Contents

1 Configuring IP Source Guard

1.1 Introduction

1.1.1 Overview

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

1.1.2 Principles

1. Basic Concepts

- Source IP address

  Indicate the source IP address field in IP 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 IP Source Guard. Data in the user record binding database comes from the following two sources:

  Dynamic Host Configuration Protocol (DHCP) Snooping binding database: When IP Source Guard is enabled, data of the DHCP Snooping binding database is synchronized to the user record binding database of IP Source Guard. In this case, IP packets are filtered strictly through IP Source Guard on devices with DHCP Snooping enabled.

  Static user configuration: static user information configured by running the **ip source binding** command.

- Excluded VLAN

  When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard. A maximum of 32 excluded VLANs can be specified for one interface.

2. Checking the Source Address Fields of Packets

IP packets passing through an interface are checked based on the source IP address or source IP address and MAC address to prevent malicious users from forging packets to launch attacks. When there is no need to check or filter IP packets within a VLAN, users can specify this VLAN as an excluded VLAN to release such packets.

When IP 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 IP address

  The source IP addresses of all IP packets passing through an interface are checked. Packets are allowed to pass through the interface only when the source IP addresses of these packets belong to the IP address set of the user record binding database. It is the default filtering policy of IP Source Guard.

- Filtering based on the source IP address and MAC address

  The source IP addresses and MAC addresses of IP 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 IP addresses of these packets match an entry in the user record binding database.

1.2 Restrictions and Guidelines

- Typically, IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled either before or after IP Source Guard is enabled.
- IP Source Guard cannot be configured on the trusted interfaces of DHCP Snooping or IP Source Guard.
- IP Source Guard cannot be configured on the ports that do not verify the global IP address and MAC address binding.
- IP Source Guard can be configured based on interfaces or VLANs.

1.3 Configuration Task Summary

Select any of the following configuration tasks to configure.

- Enabling IP Source Guard on an Interface
- Enabling IP Source Guard on a VLAN
- Enabling the Sole Role of the IP Source Address Binding Database as the Source of DAI Binding Entries

1.4 Enabling IP Source Guard on an Interface

1.4.1 Restrictions and Guidelines

IP Source Guard can be enabled only on switching interfaces, L2 aggregation ports, or L2 encapsulation subinterfaces.

1.4.2 Prerequisites

DHCP Snooping is enabled by running the **ip dhcp snooping** 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 source IP address binding database.

ip source binding *mac-address* { **vlan** *vlan-id* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ipv4-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) Configure the function of converting source IP address binding entries to static MAC address entries.

ip source binding sticky-mac

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

(6) Enable IP Source Guard on an interface.

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

IP Source Guard is disabled on an interface by default.

(7) (Optional) Specify an excluded VLAN for IP Source Guard on an interface.

ip verify source exclude-vlan *vlan-id*

The function of specifying excluded VLANs for IP Source Guard on an interface is disabled by default.

Excluded VLANs can be specified on an interface only after IP Source Guard is enabled on the interface. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on the interface.

1.5 Enabling IP Source Guard on a VLAN

1.5.1 Overview

When IP Source Guard is enabled on a VLAN, the source IP addresses of IP packets in the VLAN will be checked to filter out invalid IP packets.

1.5.2 Prerequisites

DHCP Snooping is enabled by running the **ip dhcp snooping** command.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

ip source binding *mac-address* { **vlan** *vlan-id* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ip-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**]

IP Source Guard is disabled on a VLAN by default.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) (Optional) Configure trusted interfaces of IP Source Guard.

ip verify source trust

No IP Source Guard trusted interface is configured by default.

The IP Source Guard trusted interface function is mutually exclusive with the IP Source Guard interface, port security, 802.1x authorization, and Address Resolution Protocol (ARP) check services.

1.6 Enabling the Sole Role of the IP Source Address Binding Database as the Source of DAI Binding Entries

1.6.1 Overview

After the sole role of the source IP address binding database as the source of DAI binding entries is configured, the bound entries are solely used for Dynamic ARP Inspection (DAI) and are not assigned to the hardware. That is, IP Source Guard is not performed.

1.6.2 Procedure (Interface Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

ip source binding *mac-address* { **vlan** *vlan-id* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ip-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) Enable the sole role of the source IP address binding database as the source of DAI binding entries.

ip verify source dai-source

The sole role of the source IP address binding database as the source of DAI binding entries is not configured by default.

1.6.3 Procedure (VLAN Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

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

ip source binding *mac-address* { **vlan** *vlan-id* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ip-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 the sole role of the source IP address binding database as the source of DAI binding entries.

ip verify source dai-source

The sole role of the source IP address binding database as the source of DAI binding entries is not configured by default.

1.7 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 ip verify source [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays user filtering entries of IP Source Guard.
show ip source binding [*ipv4-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**] [**inner-vlan** *inner-vid*] [**vxlan** *vni*]	Displays information of the source IP address binding database.
show ip source binding sticky-mac [**interface** *interface-type interface-number*]	Displays information about source IP address binding entries converted to static MAC address entries.

1.8 Common Errors

- IP Source Guard is enabled on a DHCP Snooping trusted interface.
- An excluded VLAN is specified before IP Source Guard is enabled.