Configuring IPv6 First Hop Security

IPv6 First Hop Security Overview

First Hop Security in IPv6 (FHS IPv6) is a set of IPv6 security features, whose policies can be attached to an interface or a VLAN. The following IPv6 policies are supported:

- DHCPv6 Guard
- IPv6 Router Advertisement (RA) Guard

Overview of DHCPv6 Guard

The DHCPv6 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 following privileged EXEC command.

debug ipv6 snooping dhcp-guard [**filter** <*name*>] [**interface** <*interface-id*>] [**vlan** <*vlanid*>]

Restrictions of DHCPv6 Guard

The DHCPv6 guard feature is not supported on EtherChannel ports.

Overview of IPv6 RA 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 device platform. RAs are used by devices to announce themselves on the link. The RA Guard feature analyzes the RAs and filters out bogus RAs sent by unauthorized devices. 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.

To debug RA guard packets, use the following privileged EXEC command.

debug ipv6 snooping raguard [**filter** <*name*>] [**interface** <*interface-id*>] [**vlan** <*vlanid*>]

Limitations and Restrictions of 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.

Configuring an IPv6 DHCP Guard Policy

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

Procedure

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

	Command or Action	Purpose
Step 3	**ipv6 dhcp guard policy** *policy-name* **Example:** `Router(config)# ipv6 dhcp guard policy policy1`	Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.
Step 4	**device-role** {**client** | **monitor** | **server**} **Example:** `Router(config-dhcp-guard)# device-role server`	(Optional) Filters out DHCPv6 replies and DHCPv6 advertisements on the port that are not from a device of the specified role. Default is **client**. • **client**—Default value, specifies that the attached device is a client. Server messages are dropped on this port. • **server**—Specifies that the attached device is a DHCPv6 server. Server messages are allowed on this port.
Step 5	**trusted-port** **Example:** `Router(config-dhcp-guard)# trusted-port`	(Optional) **trusted-port**—Sets the port to a trusted mode. No further policing takes place on the port. **Note** If you configure a trusted port then the device-role option is not available.
Step 6	**end** **Example:** `Router(config-dhcp-guard)# end`	Exits DHCPv6 Guard Policy configuration mode and returns to privileged EXEC mode.
Step 7	**show ipv6 dhcp guard policy** *policy_name* **Example:** `Router# show ipv6 dhcp guard policy policy1`	(Optional) Displays the configuration of the IPv6 DHCP guard policy. Omitting the *policy_name* variable displays all DHCPv6 policies.

Attaching an IPv6 DHCP Guard Policy to an Interface or a VLAN

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/0`	Specifies an interface type and identifier, and enters interface configuration mode.
Step 4	**ipv6 dhcp guard** [**attach-policy** *policy_name*] **Example:** `Router(config-if)# ipv6 dhcp guard attach-policy policy1`	Attaches the DHCP Guard policy to the interface or the specified VLAN.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show ipv6 dhcp guard policy** *policy_name* **Example:** `Router# show ipv6 dhcp guard policy1`	(Optional) Displays the policy configuration as well as all the interfaces where the policy is applied.

Configuring an IPv6 Router Advertisement Guard Policy

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Router(config)# ipv6 nd raguard policy example_policy`	Specifies the RA guard policy name and enters RA guard policy configuration mode.
Step 4	**device-role {host | monitor | router | switch}** **Example:**	Specifies the role of the device attached to the port. The default is **host**.

	Command or Action	Purpose
	`Router(config-nd-raguard)# device-role switch`	**Note** For a network with both host-facing ports and router-facing ports, along with a RA guard policy configured with **device-role host** on host-facing ports or vlan, it is mandatory to configure a RA guard policy with **device-role router** on router-facing ports to allow the RA Guard feature to work properly.
Step 5	**hop-limit** {**maximum** | **minimum**} *value* **Example:** `Router(config-nd-raguard)# hop-limit maximum 33`	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. (1–255) Range for Maximum and Minimum Hop Limit values. If not configured, this filter is disabled. Configure **minimum** to block RA messages with Hop Limit values lower than the value you specify. Configure **maximum**to block RA messages with Hop Limit values greater than the value you specify.
Step 6	**managed-config-flag** {**off** | **on**} *value* **Example:** `Router(config-nd-raguard)# managed-config-flag on`	Enables filtering of Router Advertisement messages by the managed address configuration, or "M" flag field. A rouge 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. **On**—Accepts and forwards RA messages with an M value of 1, blocks those with 0. **Off**—Accepts and forwards RA messages with an M value of 0, blocks those with 1.
Step 7	**other-config-flag** {**on** | **off**} **Example:** `Device(config-ra-guard)# other-config-flag on`	(Optional) Enables verification of the advertised “other” configuration parameter.
Step 8	**router-preference maximum** {**high** | **medium** | **low**} **Example:**	Enables filtering of Router Advertisement messages by the router preference flag. If not configured, this filter is disabled.

	Command or Action	Purpose
	`Router(config-nd-raguard)# router-preference maximum high`	• **high**—Accepts RA messages with the router preference set to high, medium, or low. • **medium**—Blocks RA messages with the router preference set to high. • **low**—Blocks RA messages with the router preference set to medium and high.
Step 9	**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} **Example:** `Router(config-nd-raguard)# match ipv6 access-list example_list`	Matches a specified prefix list or access list.
Step 10	**trusted-port** **Example:** `Router(config-nd-raguard)# trusted-port`	When configured as a trusted port, all attached devices are trusted, and no further message verification is performed.
Step 11	**end** **Example:** `Router(config-nd-raguard)# end`	Exits RA Guard policy configuration mode and returns to privileged EXEC mode.
Step 12	**show ipv6 nd raguard policy** *policy_name* **Example:** `Router# show ipv6 nd raguard policy example_policy`	(Optional)—Displays the ND guard policy configuration.

Attaching an IPv6 Router Advertisement Guard Policy to an Interface or a VLAN

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

Procedure

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Specifies an interface type and identifier; enters the interface configuration mode.

Step 4	**ipv6 nd raguard** [**attach-policy** *policy_name*]
	Example:
	`Router(config-if)# ipv6 nd raguard attach-policy example_policy`
	`Router(config-vlan-config)# ipv6 nd raguard attach-policy example_policy`
		Attaches the Neighbor Discovery Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the **attach-policy** option is not used.

Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.