IPv6 First Hop Security

This chapter contains the following sections:

address-config

To specify allowed configuration methods of global IPv6 addresses within an IPv6 Neighbor Binding policy, use the address-config command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

address-config [stateless | any] [dhcp]

no address-config

Parameters

- **stateless**—Only auto configuration for global IPv6 bound from NDP messages is allowed.
- **any**—All configuration methods for global IPv6 bound from NDP messages (stateless and manual) are allowed. If no keyword is defined the **any** keyword is applied.
- **dhcp**—Bound from DHCPv6 is allowed.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

If no keyword is defined the **address-config any** command is applied.

Example

The following example shows how to change the global configuration to allow only DHCP address configuration method:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-config dhcp
switchxxxxxx(config-nbr-binding)# exit
```

address-prefix-validation

To define the bound address prefix validation within an IPv6 Neighbor Binding policy, use the **address-prefix-validation** command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

address-prefix-validation [enable | disable]

no address-prefix-validation

Parameters

- **enable**—Enables bound address prefix validation. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables bound address prefix validation.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configured value.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

When a policy containing this command is attached to a VLAN, it overrides the global configuration and is applied to all ports of the VLAN. When this command is used in a policy attached to a port, it overrides the global and the VLAN configurations.

Example

The following example shows how to define policy1 that changes the global bound address verification in Neighbor Binding:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-prefix-validation enable
switchxxxxxx(config-nbr-binding)# exit
```

clear ipv6 first hop security counters

To clear IPv6 First Hop Security port counters, use the **clear ipv6 first hop security counters** command in privileged EXEC mode.

Syntax

clear ipv6 first hop security counters [interface *interface-id*]

Parameters

- **interface** *interface-id*—Clear IPv6 First Hop Security counters for the specified Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command clears port counters about packets handled by IPv6 First Hop Security.

Use the **interface** keyword to clear all counters for the specific port.

Use the command without keyword to clear all counters.

Example

The following example clears IPv6 First Hop Security counters on port gi1/0/1

```
switchxxxxxx# clear ipv6 first hop security counters interface gi1/0/1
```

clear ipv6 first hop security error counters

To clear IPv6 First Hop Security global error counters, use the **clear ipv6 first hop security error counters** command in privileged EXEC mode.

Syntax

clear ipv6 first hop security error counters

Command Mode

Privileged EXEC mode

User Guidelines

This command clears global error counters.

Example

The following example clears IPv6 First Hop Security error counters:

```
switchxxxxxx# clear ipv6 first hop security error counters
```

clear ipv6 neighbor binding prefix table

To remove dynamic entries from the Neighbor Prefix table, use the **clear ipv6 neighbor binding prefix table** command in Privilege EXEC configuration mode.

Syntax

clear ipv6 neighbor binding prefix table [**vlan** *vlan-id*] [*prefix-address*/*prefix-length*]

Parameters

- ***vlan-id***—Clear the dynamic prefixes that match the specified VLAN.
- ***prefix-address*/ *prefix-length***—Clear the specific dynamic prefix.

Command Mode

Privileged EXEC mode

User Guidelines

This command deletes the dynamic entries of the Neighbor Prefix table.

Use the **clear ipv6 neighbor binding prefix table vlan** *vlan-id prefix-address*/*prefix-length* command to delete one specific entry.

Use the **clear ipv6 neighbor binding prefix table vlan** *vlan-id* command to delete the dynamic entries that match the specified VLAN.

Use the **clear ipv6 neighbor binding prefix table** command to delete all dynamic entries.

Example 1. The following example clears all dynamic entries:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table
```

Example 2. The following example clears all dynamic prefixes that match VLAN 100:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100
```

Example 3. The following example clears one specific prefix:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100 2002:11aa:0000:0001::/64
```

clear ipv6 neighbor binding table

To remove dynamic entries from the Neighbor Binding table, use the **clear ipv6 neighbor binding table** command in Privilege EXEC configuration mode.

Syntax

clear ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*] [**ndp** | **dhcp**]

Parameters

- **vlan** *vlan-id*—Clear the dynamic entries that match the specified VLAN.
- **interface** *interface-id*—Clear the dynamic entries that match the specified port (Ethernet port or port channel).
- **ipv6** *ipv6-address*—Clear the dynamic entries that match the specified IPv6 address.
- **mac** *mac-address*—Clear the dynamic entries that match the specified MAC address.
- **ndp**—Clear the dynamic entries that are bound from NDP messages.
- **dhcp**—Clear the dynamic entries that are bound from DHCPv6 messages.

Command Mode

Privileged EXEC mode

User Guidelines

This command deletes the dynamic entries of the Neighbor Binding table. The dynamic entries to be deleted can be specified by the *vlan-id* argument, the *interface-id* argument, IPv6 address, MAC address, or by type of message from which they were bound.

If the **ndp** keyword and the **dhcp** keyword is not defined, the entries are removed regardless their origin. If no keywords or arguments are entered, all dynamic entries are deleted. All keyword and argument combinations are allowed.

Example

The following example clears all dynamic entries that exist on VLAN 100 & port gi1/0/1:

```
switchxxxxxx# clear ipv6 neighbor binding table vlan 100 interface gi1/0/1
```

device-role (IPv6 DHCP Guard)

To specify the role of the device attached to the port within an IPv6 DHCP Guard policy, use the **device-role** command in IPv6 DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

device-role {client | server}

no device-role

Parameters

- **client**—Sets the role of the device to DHCPv6 client.
- **server**—Sets the role of the device to DHCPv6 server.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: client.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

IPv6 DHCP Guard discards the following DHCPv6 messages sent by DHCPv6 servers/relays and received on ports configured as client:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

Example

The following example defines an IPv6 DHCP Guard policy named policy 1 and configures the port role as the server:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

device-role (Neighbor Binding)

To specify the role of the device attached to the port within an IPv6 Neighbor Binding policy, use the **device-role** command within IPv6 Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

device-role {perimeter | internal}

no device-role

Parameters

- **perimeter**—Specifies that the port is connected to devices not supporting IPv6 First Hop Security.
- **internal**—Specifies that the port is connected to devices supporting IPv6 First Hop Security.

Default Configuration

Policy attached to port or port channel: Value configured in the policy attached to the VLAN.

Policy attached to VLAN: Perimeter.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

NB Integrity supports the perimetrical model (see RFC 6620).

This model specifies two types of ports:

- **Perimeter Port**—Specifies ports connected to devices not supporting NB Integrity. NB Integrity establishes binding for neighbors connected to these ports. Source Guard does not function on these ports.
- **Internal Port**—The second type specifies ports connected to devices supporting IPv6 First Hop Security. NB Integrity does not establish binding for neighbors connected to these ports, but it does propagate the bindings established on perimeter ports.

A dynamic IPv6 address bound to a port is deleted when its role is changed from perimetrical to internal. A static IPv6 address is kept.

Example

The following example defines a Neighbor Binding policy named policy 1 and configures the port role as an internal port:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
```

device-role (RA Guard Policy)

To specify the role of the device attached to the port within an IPv6 RA Guard policy, use the **device-role** command in RA Guard Policy Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

device-role {host | router}

no device-role

Parameters

- **host**—Sets the role of the device to host.
- **router**—Sets the role of the device to router.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: host.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

RA Guard discards input RA, CPA, and ICMPv6 Redirect messages received on ports configured as host.

Example

The following example defines an RA Guard policy named policy 1 and configures the port role as **router**:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

device-role (ND Inspection Policy)

To specify the role of the device attached to the port within an IPv6 ND Inspection policy, use the **device-role** command in ND Inspection Policy Configuration mode. To disable this function, use the **no** form of this command.

Syntax

device-role {host | router}

no device-role

Parameters

- **host**—Sets the role of the device to host.
- **router**—Sets the role of the device to router.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: host.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

ND Inspection performs egress filtering of NDP messages depending on a port role.The following table specifies the filtering rules.

Message	Host	Router
RA	Permit	Permit
RS	Deny	Permit
CPA	Permit	Permit
CPS	Deny	Permit
ICMP Redirect	Permit	Permit

Example

The following example defines an ND Inspection policy named policy 1 and configures the port role as router:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

drop-unsecure

To enable dropping messages with no or invalid options or an invalid signature within an IPv6 ND Inspection policy, use the drop-unsecure command in ND Inspection Policy Configuration mode. To return to the default, use the no form of this command.

Syntax

drop-unsecure [enable | disable]

no drop-unsecure

Parameters

- **enable**—Enables dropping messages with no or invalid options or an invalid signature. If no keyword is configured this keyword is applied by default.
- **disable**—Disables dropping messages with no or invalid options or an invalid signature.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example defines an ND Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and enables the switch to drop messages with no or invalid options or an invalid signature:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure

switchxxxxxx(config-nd-inspection)# exit
```

hop-limit

To enable the verification of the advertised Cur Hop Limit value in RA messages within an IPv6 RA Guard policy, use the **hop-limit** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

hop-limit {[maximum {*value* | disable}] [minimum {*value* | disable}]}

no hop-limit [maximum] [minimum]

Parameters

- **maximum** *value*—Verifies that the hop-count limit is less than or equal to the **value** argument. Range 1-255. The value of the high boundary must be equal or greater than the value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of the hop-count limit.
- **minimum** *value*—Verifies that the hop-count limit is greater than or equal to the **value** argument. Range 1-255.
- **minimum disable**—Disables verification of the lower boundary of the hop-count limit.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Use the **disable** keyword to disable verification regardless of the global or VLAN configuration.

Example 1—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Cur Hop Limit value of 5:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit minimum 5
switchxxxxxx(config-ra-guard)# exit
```

Example 2—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables validation of the Cur Hop Limit high boundary:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit maximum disable
```

```
switchxxxxxx(config-ra-guard)# exit
```

ipv6 dhcp guard

To enable the DHCPv6 guard feature on a VLAN, use the **ipv6 dhcp guard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard

no ipv6 dhcp guard

Default Configuration

DHCPv6 Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

DHCPv6 Guard blocks messages sent by DHCPv6 servers/relays to clients received on ports that are not configured as a DHCPv6 server. Client messages or messages sent by relay agents from clients to servers are not blocked.

DHCPv6 Guard validates received DHCPv6 messages based on a DHCPv6 Guard policy attached to the source port.

Example 1—The following example enables DHCPv6 Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables DHCPv6 Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 dhcp guard
switchxxxxxx(config-if-range)# exit
```

ipv6 dhcp guard attach-policy (port mode)

To attach a DHCPv6 Guard policy to a specific port, use the **ipv6 dhcp guard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 dhcp guard attach-policy [*policy-name*]

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).
- **vlan** *v*lan-list—Specifies that the DHCPv6 Guard policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which DHCPv6 Guard is enabled.

Default Configuration

The DHCPv6 Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach a DHCPv6 Guard policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use **no ipv6 dhcp guard attach-policy** to detach all user-defined DHCP Guard policies attached to the port.

Use **no ipv6 dhcp guard attach-policy** *policy-name* to detach the specific policy from the port.

Example 1—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and the default policy port_default is detached:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the DHCPv6 Guard policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example DHCPv6 Guard detaches policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard attach-policy (VLAN mode)

To attach a DHCPv6 Guard policy to a specified VLAN, use the **ipv6 dhcp guard attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard attach-policy *policy-name*

no ipv6 dhcp guard attach-policy

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).

Default Configuration

The DHCPv6 Guard default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a DHCPv6 Guard policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to detach the current policy and to re-attach the default policy. The the **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the DHCPv6 Guard policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard policy

To define a DHCP Guard policy and place the switch in DHCPv6 Guard Policy Configuration mode, use the **ipv6 dhcp guard policy** command in Global Configuration mode. To remove the DHCPv6 guard policy, use the **no** form of this command.

Syntax

ipv6 dhcp guard policy *policy-name*

no ipv6 dhcp guard policy *policy-name*

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).

Default Configuration

No DHCPv6 Guard policy are configured

Command Mode

Global Configuration mode

User Guidelines

This command defines the DHCPv6 Guard policy name, and places the router in DHCPv6 Guard Policy Configuration mode.

Each policy of the same type (for example, DHCPv6 Guard policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports two predefined, default DHCPv6 Guard policies named: "vlan_default" and "port_default":

```
ipv6 dhcp guard policy vlan_default
      exit
      ipv6 dhcp guard policy port_default
      exit
```

The default policies are empty and cannot be removed, but can be changed. The **no ipv6 dhcp guard policy** does not remove the default policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 dhcp guard policy** command multiple times.

Before an attached policy is removed, a request for confirmation is presented to the user, as shown in Example 3 below.

Example 1—The following example defines a DHCPv6 Guard policy named policy1, places the router in DHCPv6 Guard Policy Configuration mode, configures the port to drop unsecure messages and sets the device role as router:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

Example 2—The following example defines a DHCPv6 Guard named policy1 by multiple steps:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

Example 3—The following example removes an attached DHCPv6 Guard policy:

```
switchxxxxxx(config)# no ipv6 dhcp guard policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 dhcp guard preference

To globally enable verification of the preference in messages sent by DHCPv6 servers, use the **ipv6 dhcp guard preference** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 dhcp guard preference [maximum] [minimum]

Parameters

- **maximum** *value*—Advertised preference value is lower than or equal to the **value** argument. Range 0-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Advertised preference value is greater than or equal to the **value** argument. Range 0-255.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification that the preference value in messages sent by DHCPv6 servers messages (see RFC3315) is greater than or less than the *value* argument.

Note. When DHCPv6 Guard receives a RELAY-REPL message, it takes it from the encapsulated message.

Configuring the **minimum** *value* keyword and argument specifies the minimum allowed value. The received DHCPv6 reply message with a preference value less than a value specified by the **value** argument is dropped.

Configuring the **maximum** *value* keyword and argument specifies the maximum allowed value. The received DHCPv6 reply message with a preference value greater than the value specified by the **value** argument is dropped.

Use **no ipv6 dhcp guard preference** to disable verification of the advertised preference value in DHCPv6 reply messages.

Use **no ipv6 dhcp guard preference maximum** to disable verification of the maximum boundary of the value of the advertised preference value in DHCPv6 messages.

Use the **no ipv6 dhcp guard preference minimum** command to disable verification of the minimum boundary of the value of the advertised preference value in DHCPv6 messages.

Example 1—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using two commands:

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10
switchxxxxxx(config)# ipv6 dhcp guard preference maximum 102
```

Example 2—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using a single command:

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10 maximum 102
```

ipv6 first hop security

To globally enable IPv6 First Hop Security on a VLAN, use the **ipv6 first hop security** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security

no ipv6 first hop security

Default Configuration

IPv6 First Hop Security on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the **ipv6 first hop security** command to enable IPv6 First Hop Security on a VLAN.

Example 1—The following example enables IPv6 First Hop Security on VLAN 100:

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 first hop security**

switchxxxxxx(config-if)# **exit**

Example 2—The following example enables IPv6 First Hop Security on VLANs 100-107:

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 first hop security**

switchxxxxxx(config-if-range)# **exit**

ipv6 first hop security attach-policy (port mode)

To attach an IPv6 First Hop Security policy to a specific port, use the **ipv6 first hop security attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 first hop security attach-policy [*policy-name*]

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the IPv6 First Hop Security policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which IPv6 First Hop Security is enabled.

Default Configuration

The IPv6 First Hop Security default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an IPv6 First Hop Security policy to a port.

Each succeeding usage of this command overrides the previous usage of the command with the same policy.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 first hop security attach-policy** command to detach all user-defined policies attached to the port. The default policy is reattached.

Use the **no ipv6 first hop security attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the IPv6 First Hop Security policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example the IPv6 First Hop Security policy policy1 is detached from gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security attach-policy (VLAN mode)

To attach an IPv6 First Hop Security policy to a specified VLAN, use the **ipv6 first hop security attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security attach-policy *policy-name*

no ipv6 first hop security attach-policy

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration

The IPv6 First Hop Security default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach an IPv6 First Hop Security policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to return to detach the current policy and to reattach the default policy. The **no** form of the command does not have an effect if the default policy was attached.

Example

In the following example, the IPv6 First Hop Security policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security logging packet drop

To globally enable the logging of dropped packets by the IPv6 First Hop Security feature, use the **ipv6 first hop security logging packet drop** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security logging packet drop

no ipv6 first hop security logging packet drop

Default Configuration

Logging is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to log packets that are dropped. If logging is enabled, the switch sends a rate-limited SYSLOG message every time it drops a message.

Example

The following example shows how to enable logging of dropped packets by the IPv6 first-hop security feature:

```
switchxxxxxx(config)# ipv6 first hop security logging packet drop
```

ipv6 first hop security policy

To define an IPv6 First Hop Security policy and place the switch in IPv6 First Hop Security Policy Configuration mode, use the **ipv6 first hop security policy** command in Global Configuration mode. To remove the IPv6 First Hop Security policy, use the **no** form of this command.

Syntax

ipv6 first hop security policy *policy-name*

no ipv6 first hop security policy *policy-name*

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration

No IPv6 First Hop Security policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines an IPv6 First Hop Security policy, and places the switch in IPv6 First Hop Security Policy Configuration mode. Each policy of the same type (for example, IPv6 First Hop Security policies) must have a unique name. Policies of different types can have the same policy name. The switch supports two predefined, empty, default IPv6 First Hop Security policies named: "vlan_default" and "port_default":

```
ipv6 first hop security policy vlan_default
      exit
      ipv6 first hop security policy port_default
      exit
```

These policies cannot be removed but they can be changed. The **no ipv6 first hop security policy** does not remove these policies, it only removes the policy configurations defined by the user.

You can define a policy using the **ipv6 first hop security policy** command multiple times.

If an attached policy is removed, it is detached automatically before removing.

Examples

Example 1—The following example defines the IPv6 First Hop Security policy named policy1, places the switch in IPv6 First Hop Security Policy Configuration mode, and enables logging of dropped packets:

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config)# exit
```

Example 2—The following example removes an attached IPv6 First Hop Security policy:

```
switchxxxxxx(config)# no ipv6 first hop security policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy1 will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection

To enable the IPv6 Neighbor Discovery (ND) Inspection feature on a VLAN, use the **ipv6 nd inspection** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection

no ipv6 nd inspection

Default Configuration

ND Inspection on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the command to enable ND Inspection on a VLAN. The IPv6 ND Inspection validates the Neighbor Discovery Protocol (NDP) messages using the ND Inspection policies and global ND Inspection configuration. The ND Inspection bridges NDP messages to all ports excluding the source port within the VLAN with the following exception: RS and CPS messages are not bridged to ports configured as host (see the **device-role** command). The ND inspection is performed after RA Guard.

Example 1—The following example enables ND Inspection on VLAN 100:

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 nd inspection**

switchxxxxxx(config-if)# **exit**

Example 2—The following example enables ND Inspection on VLANs 100-107:

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 nd inspection**

switchxxxxxx(config-if-range)# **exit**

ipv6 nd inspection attach-policy (port mode)

To attach an ND Inspection policy to a specific port, use the **ipv6 nd inspection attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd inspection attach-policy [*policy-name*]

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the ND Inspection policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which ND Inspection is enabled.

Default Configuration

The ND Inspection default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **ipv6 nd inspection attach-policy** command to attach an ND Inspection policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 nd inspection attach-policy** command to detach all user-defined policies attached to the port.

Use the **no ipv6 nd inspection attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the ND Inspection policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example, ND Inspection detaches policy policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection attach-policy (VLAN mode)

To attach an ND Inspection policy to a specified VLAN, use the **ipv6 nd inspection attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection attach-policy *policy-name*

no ipv6 nd inspection attach-policy

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).

Default Configuration

The ND Inspection default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a ND Inspection policy to a VLAN. If the policy specified by the **policy-name** argument is not defined, the command is rejected. Use the **no** form of the command to detach the current policy and to reattach the default policy. The **no** form of the command does not have an effect if the default policy was attached.

Example

In the following example, the ND Inspection policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection drop-unsecure

To globally enable dropping messages with no CGA and RSA Signature options, use the **ipv6 nd inspection drop-unsecure** command in Global Configuration mode. To disable this function, use the **no** form of this command.

Syntax

ipv6 nd inspection drop-unsecure

no ipv6 nd inspection drop-unsecure

Default Configuration

All messages are bridged.

Command Mode

Global Configuration mode

User Guidelines

This command drops NDP messages if they do not contain CGA and RSA Signature options.

If this command is not configured, then the **sec-level minimum** command does not have an effect.

If this command is configured, then only the **sec-level minimum** command has an effect and all other configured ND Inspection policy commands are ignored.

Example

The following example enables the switch to drop messages with no or invalid options or an invalid signature:

```
switchxxxxxx(config)# ipv6 nd inspection drop-unsecure
```

ipv6 nd inspection policy

To define an ND Inspection policy and place the switch in IPv6 ND Inspection Policy Configuration mode, use the **ipv6 nd inspection policy** command in Global Configuration mode. To remove the ND Inspection policy, use the **no** form of this command.

Syntax

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).

Default Configuration

No ND Inspection policies are configured.

Command Mode

Global Configuration mode

User Guidelines

This command defines the ND Inspection policy name, and places the router in ND Inspection Policy Configuration mode. Each policy of the same type (for example, ND Inspection policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined ND Inspection policies named: "vlan_default" and "port_default":

```
ipv6 nd inspection policy vlan_default
      exit
      ipv6 nd inspection policy port_default
      exit
```

These policies cannot be removed, but they can be changed. The **no ipv6 nd inspection policy** does not remove these policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 nd inspection policy** command multiple times.

If an attached policy is removed it is detached automatically before removing.

Example 1. The following example defines a ND Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and configures the port to drop unsecured messages and sets the device role as router:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

Example 2. The following example defines an ND Inspection policy as policy1 by a few steps:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
```

```
switchxxxxxx(config-nd-inspection)# exit
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

Example 3. The following example removes an attached ND Inspection policy:

```
switchxxxxxx(config)# no ipv6 nd inspection policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection sec-level minimum

To globally specify the minimum security level value, use the **ipv6 nd inspection sec-level minimum** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection sec-level minimum *value*

no ipv6 nd inspection sec-level minimum

Parameters

- ***value***—Sets the minimum security level. Range: 0–7.

Default Configuration

All messages are bridged.

Command Mode

Global Configuration mode

User Guidelines

This command specifies the minimum security level parameter value when the drop-unsecured feature is configured.

This command has no effect if dropping of non secure messages is disabled.

Example

The following example enables the switch to specify 2 as the minimum CGA security level:

```
switchxxxxxx(config)# ipv6 nd inspection sec-level minimum 2
```

ipv6 nd inspection validate source-mac

To globally enable checking source MAC address against the link-layer address in the source/target link-layer option, use the **ipv6 nd inspection validate source-mac** command in Global Configuration mode. To disable this function, use the **no** form of this command.

Syntax

ipv6 nd inspection validate source-mac

no ipv6 nd inspection validate source-mac

Parameters

N/A

Default Configuration

This command is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

When the switch receives an NDP message, which contains a link-layer address in the source/target link layer option, the source MAC address is checked against the link-layer address. Use this command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Example

The following example enables the switch to drop an NDP message whose link-layer address in the source/target link-layer option does not match the MAC address:

```
switchxxxxxx(config)# ipv6 nd inspection validate source-mac
```

ipv6 nd raguard

To globally enable the Router Advertisements (RA) guard feature on a VLAN, use the **ipv6 nd raguard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard

no ipv6 nd raguard

Parameters

N/A

Default Configuration

RA Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the **ipv6 nd raguard** command, to enable IPv6 RA Guard on a VLAN. The RA Guard discards RA, CPA, and ICMP Redirect messages received on ports that are not configured as router (see the **device-role** command). The RA Guard validates received RA messages based on an RA Guard policy attached to the source port.

RA Guard is performed before ND inspection.

Example 1—The following example enables RA Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables RA Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 nd raguard
switchxxxxxx(config-if-range)# exit
```

ipv6 nd raguard attach-policy (port mode)

To attach an RA Guard policy to a specific port, use the **ipv6 nd raguard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd raguard attach-policy [*policy-name*]

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the RA Guard policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which RA Guard policy is enabled.

Default Configuration

The RA Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an RA Guard policy to a port. Each time the command is used, it overrides the previous command within the same policy. If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 nd raguard attach-policy** command to detach all user-defined policies attached to the port.

Use the no **ipv6 nd raguard attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the RA Guard policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example RA Guard detaches policy policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard attach-policy (VLAN mode)

To attach an RA Guard policy to a specified VLAN, use the **ipv6 nd raguard attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard attach-policy *policy-name*

no ipv6 nd raguard attach-policy

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).

Default Configuration

The RA Guard default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach an RA Guard policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to detach the current policy and to reattach the default policy. The **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the RA Guard policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard hop-limit

To globally enable verification of the advertised Cur Hop Limit value in RA messages, use the **ipv6 nd raguard hop-limit** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard hop-limit {[maximum *value*] [minimum *value*]}

no ipv6 nd raguard hop-limit [maximum] [minimum]

Parameters

- **maximum** *value*—Verifies that the hop-count limit is lower than or equal to the **value** argument. Range 1-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Verifies that the hop-count limit is greater than or equal to the **value** argument. Range 1-255.

Default Configuration

No hop-count limit is verified.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification that the advertised Cur Hop Limit value in an RA message (see RFC4861) is greater than or less than the value set by the **value** argument.

Configuring the **minimum** *value* keyword and argument can prevent an attacker from setting a low Cur Hop Limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *value* keyword and argument enables verification that the advertised Cur Hop Limit value is less than or equal to the value set by the **value** argument. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Use the **no ipv6 nd raguard hop-limit maximum** command to disable verification of the maximum boundary of the advertised Cur Hop Limit value in an RA message.

Use the **no ipv6 nd raguard hop-limit minimum** command to disable verification of the minimum boundary of the advertised Cur Hop Limit value in an RA message.

Example 1—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using two commands:

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3
switchxxxxxx(config)# ipv6 nd raguard hop-limit maximum 100
```

Example 2—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using a single command:

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3 maximum 100
```

ipv6 nd raguard managed-config-flag

To globally enable verification of the advertised the Managed Address Configuration flag in RA messages, use the **ipv6 nd raguard managed-config-flag** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard managed-config-flag {on | off}

no ipv6 nd raguard managed-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised the Managed Address Configuration flag (or the M flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that might not be trustworthy.

Example

The following example enables M flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard managed-config-flag off
```

ipv6 nd raguard other-config-flag

To globally enable verification of the advertised “Other Configuration” flag in RA messages, use the **ipv6 nd raguard other-config-flag** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard other-config-flag {on | off}

no ipv6 nd raguard other-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised “Other Configuration” flag (or "O" flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to retrieve other configuration information through a DHCPv6 server that might not be trustworthy.

Example

The following example shows how the command enables O flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard other-config-flag off
```

ipv6 nd raguard policy

To define an RA Guard policy name and place the switch in IPv6 RA Guard Policy Configuration mode, use the **ipv6 nd raguard policy** command in Global Configuration mode. To remove the RA Guard policy, use the **no** form of this command.

Syntax

ipv6 nd raguard policy *policy-name*

no ipv6 nd raguard policy *policy-name*

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).

Default Configuration

No RA Guard policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines the RA Guard policy name, and places the switch in IPv6 RA Guard Policy Configuration mode.

Each policy of the same type (for example, RA Guard policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined RA Guard policies, named: "vlan_default" and "port_default":

```
ipv6 nd raguard policy vlan_default
exit
ipv6 nd raguard policy port_default
exit
```

The policies cannot be removed, but they can be changed. The **no ipv6 nd raguard policy** does not remove these policies, it only removes the policy configuration defined by the user.

The **vlan_default** policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The **port_default** policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the **ipv6 nd raguard policy** command multiple times. If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines an RA Guard policy named policy1, places the router in RA Guard Policy Configuration mode, and disenabled validation of the Other Configuration flag, and sets the device role as router:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
```

```
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

Example 2—The following example defines an RA Guard named policy1 using multiple steps:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

Example 3—The following example removes an attached RA Guard policy:

```
switchxxxxxx(config)# no ipv6 nd raguard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd raguard router-preference

To globally enable verification of the advertised Default Router Preference value in RA messages, use the **ipv6 nd raguard router-preference** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard router-preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 nd raguard router-preference [maximum] [minimum]

Parameters

- **maximum** *value*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191). The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191).

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised Default Router Preference value in RA messages (see RFC4191).

Configuring the **minimum** *value* keyword and argument specifies the minimum allowed value. Received RA messages with a Default Router Preference value less than the *value* argument are dropped.

Configuring the **maximum** *value* keyword and argument specifies the maximum allowed value. Received RA messages with a Default Router Preference value greater than the *value* argument are dropped.

Use the **no ipv6 nd raguard router-preference** command to disable verification of the advertised Default Router Preference value in RA messages.

Use the **no ipv6 nd raguard router-preference maximum** command to disable verification of the maximum boundary of the advertised Default Router Preference value in RA messages.

Use the **no ipv6 nd raguard router-preference minimum** command to disable verification of the advertised Default Router Preference value in RA messages.

Example 1—The following example defines that only a value of **medium** is acceptable using two commands:

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium
switchxxxxxx(config)# ipv6 nd raguard router-preference maximum medium
```

Example 2—The following example defines that only a value of **medium** is acceptable using a single command:

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium maximum medium
```

ipv6 neighbor binding

To globally enable the Neighbor Binding (NB) integrity feature on a VLAN, use the **ipv6 neighbor binding** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding

no ipv6 neighbor binding

Parameters

N/A

Default Configuration

NB integrity on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

NB integrity establishes binding for neighbors connected to the perimetrical ports belonging to the VLANs on which the feature is enabled.

Example 1—The following example enables NB integrity on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables NB integrity on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 neighbor binding
switchxxxxxx(config-if-range)# exit
```

ipv6 neighbor binding address-config

To specify allowed configuration methods of global IPv6 addresses, use the **ipv6 neighbor binding address-config** command in Global Configuration mode. To return to the default setting, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-config [stateless | any] [dhcp]

no ipv6 neighbor binding address-config

Parameters

- **stateless**—Only auto configuration is allowed for global IPv6 bound from NDP messages.
- **any**—All configuration methods for global IPv6 bound from NDP messages (stateless and manual) are allowed. If no keyword is defined the **any** keyword is applied.
- **dhcp**—Binding from DHCPv6 is allowed.

Default Configuration

Any is the default parameter.

Command Mode

Global Configuration mode

User Guidelines

This command defines allowed IPv6 address configuration methods for global IPv6 addresses.

The **stateless** and **any** keywords specify the following:

- Global IPv6 addresses are bound from NDP messages. If none of these keywords are configured, only link-local addresses are bound from NDP messages.
- How global IPv6 addresses, bound from NDP messages, are checked against the Neighbor Prefix table, if prefix validation is enabled:

  stateless—IPv6 addresses are bound from NDP messages, and only global addresses belonging to learned prefixes with set A-flag or prefixes manually configured with the **autoconfig** keyword are allowed.

  any—IPv6 addresses are bound from NDP messages and only global addresses belonging to prefixes in NPT are allowed.

Use the **dhcp** keyword, to allow binding from DHCPv6 message. IPv6 addresses bound from DHCPv6 messages are never verified against the Neighbor Prefix table. IPv6 addresses bound from DHCPv6 messages override IPv6 addresses bound from NDP messages.

Note. If the **dhcp** keyword is not configured, the switch will bind IPv6 addresses assigned by DHCPv6 from NDP messages, because a host must execute the DAD process for these addresses.

If no keyword is defined the **ipv6 neighbor binding address-config any** command is applied.

Example 1. The following example specifies that any global IPv6 address configuration method can be applied and there will be no binding from DHCPv6 messages:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any
```

Example 2. The following example specifies that any global IPv6 address binding from NDP and global IPv6 address binding from DHCPv6 messages can be applied:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any dhcp
```

Example 3. The following example specifies that only stateless global IPv6 address binding from NDP can be applied

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless
```

Example 4. The following example specifies that only the stateless IPv6 address configuration and assignment by DHCPv6 methods can be applied and binding only from NDP messages is supported:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless dhcp
```

Example 5. The following example specifies that global IPv6 addresses can be assigned only by DHCPv6:

```
switchxxxxxx(config)# ipv6 neighbor binding address-config dhcp
```

ipv6 neighbor binding address-prefix

To define a static prefix for global IPv6 addresses bound from NDP messages, use the **ipv6 neighbor binding address-prefix** command in Global Configuration mode. To delete the prefix, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-prefix vlan *vlan-id ipv6-prefix*/*prefix-length* [**autoconfig**]

no ipv6 neighbor binding address-prefix [vlan *vlan-id*] [*ipv6-prefix*/*prefix-length*]

Parameters

- ***ipv6-prefix***/*prefix-length*—IPv6 prefix.
- **vlan** *vlan-id*—ID of the specified VLAN.
- **autoconfig**—The prefix can be used for stateless configuration.

Default Configuration

No static prefix

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 neighbor binding address-prefix** command to add a static prefix to the Neighbor Prefix table.

Use the **no ipv6 neighbor binding address-prefix vlan** *vlan-id ipv6-prefix*/*prefix-length* command to remove one static entry from the Neighbor Prefix table.

Use the **no ipv6 neighbor binding address-prefix vlan** *vlan-id* command to remove all static entries from the Neighbor Prefix table defined on the given VLAN.

Use the **no ipv6 neighbor binding address-prefix** command to remove all static entries from the Neighbor Prefix table.

Example 1. The following example adds two static entries. The second one can be used for stateless configuration.

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:100::/64
autoconfig
```

Example 2. The following example deletes a single static entry:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
```

Example 3. The following example deletes all static entries defined on the specified VLAN:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100
```

Example 4. The following example deletes all static entries:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix
```

ipv6 neighbor binding address-prefix-validation

To globally enable validation of a bound IPv6 address against the Neighbor Prefix table, use the **ipv6 neighbor binding address-prefix-validation** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-prefix-validation

no ipv6 neighbor binding address-prefix-validation

Parameters

N/A

Default Configuration

The feature is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables bound address prefix validation. If the Neighbor Binding feature is enabled, the switch checks if a bound address belongs to one of the prefixes of the Neighbor Prefix table or to a manually-configured prefix list by the ipv6 neighbor binding address-prefix command in the Neighbor Binding configuration mode. If an address does not belong, it is not bound.

Example

The following example shows how to enable bound address validation against the Neighbor Prefix table:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
```

ipv6 neighbor binding attach-policy (port mode)

To attach a Neighbor Binding policy to a specific port, use the **ipv6 neighbor binding attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 neighbor binding attach-policy [*policy-name*]

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the Neighbor Binding policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which Neighbor Binding policy is enabled.

Default Configuration

The Neighbor Binding default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach a Neighbor Binding policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 neighbor binding attach-policy** command to detach all user-defined policies attached to the port.

Use the **no ipv6 neighbor binding attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10, and the Neighbor Binding policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example, Neighbor Binding Integrity detaches policy policy1 detached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding attach-policy (VLAN mode)

To attach a Neighbor Binding policy to a specific VLAN, use the **ipv6 neighbor binding attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding attach-policy *policy-name*

no ipv6 neighbor binding attach-policy

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).

Default Configuration

The Neighbor Binding default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a Neighbor Binding policy to a VLAN.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Use the **no** form of the command to return to detach the current policy and reattach the default policy. The **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the Neighbor Binding policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding lifetime

To globally change the default of the Neighbor Binding table entry lifetime, use the **ipv6 neighbor binding lifetime** command in Global Configuration mode. To return to the default setting, use the **no** form of this command.

Syntax

ipv6 neighbor binding lifetime *value*

no ipv6 neighbor binding lifetime

Parameters

- ***value***—The lifetime in minutes. The range is from 1 through 60 minutes.

Default Configuration

5 minutes

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 neighbor binding lifetime** command to change the default lifetime.

Example

The following example changes the lifetime for binding entries to 10 minutes:

```
switchxxxxxx(config)# ipv6 neighbor binding lifetime 10
```

ipv6 neighbor binding max-entries

To globally specify the maximum number of dynamic entries that are allowed to be inserted in the Binding table cache, use the **ipv6 neighbor binding max-entries** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding max-entries {[**vlan-limit** *number*] [**interface-limit** *number*] [**mac-limit** *number*]}

no ipv6 neighbor binding max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

Parameters

- **vlan-limit** *number*—Specifies a neighbor binding limit per number of VLANs.
- **interface-limit** *number*—Specifies a neighbor binding limit per port.
- **mac-limit** *number*—Specifies a neighbor binding limit per MAC address.

Default Configuration

This command is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command is used to control the contents of the Binding table. This command specifies the maximum number of dynamic entries that can be inserted in the Binding table cache. After this limit is reached, new entries are refused, and a Neighbor Discovery Protocol (NDP) traffic source with a new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

Example

The following example shows how to specify globally the maximum number of entries that can be inserted into the cache per MAC:

```
switchxxxxxx(config)# ipv6 neighbor binding max-entries mac-limit 2
```

ipv6 neighbor binding policy

To define a Neighbor Binding policy and place the switch in IPv6 Neighbor Binding Policy Configuration mode, use the **ipv6 neighbor binding policy** command in Global Configuration mode. To remove the Neighbor Binding policy, use the **no** form of this command.

Syntax

ipv6 neighbor binding policy *policy-name*

no ipv6 neighbor binding policy *policy-name*

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).

Default Configuration

No Neighbor Binding policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines a Neighbor Binding policy name, and places the router in Neighbor Binding Policy Configuration mode so that additional commands can be added to the policy.

The switch supports two predefined Neighbor Binding policies, named: "vlan_default" and "port_default":

```
ipv6 neighbor binding policy vlan_default
      exit
      ipv6 neighbor binding policy port_default
      exit
```

The policies cannot be removed, but they can be changed. The **no ipv6 neighbor binding policy** does not remove these policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 neighbor binding policy** command multiple times.

If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines a Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, enables logging, and defines the port as internal:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# logging binding
switchxxxxxx(config-nbr-binding)# exit
```

Example 2—The following example defines a Neighbor Binding policy named policy1 using multiple steps:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
logging binding
witchxxxxxx(config-nbr-binding)# exit
```

Example 3—The following example remove an attached Neighbor Binding policy:

```
switchxxxxxx(config)# no ipv6 neighbor binding policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 neighbor binding static

To add a static entry to the Neighbor Binding table, use the **ipv6 neighbor binding static** command in Global Configuration mode. To remove the static entry, use the **no** form of this command.

Syntax

ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id* **interface** *interface-id* **mac** *mac-address*

no ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id*

Parameters

- **ipv6** *ipv6-address*—IPv6 address of the static entry.
- **vlan** *vlan-id*—ID of the specified VLAN.
- **interface** *interface-id*—Adds static entries to the specified port.
- **mac** *mac-address*—MAC address of the static entry.

Default Configuration

No static entry.

Command Mode

Global Configuration mode

User Guidelines

This command is used to add static entries to the Neighbor Binding table. Static entries can be configured regardless the port role.

If the entry (dynamic or static) already exists, the new static entry overrides the existing one.

If the Neighbor Binding table overflows, the static entry is not added.

Example

The following example adds a static entry:

```
switchxxxxxx(config)# ipv6 neighbor binding static ipv6 2001:600::1 vlan 100 interface
gi1/0/1 mac 00BB.CC01.F500
```

ipv6 source guard

To enable the IPv6 Source Guard feature on a VLAN, use the **ipv6 source guard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 source guard

no ipv6 source guard

Default Configuration

Source Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

IPv6 Source Guard blocks an IPv6 data message arriving on a port if its source IPv6 address is bound to another port, or it is unknown.

Example 1—The following example enables IPv6 Source Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 source guard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables IPv6 Source Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 source guard
switchxxxxxx(config-if-range)# exit
```

ipv6 source guard attach-policy (port mode)

To attach an IPv6 Source Guard policy to a specific port, use the **ipv6 source guard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 source guard attach-policy *policy-name*

no ipv6 source guard attach-policy

Parameters

- ***policy-name***—The IPv6 Source Guard policy name (up to 32 characters).

Default Configuration

The IPv6 Source Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an IPv6 Source Guard policy to a port.

Each succeeding **ipv6 source guard attach-policy** command overrides the previous policy attachment on the same port.

IPv6 Source guard policies can be used to block forwarding IPv6 data messages with unknown source IPv6 addresses or with source IPv6 addresses bound to a port differing from the input one.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port.
- The global rules are added to the set if they have not been added.

Use the no ipv6 source guard attach-policy command to detach the user defined policy attached to the port and to reattach the default policy with name "port_default".

Example 1—In the following example, the IPv6 Source Guard policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 source guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example IPv6 Source Guard detaches policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 source guard attach-policy
switchxxxxxx(config-if)# exit
```

ipv6 source guard policy

To define an IPv6 Source Guard policy name and place the user in IPv6 Source Guard Configuration, use the **ipv6 source guard policy** command in Global Configuration mode. To remove the IPv6 Source Guard policy name, use the **no** form of this command.

Syntax

ipv6 source guard policy *policy-name*

no ipv6 source guard policy *policy-name*

Parameters

- ***policy-name***—The IPv6 Source Guard policy name (up to 32 characters).

Default Configuration

No IPv6 Source Guard policies are configured.

Command Mode

Global Configuration mode

User Guidelines

This command defines the IPv6 Source Guard policy name, and places the router in IPv6 Source Guard Policy Configuration mode.

Each policy of the same type (for example, IPv6 Source Guard policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports one predefined IPv6 Source Guard policy named: "port_default":

```
ipv6 source guard policy port_default
      exit
```

The policy cannot be removed, but it can be changed. The **no ipv6 source guard policy** does not remove the policy, it only removes any policy configurations defined by the user.

If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines the IPv6 Source Guard policy named policy1, places the router in IPv6 Source Guard Policy Configuration mode, and configures the port as trusted:

```
switchxxxxxx(config)# ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config)# exit
```

Example 2—The following example removes the attached IPv6 Source Guard policy:

```
switchxxxxxx(config)# no ipv6 source guard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

logging binding

To enable the logging of Binding table main events within an IPv6 Neighbor Binding policy, use the **logging binding** command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

logging binding [enable | disable]

no logging binding

Parameters

- **enable**—Enables logging of Binding table main events. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables logging of Binding table main events.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of Binding table main events within the IPv6 Neighbor Binding policy named policy1:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# logging binding enable
switchxxxxxx(config-nbr-binding)# exit
```

logging packet drop

To enable the logging of dropped packets within an IPv6 First Hop Security policy, use the **logging packet drop** command in IPv6 First Hop Security Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

logging packet drop [enable | disable]

no logging packet drop

Parameters

- **enable**—Enables logging of dropped packets. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables logging of dropped packets.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

IPv6 First Hop Security Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of dropped messaged with the IPv6 First Hop Security Policy named policy1:

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config-ipv6-fhs)# exit
```

managed-config-flag

To enable verification of the advertised Managed Address Configuration flag within an IPv6 RA Guard policy, use the **managed-config-flag** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

managed-config-flag {on | off | disable}

no managed-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.
- **disable**—The value of the flag is not validated.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and enables M flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# managed-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

match ra address

To enable verification of the router's IPv6 address in received RA messages within an IPv6 RA Guard policy, use the **match ra address** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match ra address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra address

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the router’s IPv6 address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: router's addresses are not verified.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

This command enables verification of the router's IPv6 address in received RA messages by a configured prefix list. If the router’s source IPv6 address does not match the prefix list or if the prefix list is not configured, the RA message is dropped.

Use the **disable** keyword to disable verification of the router’s IPv6 address regardless of the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, matches the router addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the router with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra address prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

match ra prefixes

To enable verification of the advertised prefixes in received RA messages within an IPv6 RA Guard policy, use the **match ra prefixes** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match ra prefixes {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra prefixes

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the advertised prefixes in received RA messages.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: advertised prefixes are not verified.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

This command enables verification of the advertised prefixes in received RA messages by a configured prefix list. If an advertised prefix does not match the prefix list, or if the prefix list is not configured, the RA message is dropped.

Use the **disable** keyword to disable verification of the advertised prefixes in received RA messages in both global or the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard configuration mode, matches the prefixes to the prefix list named list1, and the 2001:101::/64 prefixes and denies 2001:100::/64 prefixes:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra prefixes prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/64
```

match reply

To enable verification of the assigned IPv6 addressed in messages sent by DHCPv6 servers/relays to a configured prefix list within a DHCPv6 Guard policy, use the **match reply** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match reply {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match reply

Parameters

- ***ipv6-prefix-list-name***—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the advertised prefixes in replies.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: advertised prefixes are not verified.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

IPv6 DHCP Guard verifies the assigned IPv6 addresses to the configure prefix list passed in the IA_NA and IA_TA options of the following DHCPv6 messages sent by DHCPv6 servers/relays:

- ADVERTISE
- REPLY
- RELAY-REPL

Note 1. Assigned addresses are not verified if a value of the Status Code option (if it presents) differs from the following ones:

- Success
- UseMulticast

Note 2. In RELAY-REPL messages DHCPv6 Guard validates the message encapsulated in the DHCP-relay-message option.

Use the **disable** keyword to disable verification of the assigned IPv6 addresses in replies.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard policy configuration mode, matches the assigned addresses to the prefix list named list1: all assigned IPv6

addresses must belong to 2001:0DB8:100:200/64 or to 2001:0DB8:100::/48. The "**ge 128**" parameter must be configured for each prefix of the prefix-list with prefix length less than 128.

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match reply prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:100:200/64 ge 128
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/48 ge 128
```

match server address

To enable verification of the source IPv6 address in messages sent by DHCPv6 servers or DHCPv6 Relays to a configured prefix list within a DHCPv6 Guard policy, use the **match server address** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match server address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match server address

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the DHCP server's and relay's IPv6 address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: server's addresses are not verified.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

This command enables verification of the source IPv6 address in messages sent by DHCPv6 servers and DHCPv6 Relays to a configured prefix list. If the source IPv6 address does not match the configured prefix list, or if the prefix list is not configured, the DHCPv6 reply is dropped.

IPv6 DHCP Guard verifies the source IPv6 address in the following DHCPv6 messages sent by DHCPv6 servers/relays:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

Use the **disable** keyword to disable verification of the DHCP server's and relay's IPv6 address.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, matches the server or relay addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the server with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

max-entries

To define the maximum number of dynamic entries that can be inserted in the Binding table cache within an IPv6 Neighbor Binding policy, use the **max-entries** command in Neighbor Binding Policy Configuration mode.To return to the default, use the **no** form of this command.

Syntax

max-entries {[**vlan-limit** {*number* | **disable**}] [**interface-limit** {*number* | **disable**}] [**mac-limit** {*number* | **disable**}]}

no max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

Parameters

- **vlan-limit** *number*—Specifies a neighbor binding limit per VLANs. The parameter is ignored in a policy attached to port.
- **vlan-limit disable**—Disables a neighbor binding limit per VLANs.
- **interface-limit** *number*—Specifies a neighbor binding limit per port.
- **interface-limit disable**—Disables a neighbor binding limit per port.
- **mac-limit** *number*—Specifies a neighbor binding limit per MAC address.
- **mac-limit disable**—Disables a neighbor binding limit per MAC address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example 1—The following example defines an Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# max-entries interface-limit 25
switchxxxxxx(config)# exit
```

Example 2—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables limit per MAC:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# max-entries mac-limit disable

switchxxxxxx(config-ra-guard)# exit
```

other-config-flag

To enable the verification of the advertised the Other Configuration flag in RA messages within an IPv6 RA Guard policy, use the **other-config-flag** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

other-config-flag {on | off | disable}

no other-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.
- **disable**—The value of the flag is not validated.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

Use the **disable** keyword to disable flag validation in both global or VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and enables O flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

preference

To enable verification of the preference in messages sent by DHCPv6 servers within a DHCPv6 Guard policy, use the **preference** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

preference {[**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]}

no preference [maximum] [minimum]

Parameters

- **maximum** *value*—Advertised preference value is lower or equal than that set by the value argument. Range 0-255. A value of the high boundary must be equal to or greater than a value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of the advertised preference value.
- **minimum** *value*—Advertised preference value is greater than or equal to the **value** argument. Range 0-255.
- **minimum disable**—Disables verification of the lower boundary of the advertised preference value.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

Use the **disable** keyword to disable verification in both global or VLAN configuration.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, and defines a minimum preference value of 10:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# preference minimum 10
switchxxxxxx(config-dhcp-guard)# exit
```

router-preference

To enable verification of advertised Default Router Preference value in RA messages within an IPv6 RA Guard policy, use the **router-preference** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

router-preference [**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]

no router-preference [maximum] [minimum]

Parameters

- **maximum** *value*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191). A value of the high boundary must be equal to or greater than a value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of Advertised Default Router Preference.
- **minimum** *value*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191).
- **minimum disable**—Disables verification of the low boundary of Advertised Default Router Preference.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Default Router Preference value of medium:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# router-preference minimum medium
switchxxxxxx(config-ra-guard)# exit
```

sec-level minimum

To specify the minimum security level value within an Ipv6 ND Inspection policy, use the **sec-level minimum** command in ND Inspection policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

sec-level minimum *value* | disable

no sec-level minimum

Parameters

- ***value***—Sets the minimum security level, which is a value from 0 through 7.
- **disable**—Disables verification of security level parameter

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

This command has no effect if dropping of unsecured messages is disabled.

Example

The following example defines an NDP Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and specifies 2 as the minimum CGA security level:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# sec-level minimum 2
switchxxxxxx(config-nd-inspection)# exit
```

show ipv6 dhcp guard

To display DHCPv6 Guard global configuration, use the **show ipv6 dhcp guard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 dhcp guard

Command Mode

Privileged EXEC mode

User Guidelines

The **show ipv6 dhcp guard** command displays DHCPv6 Guard global configuration.

Example

The following example gives an example of the output of the **show ipv6 dhcp guard** command:

```
switchxxxxxx# show ipv6 dhcp guard
IPv6 DHCP Guard is enabled on VLANs:1-4,6,7,100-120
Default Preference
  minimum: 10
  maximum: 100
```

show ipv6 dhcp guard policy

To display DHCPv6 guard policies on all ports configured with the DHCPv6 guard feature, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

Syntax

show ipv6 dhcp guard policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the DHCPv6 guard policy with the given name.
- **active**—Displays the attached DHCPv6 guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the DHCPv6 guard feature.

Example 1—The following example displays the Policy Configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 dhcp guard policy policy1
DHCPv6 Guard Policy: policy1
  device-role: server
  preference
    minimum: 1
    maximum: 200
  server address prefix list: list1
  reply prefix list name: list10
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 dhcp guard policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 dhcp guard policy
policy1
policy2
```

show ipv6 first hop security

To display all IPv6 First Hop Security global configuration, use the **show ipv6 first hop security** command in Privilege EXEC configuration mode.

Syntax

show ipv6 first hop security

Command Mode

Privileged EXEC mode

User Guidelines

This command displays all IPv6 First Hop Security global configuration.

Example

The following example gives an example of the **show ipv6 first hop security** command:

```
switchxxxxxx# show ipv6 first hop security
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
Logging Packet Drop: enabled
```

show ipv6 first hop security active policies

To display information about the policies applied to the port and to the VLAN, use the **show ipv6 first hop security active policies** command in privileged EXEC mode.

Syntax

show ipv6 first hop security active policies interface *interface-id* vlan *vlan-id*

Parameters

- **interface** *interface-id*—Port Identifier (Ethernet port or port channel).
- **vlan** *vlan-id*—VLAN Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays policies applied to frames arriving on given port and belonging to the given VLAN. The policies are calculated automatically by using the policies attached to the port, VLAN, and the global configuration

Example

The following example displays the active attached policies on gi1/0/1 and VLAN 100:

```
switchxxxxxx# show ipv6 first hop security active policies interface gi1/0/1 vlan 100
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
IPv6 DHCP Guard is enabled on VLANs:1-4
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
IPv6 Neighbor Binding Integrity is enabled on VLANs:1-4,6,7,100-120
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
IPv6 Source Guard is enabled on VLANs:1-3,7,100-112
gi1/0/1, VLAN 100
IPv6 First Hop Security Policy:
  logging packet drop: enabled (from global configuration)
DHCPv6 Guard Policy:
  device-role: server (from policy1 attached to the port)
  reply prefix list name: list10 (from policy2 attached to the VLAN)
  server address prefix list name: list22 (from policy2 attached to the VLAN)
  preference
    minimum: 1 (from policy2 attached to the VLAN)
    maximum: 200 (from policy2 attached to the VLAN)
ND Inspection Policy:
  device-role: host (default)
  drop-unsecure: enabled (from policy2 attached to the VLAN)
  sec-level minimum: 3 (from policy1 attached to the port)
  validate source-mac: enabled (from global configuration)
Neighbor Binding Policy: policy1
  device-role: perimiter (default)
  logging binding: enabled (from policy1 attached to the port)
  address-prefix-validation: enabled (from policy2 attached to the VLAN)
  address-config: any (default)
  maximum entries
```

```
   VLAN: unlimited (from global configuration)
   Port: 1 (from policy1 attached to the port)
   MAC: 2 (from policy2 attached to the VLAN)
RA Guard Policy:
  device-role: router (from policy1 attached to the port)
  hop-limit:
    minimum: 10 (from policy2 attached to the VLAN)
    maximum: 20 (from global configuration)
  manage-config-flag: on(from policy2 attached to the VLAN)
  ra address verification::  disabled(default)
  ra prefixes prefix list name: list1(from policy2 attached to the VLAN)
  other-flag: disabled (default)
  router-preference:
    minimum: medium (from policy2 attached to the VLAN)
    maximum: medium (from policy2 attached to the VLAN)
IPv6 Source Guard Policy:
  trusted port: enabled (from policy1 attached to the port)
```

show ipv6 first hop security attached policies

To display information about the policies attached to the port and to the VLAN, use the **show ipv6 first hop security attached policies** command in privileged EXEC mode.

Syntax

show ipv6 first hop security attached policies interface *interface-id* vlan *vlan-id*

Parameters

- **interface** *interface-id*—Port Identifier (Ethernet port or port channel).
- **vlan** *vlan-id*—VLAN Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays policies of all IPv6 First Hop Security attached to a VLAN specified by the *vlan-id* argument and displays all policies attached to a port and to VLAN specified by the *interface-id* and *vlan-id* arguments.

Examples

The following example displays the attached policy on gi1/0/1 and VLAN 100:

```
switchxxxxxx# show ipv6 first hop security attached policies interface gi1/0/1 vlan 100
Attached to VLAN 100
  RA Guard Policy: policy1
  Neighbor Bind Policy: policy2
Attached to port gi1/0/1 and VLAN 100
  IPv6 First Hop Security Policy: FHSpolicy
  ND Inspection Policy: policy1
  RA Guard Policy: policy3
  Neighbor Bind Policy: policy3
  IPv6 Source Guard Policy: policy4
```

show ipv6 first hop security counters

To display information about the packets counted by the port counter, use the **show ipv6 first hop security counters** command in privileged EXEC mode.

Syntax

show ipv6 first hop security counters interface *interface-id*

Parameters

- **interface** *interface-id*—Displays counters for specified Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays packets handled by the switch that are being counted in port counters. The switch counts packets captured per port and records whether the packet was received, bridged, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples displays information about packets counted on port gi1/0/1:

```
switchxxxxxx# show ipv6 first hop security counters interface gi1/0/1
Received messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[63] RS[0] NA[13] NS[0] REDIR[0]
  DHCPv6     ADV[0] REP[20] REC[0] REL-REP[0] LEAS-REP[10] RLS[0] DEC[0]
Dropped messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[2] RS[0] NA[0] NS[0] REDIR[0]
  DHCPv6     ADV[1] REP[2] REC[0] REL-REP[1] LEAS-REP[0] RLS[0] DEC[0]
Dropped reasons on gi1/0/1:
  Feature         Number Reason
  DHCP Guard           2  Server message on client port
  DHCP Guard           1  Unauthorized assigned address
  DHCP Guard           1  Unauthorized server source address
  DHCP Guard           0  Unauthorized server preference
  RA guard             1  Router message on host port
  RA guard             1  Unauthorized source address
  RA guard             0  Unauthorized advertise prefix
  RA guard             0  Unauthorized router preference
  RA guard             0  Unauthorized other config flag
  RA guard             0  Unauthorized managed config flag
  RA guard             0  Unauthorized cur hop limit
  ND Inspection        0  Invalid source MAC
  ND Inspection        0  Unsecure message
  ND Inspection        0  Unauthorized sec level
  Source guard         0  NoBinding
  NB Integrity         0  Illegal ICMPv6 message
  NB Integrity         0  Illegal DHCPv6 message
```

show ipv6 first hop security error counters

To display global error counters, use the **show ipv6 first hop security error counters** command in privileged EXEC mode.

Syntax

show ipv6 first hop security error counters

Command Mode

Privileged EXEC mode

User Guidelines

This command displays global error counters.

Example 1—The following examples displays global error counters:

```
switchxxxxxx# show ipv6 first hop security error counters
Neighbor Binding Table Overflow counter: 0
Neighbor Prefix Table Overflow counter: 0
TCAM Overflow counter: 0
```

show ipv6 first hop security policy

To display IPv6 First Hop Security policies on all ports configured with the IPv6 First Hop Security feature, use the **show ipv6 first hop security policy** command in privileged EXEC mode.

Syntax

show ipv6 first hop security policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the IPv6 First Hop policy with the given name.
- **active**—Displays the attached Ipv6 First Hop Security policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the IPv6 First Hop feature.

Example 1—The following example displays the Policy Configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 first hop security policy policy1
IPv6D First Hop Security Policy: policy1
  logging packet drop: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 first hop security policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 first hop security policy
policy1
policy2
```

show ipv6 nd inspection

To display ND Inspection global configuration, use the **show ipv6 nd inspection** command in Privilege EXEC configuration mode.

Syntax

show ipv6 nd inspection

Command Mode

Privileged EXEC mode

User Guidelines

This command displays ND Inspection global configuration.

Example

The following example gives an example of the **show ipv6 nd snooping** command output:

```
switchxxxxxx# show ipv6 nd snooping
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
unsecure drop: enabled
sec-level minimum value: 2
source mac validation: disabled
```

show ipv6 nd inspection policy

To display an IPv6 ND Inspection policy on all ports configured with the ND Inspection feature, use the **show ipv6 nd inspection policy** command in privileged EXEC mode.

Syntax

show ipv6 nd inspection policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the ND Inspection policy with the given name.
- **active**—Displays the attached ND Inspection policies.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 nd inspection policy policy1
ND Inspection Policy: policy1
  device-role: router
  drop-unsecure: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 nd inspection policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 nd inspection policy
policy1
policy2
```

show ipv6 nd raguard

To display RA Guard global configuration, use the **show ipv6 nd raguard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 nd raguard

Command Mode

Privileged EXEC mode

Example

The following example gives an example of the **show ipv6 nd raguard** command output:

```
switchxxxxxx# show ipv6 nd raguard
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
"Managed address configuration" flag (M-flag:) off
"Other configuration" flag (O-flag): disabled
Hop Limit:
  minimum: 10
  maximum: 100
Default Router Preference:
  minimum: 1
  maximum: 1
```

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all ports configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

Syntax

show ipv6 nd raguard policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the RA guard policy with the given name.
- **active**—Displays the attached user defined RA guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the RA guard feature.

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 nd raguard policy raguard1
RA Guard Policy: policy1
  device-role: router
  router address prefix list name: list1
  prefixes prefix list name: list2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 nd raguard policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	port-default	gi1/0/1-4	1-4094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 nd raguard policy
policy1
policy2
```

show ipv6 neighbor binding

To display Neighbor Binding global configuration, use the **show ipv6 neighbor binding** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding

Command Mode

Privileged EXEC mode

User Guidelines

This displays Neighbor Binding global configuration.

Example

The following example gives an example of the **show ipv6 neighbor binding** command output:

```
switchxxxxxx# show ipv6 neighbor binding
Neighbor Binding Integrity is enabled on VLANs:1-4,6-7,100-120
Binding logging: disabled
Binding lifetime: 56 minutes
Address Configuration method: dhcp
Binding address prefix validation: disabled
Maximum entries
 VLAN: unlimited
 Port: 1
 MAC: 1
```

show ipv6 neighbor binding policy

To display Neighbor Binding policies, use the **show ipv6 neighbor binding policy** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding policy [*policy-name* | active]

Parameters

- ***policy-name***—Neighbor Binding policy name.
- **active**—Displays the attached Neighbor Binding policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command either displays all policies or a specific one.

Examples

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 neighbor binding policy policy1
Neighbor Binding Policy: policy1
  address configuration method: dhcp
  binding address prefix validation: disabled
  device-role: perimiter
  binding logging: disabled
  max-entries
   VLAN: unlimited
   Port: 10
   MAC: 2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 neighbor binding policy active
Attached to VLAN:
  Policy Name     VLANs
  policy2         200-300
  vlan-default    1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-4	1-100
	port-default	gi1/0/1-4	101-4094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 neighbor binding policy
policy1
policy2
```

show ipv6 neighbor binding prefix table

To display contents of the Neighbor Prefix table, use the **show ipv6 neighbor binding prefix table** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding prefix table [**vlan** *vlan-id*]

Parameters

- **vlan** *vlan-id*—Displays the prefixes that match the specified VLAN.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the Neighbor Prefix table. The display output can be limited to the specified VLAN. If no VLAN is configured, all prefixes are displayed.

Example

The following example displays the learned prefixes:

```
switchxxxxxx# show ipv6 neighbor binding prefix table
Flags: A - the prefix can be used for autoconfig (stateless configuration)
Neighbor Prefix Table has 4 entries
VLAN  Prefix         Type    Flags   Remaining Lifetime
   7  2004:1::/64   static    A
   7  2006:1::/64   dynamic              1230
   7  2008:1::/64   static
1027  2002:1::/64   dynamic   A            230
```

show ipv6 neighbor binding table

To display contents of the Binding table, use the **show ipv6 neighbor binding table** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*]

Parameters

- **vlan** *vlan-id*—Displays the Binding table entries that match the specified VLAN.
- **interface** *interface-id*—Displays the Binding table entries that match the specified port (Ethernet port or port channel).
- **ipv6** *ipv6-address*—Displays the Binding table entries that match the specified IPv6 address.
- **mac** *mac-address*—Displays the Binding table entries that match the specified MAC address.

Command Mode

Privileged EXEC mode

User Guidelines

This displays the contents of the Binding table. The display output can be specified by the specified VLAN, port, IPv6 address, or MAC address. If no keywords or arguments are entered, all Binding table contents are displayed.

Any keyword and argument combinations are allowed.

Example

The following example displays the contents of the Binding table:

```
switchxxxxxx# show ipv6 neighbor binding table
Binding Table has 4 entries
```

VLAN	IPv6 address	Inter	MAC address	Origin	State	Expir	TCAM
-----	----------	-------	------------	------	-----	Time	Ovrfl
100	2001:300::1	gi1/0/1	AABB.CC01.F500	NDP	VALID	------	-----
100	2001:600::1	gi1/0/1	AABB.CC01.F510	NDP NDP	TENT	559	*
100	2001:100::2	gi1/0/2	AABB.CC01.F160	NDP	VALID	96	
200	2001:200::3	gi1/0/2			VALID	79	

```
Field Descriptions:
```

- **VLAN**—VLAN the host belongs to.
- **IPv6 address**—IPv6 address of the host.

- **Inter**—port the host is connected on.
- **MAC address**—MAC address of the host.
- **Origin**—Protocol that has added the IPv6 address:
- **Static**—The static IPv6 address manually defined by the i**pv6 neighbor binding static** command.
- **NDP**—The IPv6 address learnt from the NDP protocol messages.
- **DHCP**—The IPv6 address learnt from the DHCPv6 protocol messages.
- **State**—Entry's state:
- **TENT**—The new host IPv6 address is under validation. Since its lifetime is less than 1sec its expiration time is not displayed.
- **VALID**—The host IPv6 address was bound.
- **Expir. Time**—Left time in seconds until the entry will be removed, if it is not confirmed.
- **TCAM Ovrflw**—Entries marked by '*' have not been added to TCAM because TCAM overflow.

show ipv6 source guard

To display IPv6 Source Guard global configuration, use the **show ipv6 source guard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 source guard

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This displays IPv6 Source Guard global configuration.

Example

The following example gives an example of the **show ipv6 source guard** command output:

```
switchxxxxxx# show ipv6 source guard
IPv6 Source Guard is enabled on VLANs:1-4,6,7,100-120
```

show ipv6 source guard policy

To display IPv6 Source Guard policies, use the **show ipv6 source guard policy** command in Privilege EXEC configuration mode.

Syntax

show ipv6 source guard policy [*policy-name* | active]

Parameters

- ***policy-name***—IPv6 Source Guard policy name.
- **active**—Displays the attached IPv6 Source Guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays all configured IPv6 Source Guard policies, the given one or all attached IPv6 Source Guard policies.

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 source guard policy policy1
Neighbor Binding Policy: policy1
  trusted port: disabled
  Attached to ports:
   Ports
   gi1/0/1-2
   gi1/0/4
   Po1-4
```

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 source guard policy active
Attached to VLAN:
Attached to ports:
```

	Policy Name	Ports
	policy1	gi1/0/1-2
	port-default	gi1/0/1-2
		gi1/0/3

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 source guard policy
policy1
policy2
```

trusted-port (IPv6 Source Guard)

To configure a port as trusted port within an IPv6 Source Guard policy, use the **trusted-port** command in IPv6 Source Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

trusted-port

no trusted-port

Default Configuration

not trusted.

Command Mode

IPv6 Source Guard Policy Configuration mode

User Guidelines

IPv6 data messages bridged from trusted ports are not validated by IPv6 Source Guard.

Example

The following example defines a policy that defines a port as trusted:

```
switchxxxxxx(config)# ipv6 ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config-ipv6-srcguard)# exit
```

validate source-mac

To enable checking the MAC addresses against the link-layer address within an IPv6 ND Inspection policy, use the **validate source-mac** command in ND Inspection Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

validate source-mac [enable | disable]

no validate source-mac

Parameters

- **enable**—Enables validation of the MAC address against the link-layer address. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables validation of MAC address against the link-layer address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables the router to drop an NDP message whose link-layer address does not match the MAC address:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# validate source-mac
switchxxxxxx(config-nd-inspection)# exit
```