Configuring IPv6 RA Guard

Restrictions for IPv6 Router Advertisement Guard

- The IPv6 Router Advertisement 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.

- Packets dropped by the IPv6 Router Advertisement Guard feature can be spanned.

Information About IPv6 Router Advertisement Guard

The following sections provide information on IPv6 global policies and IPv6 router advertisement guard.

About IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 neighbor discovery inspection and IPv6 router advertisement guard are IPv6 global policies features. Every time an neighbor discovery

inspection or router advertisement 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.

About IPv6 Router Advertisement Guard

The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices. In host mode, all router advertisement and router redirect messages are disallowed on the port. The router advertisement guard feature compares configuration information on the Layer 2 device with the information found in the received router advertisement frame. Once the Layer 2 device has validated the content of the router advertisement frame and router redirect frame against the configuration, it forwards the router advertisement to its unicast or multicast destination. If the router advertisement frame content is not validated, the router advertisement is dropped.

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

How to Configure IPv6 Router Advertisement Guard

The following section provides information on configuring IPv6 router advertisement guard policy on a device and configuring router advertisement on an interface

Configuring the IPv6 Router Advertisement Guard Policy on the Device

To configure IPv6 router advertisement guard policy on the device, perform this procedure:

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 router advertisement guard policy name and enters router advertisement guard policy configuration mode.

	Command or Action	**Purpose**
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.
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 router advertisement guard policing will be disabled.
Step 12	**exit** **Example:** Device(config-ra-guard)# **exit**	Exits router advertisement guard policy configuration mode and returns to global configuration mode.

Configuring IPv6 Router Advertisement Guard on an Interface

To configure IPv6 router advertisement guard on an interface, perform this procedure:

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	**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 Router Advertisement 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 router advertisement guard policy on all interfaces configured with the router advertisement guard.
Step 7	**debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*] **Example:** `Device# debug ipv6 snooping raguard`	Enables debugging for IPv6 router advertisement guard snooping information.

Configuration Examples for IPv6 Router Advertisement Guard

The following sections provide configuration examples for IPv6 router advertisement guard.

Example: Configuring IPv6 Router Advertisement Guard

The following example shows how to configure IPv6 router advertisement guard:

```
Device> enable
Device# configure terminal
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: Viewing IPv6 Neighbor Discovery Inspection and Router Advertisement Guard Configurations on an Interface

The following example shows information about an interface on which both the neighbor discovery inspection and router advertisement guard are configured.

```
Device> enable
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
```

Feature Information for Configuring IPv6 Router Advertisement 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 Configuring IPv6 Router Advertisement Guard

Feature Name	Releases	Feature Information
Configuring IPv6 Router Advertisement Guard	Cisco IOS Release 15.2(7)E1	The feature was introduced.