IPv6 FHS

Feature history for IPv6 First Hop Security

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	IPv6 First Hop Security: IPv6 First Hop Security is a set of IPv6 security features that protects networks by mitigating such security breaches.	Cisco C9350 Series Smart Switches

Understand IPv6 First Hop Security

IPv6 networks face security threats and breaches in the form of router impersonation (man-in-the-middle attacks), address theft, address spoofing, misconfigurations errors, and so on. The First Hop Security in IPv6 (IPv6 FHS) is a set of IPv6 security features that protects networks by mitigating such security breaches. It does this by establishing security at the first switch connecting the end-hosts. The first hop for a host is very often a Layer 2 switch.

IPv6 FHS consists of the IPv6 Router Advertisement Guard and IPv6 DHCP Guard security features. Each of these security features addresses a different aspect of first hop security. To use a security feature, configure the corresponding policy.

Policies specify a particular behavior and must be attached to a target, which can be a physical interface, an EtherChannel interface, or a VLAN. An IPv6 software policy database service stores and accesses these

policies. When a policy is configured or modified, the attributes of the policy are stored or updated in the software policy database, and applied as specified.

In addition to the security features, the IPv6 FHS Binding Table contains IPv6 neighbors connected to the device. A binding entry includes: IP and MAC address of the host, interface, VLAN, state of the entry, etc. This database or binding table is used by other features (such as IPv6 ND Inspection) to validate the link-layer address (LLA), the IPv4 or IPv6 address, and the prefix binding of neighbors, to prevent spoofing and redirect attacks. The binding table updates via the IPv6 Snooping feature and manually added static binding entries.

Note The IPv6 FHS Binding Table is supported through the Switch Integrated Security Feature (SISF) feature. For more information, refer the *Switch Integrated Security Features* chapter.

IPv6 Router Advertisement Guard

This feature enables the network administrator to block or reject unwanted or rogue Router Advertisement (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 processes the RAs and filters out invalid 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 the configuration data on the Layer 2 device with the incoming RA frame information. 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.

The SISF-based device-tracking mechanism operates by forwarding router solicitation packets on interfaces configured with RA guard policies and designated as router-facing. If no such interface exists, the router solicitation messages are dropped, which might delay the router discovery for onboarding hosts as they will be unable to discover the router until it sends a periodic unsolicited router advertisement.

IPv6 DHCP Guard

The IPv6 DHCP 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 debug DHCP guard packets, use the **debug ipv6 snooping dhcp-guard** privileged EXEC command.

Prerequisites for IPv6 First Hop Security

Configure the necessary IPv6 enabled SDM template.

Restrictions for IPv6 First Hop Security

Legacy deprecated configurations from older platforms or releases will not work on newer platforms or releases. We recommend you convert legacy commands to the SISF-based device tracking CLI commands. For more information, refer *Switch Integrated Security Features* chapter.

These restrictions apply when applying FHS policies to EtherChannel interfaces (Port Channels):

- A physical port with an FHS policy attached cannot join an EtherChannel group.
- An FHS policy cannot be attached to a physical port when it is a member of an EtherChannel group.

Configure IPv6 First Hop Security

This section provides information about the various tasks to configure IPv6 first hop security.

Configure the IPv6 binding table content

Follow these steps to configure IPv6 binding table content:

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	[**no**] **ipv6 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** *interface_type stack/module/port hw_address* [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**tracking**{ [**default** | **disable**] [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds* | **default** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**]}] **Example:** `Device(config)# ipv6 neighbor binding`	Adds a static entry to the binding table database.
Step 4	[**no**] **ipv6 neighbor binding max-entries** *number* [**mac-limit** *number* | **port-limit** *number* [**mac-limit** *number*] | **vlan-limit** *number* [[**mac-limit** *number*] | [**port-limit** *number* [**mac-limit***number*]]] **Example:** `Device(config)# ipv6 neighbor binding max-entries 30000`	Specifies the maximum number of entries that are allowed to be inserted in the binding table cache.

	Command or Action	Purpose
Step 5	**ipv6 neighbor binding logging** **Example:** `Device(config)# ipv6 neighbor binding logging`	Enables the logging of binding table main events.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**show ipv6 neighbor binding** **Example:** `Device# show ipv6 neighbor binding`	Displays contents of a binding table.

Configure an IPv6 Router Advertisement Guard policy

Follow these steps to configure an IPv6 Router Advertisement policy:

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 example_policy`	Specifies the RA guard policy name and enters RA guard policy configuration mode.
Step 4	[**no**]**device-role** {**host** | **monitor** | **router** | **switch**} **Example:** `Device(config-nd-raguard)# device-role switch`	Specifies the role of the device attached to the port. The default is **host**. **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.

	Command or Action	Purpose
Step 5	**hop-limit** {**maximum** | **minimum**} *value* **Example:** `Device(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. The range for Maximum and Minimum Hop Limit values is 1 to 255. 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**} **Example:** `Device(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	**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} **Example:** `Device(config-nd-raguard)# match ipv6 access-list example_list`	Matches a specified prefix list or access list.
Step 8	**other-config-flag** {**on** | **off**} **Example:** `Device(config-nd-raguard)# other-config-flag on`	Enables filtering of Router Advertisement messages by the Other Configuration, or "O" flag field. A rouge RA message with an O 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 O value of 1, blocks those with 0.

	Command or Action	Purpose
		• **Off**: Accepts and forwards RA messages with an O value of 0, blocks those with 1.
Step 9	[**no**]**router-preference maximum** {**high** | **medium** | **low**} **Example:** `Device(config-nd-raguard)# router-preference maximum high`	Enables filtering of Router Advertisement messages by the router preference flag. If not configured, this filter is disabled. • **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 10	**trusted-port** **Example:** `Device(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	**default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list**} | **other-config-flag** | **router-preference maximum** | **trusted-port**} **Example:** `Device(config-nd-raguard)# default hop-limit`	Restores a command to its default value.
Step 12	**end** **Example:** `Device(config-nd-raguard)# end`	Exits RA Guard policy configuration mode and returns to privileged EXEC mode.
Step 13	**show ipv6 nd raguard policy** *policy_name* **Example:** `Device# show ipv6 nd raguard policy example_policy`	(Optional) Displays the ND guard policy configuration.

Attach an IPv6 Router Advertisement Guard policy to an interface

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:** `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 gigabitethernet 1/1/4`	Specifies an interface type and identifier; enters the interface configuration mode.

Step 4	**ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	Example:
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy`
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	`Device(config-if)# ipv6 nd raguard vlan 222, 223,224`
		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:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Attach an IPv6 Router Advertisement Guard policy to a Layer 2 EtherChannel

Follow these steps to attach an IPv6 Router Advertisement Guard Policy on an EtherChannel interface or VLAN:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface range** *type number* **Example:** `Device(config)# interface Port-channel 11`	Specifies the port-channel interface name assigned when the EtherChannel was created. Enters interface range configuration mode. **Tip** Enter the **show interfaces summary** command in privileged EXEC mode for quick reference to interface names and types.

Step 4	**ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	Example:
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	`Device(config-if-range)# ipv6 nd raguard vlan 222, 223,224`
		Attaches the RA Guard 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:** `Device(config-if-range)# end`	Exits interface range configuration mode and returns to privileged EXEC mode.

Attach an IPv6 Router Advertisement Guard policy to VLANs globally

Follow these steps to attach an IPv6 Router Advertisement policy to VLANs regardless of interface:

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.

	Command or Action	Purpose
Step 3	**vlan configuration** *vlan_list* **Example:** `Device(config)# vlan configuration 335`	Specifies the VLANs to which the IPv6 RA Guard policy will be attached, and enters VLAN interface configuration mode.
Step 4	**ipv6 dhcp guard** [**attach-policy** *policy_name*] **Example:** `Device(config-vlan-config)# ipv6 nd raguard attach-policy example_policy`	Attaches the IPv6 RA Guard policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the **attach-policy** option is not used.
Step 5	**end** **Example:** `Device(config-vlan-config)# end`	Exits VLAN interface configuration mode and returns to privileged EXEC mode.

Configure an IPv6 DHCP Guard policy

Follow these steps to configure an IPv6 DHCP (DHCPv6) Guard policy:

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 dhcp guard policy** *policy-name* **Example:** `Device(config)# ipv6 dhcp guard policy example_policy`	Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.
Step 4	**device-role** {**client** | **server**} **Example:** `Device(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.

	Command or Action	Purpose

Step 5	**match server access-list** *ipv6-access-list-name*
	Example:
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`Device(config)# ipv6 access-list my_acls`
	`Device(config-ipv6-acl)# permit host 2001:BD8:::1 any`
	
	`;;configure DCHPv6 Guard to match approved access list.`
	`Device(config-dhcp-guard)# match server access-list my_acls`
		(Optional). Enables verification that the advertised DHCPv6 server or relay address is from an authorized server access list (The destination address in the access list is 'any'). If not configured, this check will be bypassed. An empty access list is treated as a permit all.

Step 6	**match reply prefix-list** *ipv6-prefix-list-name*
	Example:
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`Device(config)# ipv6 prefix-list my_prefix permit 2001:DB8::/64 le 128`
	
	`;; Configure DCHPv6 Guard to match prefix`
	`Device(config-dhcp-guard)# match reply prefix-list my_prefix`
		(Optional) Enables verification of the advertised prefixes in DHCPv6 reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.

Step 7	**preference** {**max** *limit* | **min** *limit*}
	Example:
	`Device(config-dhcp-guard)# preference max 250`
	`Device(config-dhcp-guard)#preference min 150`
		Configure **max** and **min** when **device-role** is **server** to filter DCHPv6 server advertisements by the server preference value. The defaults permit all advertisements.
		• **max** *limit*: (0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. Default is 255. If not specified, this check will be bypassed.
		• **min** *limit*: (0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. Default is 0. If not specified, this check will be bypassed.

Step 8	**trusted-port** **Example:** `Device(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 9	**default** {**device-role** | **trusted-port**} **Example:**	(Optional) **default**: Sets a command to its defaults.

	Command or Action	Purpose
	`Device(config-dhcp-guard)# default device-role`	
Step 10	**end** **Example:** `Device(config-dhcp-guard)# end`	Exits DHCPv6 Guard Policy configuration mode and returns to privileged EXEC mode.
Step 11	**show ipv6 dhcp guard policy** *policy_name* **Example:** `Device# show ipv6 dhcp guard policy example_policy`	(Optional) Displays the configuration of the IPv6 DHCP guard policy. Omitting the *policy_name* variable displays all DHCPv6 policies.

Attach an IPv6 DHCP Guard policy to an interface

Follow these steps to to attach an IPv6 DHCP guard policy to an interface or a VLAN:

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 gigabitethernet 1/1/4`	Specifies an interface type and identifier, and enters interface configuration mode.

Step 4	**ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	Example:
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy`
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	`Device(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the **attach-policy** option is not used.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Attach an IPv6 DHCP Guard policy to a Layer 2 EtherChannel

Follow these steps to attach an IPv6 DHCP Guard policy on an EtherChannel interface or VLAN:

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 range** *Interface_name* **Example:** `Device(config)# interface Port-channel 11`	Specify the port-channel interface name assigned when the EtherChannel was created. Enters interface range configuration mode. **Tip** Enter the **show interfaces summary** command in privileged EXEC mode for quick reference to interface names and types.

Step 4	**ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	Example:
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	`Device(config-if-range)# ipv6 dhcp guard vlan 222, 223,224`
		Attaches the DHCP Guard 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:** `Device(config-if-range)# end`	Exits interface range configuration mode and returns to privileged EXEC mode.

Attach an IPv6 DHCP Guard policy to VLANs globally

Follow these steps to attach an IPv6 DHCP Guard policy to VLANs across multiple interfaces:

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	**vlan configuration** *vlan_list* **Example:** `Device(config)# vlan configuration 334`	Specifies the VLANs to which the IPv6 Snooping policy will be attached, and enters VLAN interface configuration mode.
Step 4	**ipv6 dhcp guard** [**attach-policy** *policy_name*] **Example:** `Device(config-vlan-config)# ipv6 dhcp guard attach-policy example_policy`	Attaches the IPv6 Neighbor Discovery policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the **attach-policy** option is not used.
Step 5	**end** **Example:** `Device(config-vlan-config)# end`	Exits VLAN interface configuration mode and returns to privileged EXEC mode.