Contents

1 Configuring IPv6 Source Guard

1.1 Introduction

1.1.1 Overview

The IPv6 Source Guard function enables the hardware to filter IPv6 packets to ensure that only users whose IPv6 packets match information in the database of the hardware can access the network normally, preventing users from privately setting IPv6 addresses or forging IPv6 packets.

1.1.2 Principles

1. Basic Concepts

- Source IPv6 address

  Indicate the source IPv6 address field in IPv6 packets.

- Source MAC address

  Indicate the source media access control (MAC) address field in L2 packets.

- User record binding database

  The user record binding database is the basis for IPv6 Source Guard. Data in the user record binding database comes from the following two sources:

  - Dynamic Host Configuration Protocol version 6 (DHCPv6) and neighbor discovery (ND) Snooping binding databases: After IPv6 Source Guard is enabled, information in the DHCPv6 and ND Snooping binding databases is synchronized to the user binding database of IPv6 Source Guard. In this case, IPv6 packets are filtered strictly through IPv6 Source Guard on devices with DHCPv6 or ND Snooping enabled. DHCPv6 Snooping and ND Snooping are two independent functions. Users can enable both functions or either function.
  - Static user configuration: including static user information bound by running the **ipv6 source binding** command and local link addresses (fe80::/10) and undefined addresses (::/128) released by running the **ipv6 verify source permit link-local** command.

2. Checking the Source Address Fields of Packets

IPv6 packets passing through an interface are checked based on the source IPv6 address or source IPv6 address and MAC address to prevent malicious users from forging packets to launch attacks.

When IPv6 Source Guard is enabled on an interface, the device checks the source addresses of packets passing through the interface, which can be a switching interface, L2 aggregation port (link aggregation), or L2 encapsulation subinterface. Only the packets whose source addresses match entries in the user record binding database can pass through the interface. There are two matching methods:

- Filtering based on the source IPv6 address

The source IPv6 addresses of all IPv6 packets passing through an interface are checked. Only the packets whose source IPv6 addresses match entries in the user record binding database can pass through the interface. It is the default filtering policy of IPv6 Source Guard.

- Filtering based on the source IPv6 address and MAC address

  The source IPv6 addresses and MAC addresses of IPv6 packets passing through an interface are checked. Packets are allowed to pass through the interface only when both the L2 source MAC addresses and L3 source IPv6 addresses of these packets match an entry in the user record binding database.

1.2 Restrictions and Guidelines

- Typically, IPv6 Source Guard needs to work with DHCPv6 Snooping or ND Snooping. Therefore, DHCPv6 Snooping or ND Snooping should also be enabled. DHCPv6 Snooping or ND Snooping can be enabled either before or after IP Source Guard is enabled.
- If DHCPv6 Snooping is enabled on a device, the device does not check DHCPv6 packets.
- If ND Snooping is enabled on a device, the device does not check ND packets.

1.3 Configuration Task Summary

Select any of the following configuration tasks to configure.

- Enabling IPv6 Source Guard on an Interface
- Enabling IPv6 Source Guard on a VLAN

1.4 Enabling IPv6 Source Guard on an Interface

1.4.1 Restrictions and Guidelines

IPv6 Source Guard depends on DHCPv6 Snooping or ND Snooping. Users need to enable IPv6 Source Guard on an untrusted interface of DHCPv6 Snooping or ND Snooping.

1.4.2 Prerequisites

At least DHCPv6 Snooping or DN Snooping is enabled. To enable DHCPv6 Snooping, run the **ipv6 dhcp snooping** command. To enable ND Snooping, run the **ipv6 nd snooping enable** command.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the IPv6 source address binding database.

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Enable the function of converting IPv6 source address binding entries to static MAC address entries.

ipv6 source binding sticky-mac

The function of converting IPv6 source address binding entries to static MAC address entries is disabled by default.

(6) (Optional) Enable local link address release on an interface.

ipv6 verify source permit link-local

The local link address release function is disabled on an interface by default.

This command can be configured only on L2 switching interfaces and L2 aggregation ports.

Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

(7) Enable IPv6 Source Guard on an interface.

ipv6 **verify source** [**port**-**security**]

IPv6 Source Guard is disabled on an interface by default.

1.5 Enabling IPv6 Source Guard on a VLAN

1.5.1 Configuration Tasks

Enabling IPv6 Source Guard on a VLAN includes the following tasks:

(1) Enabling IPv6 Source Guard on a VLAN

(2) Configuring a Trusted Interface

(3) (Optional) Configuring an Untrusted Interface

1.5.2 Enabling IPv6 Source Guard on a VLAN

1. Prerequisites

At least DHCPv6 Snooping or DN Snooping is enabled. To enable DHCPv6 Snooping, run the **ipv6 dhcp snooping** command. To enable ND Snooping, run the **ipv6 nd snooping enable** command.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the IPv6 source address binding database.

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

(5) Enable IPv6 Source Guard on a VLAN.

ipv6 verify source [**port-security**]

IPv6 Source Guard is disabled on a VLAN by default.

1.5.3 Configuring a Trusted Interface

1. Introduction

To enable IPv6 Source Guard on a VLAN, configure the uplink interface as an IPv6 Source Guard trusted interface. On the IPv6 Source Guard trusted interface, IPv6 Source Guard is not performed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the uplink interface as an IPv6 Source Guard trusted interface.

ipv6 verify source trust

No interface is configured as an IPv6 Source Guard trusted interface by default.

1.5.4 Configuring an Untrusted Interface

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) The following configurations are optional. Please configure at least one task.

- Enable the function of converting IPv6 source address binding entries to static MAC address entries.

  ipv6 **source binding sticky-mac**

  The function of converting IPv6 source address binding entries to static MAC address entries is disabled by default.

- Enable local link address release on an interface.

  ipv6 **verify source permit link-local**

  The local link address release function is disabled on an interface by default.

  This command can be configured only on L2 switching interfaces and L2 aggregation ports.

  Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]	Displays information of the IPv6 source address binding database.
show ipv6 source binding sticky-mac [**interface** *interface-type interface number*]	Displays information about IPv6 source address binding entries converted to static MAC address entries.