

IPv6 RA Guard

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.

- Restrictions for IPv6 RA Guard, on page 1
- Information About IPv6 RA Guard, on page 2
- How to Configure IPv6 RA Guard, on page 2
- Configuration Examples for IPv6 RA Guard, on page 5
- Additional References, on page 6
- Feature Information for IPv6 RA Guard, on page 7

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 not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- 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

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.

In the wireless deployment RAs coming on wireless ports are dropped as routers cannot reside on these interfaces.

How to Configure IPv6 RA Guard

Configuring the IPv6 RA Guard Policy on the Device



Note When the **ipv6 nd raguard** command is configured on ports, router solicitation messages are not replicated to these ports. To replicate router solicitation messages, all ports that face routers must be set to the router role.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard 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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Device(config)# ipv6 nd raguard policy policy1`	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 4	**device-role** {**host**	**router**} **Example:** `Device(config-ra-guard)# device-role router`	Specifies the role of the device attached to the port.
Step 5	**hop-limit** {**maximum**	**minimum** *limit*} **Example:** `Device(config-ra-guard)# hop-limit minimum 3`	(Optional) Enables verification of the advertised hop count limit. • 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. • If not configured, this check will be bypassed.
Step 7	**match ipv6 access-list** *ipv6-access-list-name* **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. • If not configured, this check will be bypassed.
Step 8	**match ra prefix-list** *ipv6-prefix-list-name* **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. • If not configured, this check will be bypassed.

	Command or Action	Purpose
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. • 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 raguard attach-policy** [*policy-name* [**vlan** {**add** \| **except** \| **none** \| **remove** \| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
5. **exit**
6. **show ipv6 nd raguard policy** [*policy-name*]
7. **debug ipv6 snooping raguard** [*filter* \| *interface* \| *vlanid*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 3/13`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] **Example:** `Device(config-if)# ipv6 nd raguard attach-policy`	Applies the IPv6 RA Guard feature to a specified interface.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**show ipv6 nd raguard policy** [*policy-name*] **Example:** `Device# show ipv6 nd raguard policy raguard1`	Displays the RA guard policy on all interfaces configured with the RA guard.
Step 7	**debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*] **Example:** `Device# debug ipv6 snooping raguard`	Enables debugging for IPv6 RA guard snooping information.

Configuration Examples for IPv6 RA Guard

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
                                                  punt      ND Inspection
ICMP         58               RA        86        drop      RA guard
                                                  punt      ND Inspection
ICMP         58               NS        87        punt      ND Inspection
ICM          58               NA        88        punt      ND Inspection
ICMP         58               REDIR     89        drop      RA Guard
                                                  punt      ND Inspection
```

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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)SXI4 12.2(50)SY 12.2(54)SG 15.0(2)SE 15.0(2)SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.2SG	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**.