</pre>	<p>Specifies an interface type and number, and places the device in interface configuration mode.</p>
<p>Step 4 ipv6 nd rguard attach-policy [<i>policy-name</i> [vlan {add except none remove all} <i>vlan</i> [<i>vlan1</i>, <i>vlan2</i>, <i>vlan3</i>...]]]</p> <p>Example:</p> <pre>Device(config-if)# ipv6 nd rguard attach-policy</pre>	<p>Applies the IPv6 RA Guard feature to a specified interface.</p>
<p>Step 5 exit</p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	<p>Exits interface configuration mode.</p>

Command or Action	Purpose
Step 6 <code>show ipv6 nd raguard policy [policy-name]</code> Example: Device# <code>show ipv6 nd raguard policy raguard1</code>	Displays the RA guard policy on all interfaces configured with the RA guard.
Step 7 <code>debug ipv6 snooping raguard [filter interface vlanid]</code> Example: Device# <code>debug ipv6 snooping raguard</code>	Enables debugging for IPv6 RA guard snooping information.

Configuration Examples for IPv6 RA Guard

- [Example: IPv6 RA Guard Configuration, page 6](#)
- [Example: Configuring IPv6 ND Inspection and RA Guard, page 6](#)

Example: IPv6 RA Guard Configuration

```

Device(config)# interface fastethernet 3/13

Device(config-if)# ipv6 nd raguard attach-policy

Device# show running-config interface fastethernet 3/13

Building configuration...
Current configuration : 129 bytes
!
interface FastEthernet3/13
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end

```

Example: Configuring IPv6 ND Inspection and RA Guard

This example provides information about an interface on which both the Neighbor Discovery Inspection and RA Guard features are configured:

```

Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol      Protocol value  Message  Value  Action  Feature
ICMP          58              RS       85     punt   RA Guard
              58              RA       86     drop   ND Inspection
              58              NS       87     punt   RA guard
              58              NA       88     punt   ND Inspection

```

ICMP	58	REDIR	89	drop punt	RA Guard ND Inspection
------	----	-------	----	--------------	---------------------------

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 RA Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for IPv6 RA Guard

Feature Name	Releases	Feature Information
IPv6 RA Guard	12.2(33)SX14	The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform.
	12.2(50)SY	
	12.2(54)SG	
	15.0(2)SE	
	15.0(2)SG	The following commands were introduced or modified: debug ipv6 snooping raguard , device-role , hop-limit , ipv6 nd raguard attach-policy , ipv6 nd raguard policy , managed-config-flag , match ipv6 access-list , match ra prefix-list , other-config-flag , router-preference maximum , show ipv6 nd raguard policy .
	15.2(4)S	
	15.2(4)M	
	Cisco IOS XE Release 3.2SE	
Cisco IOS XE Release 3.2SG		

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.