



Configuring IPv6 First-Hop Security

This chapter describes how to configure IPv6 First-Hop Security on Cisco NX-OS devices and includes the following sections:

- [Introduction to First-Hop Security, on page 1](#)
- [RA Guard, on page 2](#)
- [DHCPv6 Guard, on page 3](#)
- [IPv6 Snooping, on page 3](#)
- [How to Configure IPv6 FHS, on page 5](#)
- [Configuration Examples, on page 13](#)
- [Additional References for IPv6 First-Hop Security, on page 14](#)

Introduction to First-Hop Security

The Layer 2 and Layer 3 switches operate in the Layer 2 domains with technologies, such as server virtualization, Overlay Transport Virtualization (OTV), and Layer 2 mobility. These devices are sometimes referred to as "first hops", specifically when they are facing end nodes. The First-Hop Security feature provides end node protection and optimizes link operations on IPv6 or dual-stack networks.

First-Hop Security (FHS) is a set of features to optimize IPv6 link operation, as well as help with scale in large L2 domains. These features provide protection from a wide host of rogue or mis-configured users, and this can be extended with additional features for different deployment scenarios, or attack vectors.

The following FHS features are supported:

- IPv6 RA Guard
- DHCPv6 Guard
- IPv6 Snooping



Note Use the **feature dhcp** command to enable the FHS feature.

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 snooping, DHCPv6 guard, and IPv6 RA guard are IPv6 global policies features. Every time IPv6 snooping, DHCPv6 guard, or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface or VLAN, and the software policy database entry is updated to include this interface to which the policy is applied.

All port level FHS policies are programmed in the ifacl region, while the VLAN level policies are programmed in the FHS region. Use the **hardware profile tcam region fhs *tcam_size*** command to configure the FHS region. The range for the TCAM size is 0-4096.

All FHS packets take the **copp-s-dhcpreq** queue for software processing.

IPv6 First-Hop Security Binding Table

A database of table of IPv6 neighbors connected to the device is created from information sources, such as IPv6 snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

RA Guard

Overview of 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.

Guidelines and Limitations of IPv6 RA Guard

The guidelines and limitations of IPv6 RA Guard are as follows:

- 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 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.
- IPv6 RA Guard cannot be enabled if SFLOW is enabled.
- IPv6 RA Guard cannot be enabled on VXLAN ports.
- 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.

DHCPv6 Guard

Overview of DHCP—DHCPv6 Guard

The DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked. The filtering decision is determined by the device role assigned to the receiving switch port, trunk, or VLAN.

Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of DHCP server advertisements occurs for server preference checking.

If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

Guidelines and Limitations of DHCPv6 Guard

The guidelines and limitations of DHCPv6 Guard are as follows:

- If a packet arriving from the DHCP server is a Relay Forward or a Relay Reply, only the device role is checked. In addition, IPv6 DHCP Guard does not apply the policy for a packet sent out by the local relay agent running on the switch.
- DHCP Guard cannot be enabled if SFLOW is enabled.
- DHCP Guard is not supported on VXLAN ports.

IPv6 Snooping

Overview of IPv6 Snooping

IPv6 "snooping," feature bundles several Layer 2 IPv6 first-hop security features, which operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 snooping learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes snooping messages in order to build a trusted binding table. IPv6 snooping messages that do not have valid bindings are dropped. An IPv6 snooping message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

When IPv6 snooping is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the snooping protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For snooping traffic, Neighbor Discovery Protocol (NDP) messages are directed to SISF. For DHCPv6, UDP messages sourced from `dhcpv6_client` and `dhcpv6_server` ports are redirected.

IPv6 snooping registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 snooping entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 snooping decision.

IPv6 snooping provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

Additionally, IPv6 snooping is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects snooping and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

Guidelines and Limitations for IPv6 Snooping

The guidelines and limitations of IPv6 Snooping are as follows:

- You must perform the same configurations on both the vPC peers.
- The IPv6 Snooping feature is supported only in the hardware when the ternary content addressable memory (TCAM) is programmed.
- The IPv6 Snooping feature can be configured on a switch port interface or on the VLAN only ingress port.
- The tracking functionality of the IPv6 snooping policy will not work if the Neighbor Discovery protocol is disabled in the configured IPv6 snooping policy.
- For the IPv6 Snooping to learn DHCP bindings, it must see both, the server and the client replies. A IPv6 snooping policy must be attached to both the client facing interface (or VLAN), as well as the DHCP server facing interface (or VLAN). In the case of a DHCP Relay, a IPv6 snooping policy must be attached at the VLAN level to see the server replies.

How to Configure IPv6 FHS

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ipv6 nd raguard policy <i>policy-name</i> Example: Device(config)# ipv6 nd raguard policy policy1	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 3	device-role {host router monitor switch} Example: Device(config-ra-guard)# device-role router	Specifies the role of the device attached to the port.
Step 4	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 5	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 6	other-config-flag {on off} Example: Device(config-ra-guard)# other-config-flag on	(Optional) Enables verification of the advertised “other” configuration parameter.

	Command or Action	Purpose
Step 7	router-preference maximum {high low medium} Example: <pre>Device(config-ra-guard)# router-preference maximum high</pre>	(Optional) Enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit.
Step 8	trusted-port Example: <pre>Device(config-ra-guard)# trusted-port</pre>	(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 9	exit Example: <pre>Device(config-ra-guard)# exit</pre>	Exits RA guard policy configuration mode and returns to global configuration mode.

Configuring IPv6 RA Guard on an Interface

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	interface type number Example: <pre>Device(config)# interface fastethernet 3/13</pre>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 3	ipv6 nd raguard attach-policy [policy-name] Example: <pre>Device(config-if)# ipv6 nd raguard attach-policy</pre>	Applies the IPv6 RA Guard feature to a specified interface.
Step 4	exit Example: <pre>Device(config-if)# exit</pre>	Exits interface configuration mode.
Step 5	show ipv6 nd raguard policy [policy-name] Example: <pre>switch# show ipv6 nd raguard policy host Policy host configuration: device-role host</pre>	Displays the RA guard policy on all interfaces configured with the RA guard.

	Command or Action	Purpose
	Policy applied on the following interfaces: <pre>Et0/0 vlan all Et1/0 vlan all</pre>	
Step 6	debug ipv6 snooping raguad [<i>filter</i> <i>interface</i> <i>vlanid</i>] Example: Device# debug ipv6 snooping raguad	Enables debugging for IPv6 RA guard snooping information.

Configuring DHCP—DHCPv6 Guard

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ipv6 dhcp guard policy <i>policy-name</i> Example: Device(config)# ipv6 dhcp guard policy poll	Defines the DHCPv6 guard policy name and enters DHCP guard configuration mode.
Step 3	device-role { <i>client</i> <i>server</i> } Example: Device(config-dhcp-guard)# device-role server	Specifies the device role of the device attached to the target (interface or VLAN).
Step 4	preference min <i>limit</i> Example: Device(config-dhcp-guard)# preference min 0	(Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. If not specified, this check will be bypassed.
Step 5	preference max <i>limit</i> Example: Device(config-dhcp-guard)# preference max 255	(Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. If not specified, this check will be bypassed.

	Command or Action	Purpose
Step 6	trusted-port Example: <pre>Device(config-dhcp-guard)# trusted-port</pre>	(Optional) Specifies that this policy is being applied to trusted ports. All DHCP guard policing will be disabled.
Step 7	exit Example: <pre>Device(config-dhcp-guard)# exit</pre>	Exits DHCP guard configuration mode and returns to global configuration mode.
Step 8	interface type number Example: <pre>Device(config)# interface GigabitEthernet 0/2/0</pre>	Specifies an interface and enters interface configuration mode.
Step 9	switchport Example: <pre>Device(config-if)# switchport</pre>	Puts an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 10	ipv6 dhcp guard [attach-policy policy-name] Example: <pre>Device(config-if)# ipv6 dhcp guard attach-policy poll</pre>	Attaches a DHCPv6 guard policy to an interface.
Step 11	exit Example: <pre>Device(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
Step 12	vlan configuration vlan-id Example: <pre>Device(config)# vlan configuration 1</pre>	Specifies a VLAN and enters VLAN configuration mode.
Step 13	ipv6 dhcp guard [attach-policy policy-name] Example: <pre>Device(config-vlan-config)# ipv6 dhcp guard attach-policy poll</pre>	Attaches a DHCPv6 guard policy to a VLAN.
Step 14	exit Example: <pre>Device(config-vlan-config)# exit</pre>	Exits VLAN configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 15	exit Example: <pre>Device(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 16	show ipv6 dhcp guard policy [policy-name] Example: <pre>Device# show ipv6 dhcp policy guard poll</pre>	(Optional) Displays the policy configuration as well as all the interfaces where the policy is applied.

Configuring IPv6 Snooping

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	ipv6 snooping policy policy-name Example: <pre>Device(config)# ipv6 snooping policy policy1</pre>	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.
Step 3	device-role { node switch } Example: <pre>Device(config-snoop-policy)# device-node switch</pre>	Specifies the role of the device attached to the target (interface or VLAN): <ul style="list-style-type: none"> • node—Is the default. Bindings are created and entries are probed. • switch—Entries are not probed and when a trusted port is enabled, bindings are not created.
Step 4	[no] limit address-count Example: <pre>Device(config-snoop-policy)# limit address-count 500</pre>	Limits the number of binding entries, a no limit address-count means no limit.
Step 5	[no] protocol dhcp ndp Example: <pre>Device(config-snoop-policy)# protocol dhcp</pre> <pre>Device(config-snoop-policy)# protocol ndp</pre>	Turns on or switches off either DHCP or NDP gleaning.

	Command or Action	Purpose
Step 6	trusted-port Example: <pre>Device(config-snoop-policy)# trusted-port</pre>	Specifies that the policy be applied to a trusted port. If an entry is a trusted-port, none of its traffic will be blocked or dropped.
Step 7	security-level <i>glean guard inspect</i> Example: <pre>Device(config-snoop-policy)# security-level guard</pre>	Specifies the type of security level applied to the policy, such as: <ul style="list-style-type: none"> • glean—learns bindings but does not drop packets. • inspect—learns bindings and drops packets in case it detects an issue, such as an address theft. • guard—works like inspect, but in addition drops IPv6, ND, RA, and IPv6 DHCP server packets in case of a threat.
Step 8	tracking Example: <pre>Device(config-snoop-policy)# tracking enable</pre>	Enables tracking.
Step 9	exit Example: <pre>Device(config-snoop-policy)# exit</pre>	Exits snooping configuration mode and returns to global configuration mode.
Step 10	interface <i>type-number</i> Example: <pre>Device(config-if)# interface ethernet 1/25</pre>	Specifies an interface and enters interface configuration mode.
Step 11	[no] switchport Example: <pre>Device(config-if)# switchport</pre>	Switches between Layer 2 and Layer 3 mode.
Step 12	ipv6 snooping attach-policy <i>policy-name</i> Example: <pre>Device(config-if)# ipv6 snooping attach-policy policy1</pre>	Attaches the IPv6 snooping policy to an interface.
Step 13	exit Example: <pre>Device(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
Step 14	vlan configuration <i>vlan-id</i> Example:	Specifies a VLAN and enters VLAN configuration mode.

	Command or Action	Purpose
	Device(config)# vlan configuration 333	
Step 15	ipv6 snooping attach-policy <i>policy-name</i> Example: Device(config-vlan-config)# ipv6 snooping attach-policy policy1	Attaches the IPv6 snooping policy to a VLAN.
Step 16	exit Example: Device(config-vlan-config)# exit	Exits VLAN configuration mode and returns to global configuration mode.
Step 17	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 18	show ipv6 snooping policy <i>policy-name</i> Example: Device(config)# show ipv6 snooping policy policy1	Displays the policy configuration and the interfaces where the policy is applied.

Configuring IPv6 First-Hop Security Binding Table

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	ipv6 neighbor binding vlan <i>vlan-id</i> {interface <i>type number</i> ipv6-address mac-address} [tracking [disable enable retry-interval <i>value</i>] reachable-lifetime <i>value</i>] Example: Device(config)# ipv6 neighbor binding vlan 100 interface Ethernet 0/0 reachable-lifetime 100	Adds a static entry to the binding table database.
Step 3	ipv6 neighbor binding max-entries <i>entries</i> [vlan-limit <i>number</i> interface-limit <i>number</i> mac-limit <i>number</i>] Example:	Specifies the maximum number of entries that are allowed to be inserted in the binding table cache.

	Command or Action	Purpose
	Device(config)# ipv6 neighbor binding max-entries 100	
Step 4	ipv6 neighbor binding logging Example: Device(config)# ipv6 neighbor binding logging	Enables the logging of binding table main events.
Step 5	ipv6 neighbor tracking retry-interval <i>value</i> Example: Device(config)# ipv6 neighbor binding retry-interval 8	Tracks entries in the binding table.
Step 6	exit Example: Device(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 7	show ipv6 neighbor binding [vlan <i>vlan-id</i> interface <i>type number</i> ipv6 <i>ipv6-address</i> mac <i>mac-address</i>] Example: Device# show ipv6 neighbor binding	Displays the contents of a binding table.

Verifying and Troubleshooting IPv6 Snooping

Procedure

	Command or Action	Purpose
Step 1	show ipv6 snooping capture-policy [interface <i>type number</i>] Example: Device# show ipv6 snooping capture-policy interface ethernet 0/0	Displays snooping message capture policies.
Step 2	show ipv6 snooping counter [interface <i>type number</i>] Example: Device# show ipv6 snooping counter interface FastEthernet 4/12	Displays information about the packets counted by the interface counter.

	Command or Action	Purpose
Step 3	show ipv6 snooping features Example: Device# show ipv6 snooping features	Displays information about snooping features configured on the device.
Step 4	show ipv6 snooping policies [interface type number] Example: Device# show ipv6 snooping policies	Displays information about the configured policies and the interfaces to which they are attached.
Step 5	debug ipv6 snooping Example: Device# debug ipv6 snooping	Enables debugging for snooping information in IPv6.

Configuration Examples

Example: IPv6 RA Guard Configuration

```

switch(config)# interface fastethernet 3/13

switch(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 DHCP—DHCPv6 Guard

The following example displays a sample configuration for DHCPv6 Guard:

```

configure terminal
ipv6 dhcp guard policy poll
device-role server
preference min 0
preference max 255
trusted-port

```

Example: Configuring IPv6 First-Hop Security Binding Table

```

interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy poll
 vlan configuration 1
   ipv6 dhcp guard attach-policy poll
 show ipv6 dhcp guard policy poll

```

Example: Configuring IPv6 First-Hop Security Binding Table

```

config terminal
 ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0
 ipv6 neighbor binding max-entries 100
 ipv6 neighbor binding logging
 ipv6 neighbor binding retry-interval 8
 exit
 show ipv6 neighbor binding

```

Example: Configuring IPv6 Snooping

```

switch (config)# ipv6 snooping policy policy1
switch(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
switch(config-ipv6-snooping)# exit
.
.
.
switch# show ipv6 snooping policies policy1
Policy policy1 configuration:
  trusted-port
  device-role node
Policy applied on the following interfaces:
  Et0/0      vlan all
  Et1/0      vlan all
Policy applied on the following vlans:
  vlan 1-100,200,300-400

```

Additional References for IPv6 First-Hop Security

This section includes additional information related to configuring IPv6 First-Hop Security.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i>