1 IP Source Guard Commands

Command	Function
ip source binding	Add static user information to the source IP address binding database.
ip source binding sticky-mac	Enable the function of converting source IP address binding entries to static MAC address entries.
ip verify source	Enable IP Source Guard on an interface or a VLAN.
ip verify source dai-source	Enable the sole role of the source IP address binding database as the source of Dynamic ARP Inspection (DAI) binding entries.
ip verify source exclude-vlan	Specify an excluded VLAN for IP Source Guard on an interface.
ip verify source trust	Configure an IP Source Guard trusted interface.
show ip source binding	Display information of the source IP address binding database.
show ip source binding sticky-mac	Display information about source IP address binding entries converted to static MAC address entries.
show ip verify source	Display user filtering entries of IP Source Guard.

1.1 ip source binding

Function

Run the **ip source binding** command to add static user information to the source IP address binding database.

Run the **no** form of this command to remove this configuration.

No static user information is added by default.

Syntax

ip source binding *mac-address* **vlan** *vlan-id ipv4-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

no ip source binding *mac-address* **vlan** *vlan-id ipv4-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

Parameter Description

mac-address: Media access control (MAC) address of a statically added user.

vlan-id: ID of the virtual local area network (VLAN) to which a statically added user belongs. For products that support QinQ termination, it refers to the outer VLAN ID of a user.

ipv4-address: IPv4 address of a statically added user.

interface *interface-type interface-number*: Specifies the interface statically added.

ip-mac: Specifies that the IP address and MAC address binding type is used globally.

ip-only: Specifies that the IP address binding type is used globally.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by Dynamic Host Configuration Protocol (DHCP).

This command can be configured only on L2 switching interfaces, L2 aggregation ports (link aggregation), and encapsulation subinterfaces. When this command is configured on other types of interfaces, the configuration will fail.

Users can configure global binding user records to enable legitimate users to pass IP Source Guard detection on all interfaces.

Note

- A configured binding record takes effect either on the access interface or globally.
- When duplicate user records exist, attributes of the new record will overwrite those of the old record.

Examples

The following example adds a static user record to the source IP address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IP address is 1.1.1.1, and the interface is GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
gigabitethernet 0/1
```

The following example adds a static user record to the source IP address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IP address is 1.1.1.1, and the filtering type is IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
```

Notifications

When the **no** form of this command is run to delete static configuration and the entered parameters are different from those previously configured, the following notification will be displayed:

```
% Failed to execute command, because of "No such binding entry[mac 0000.0000.0001
ip 1.1.1.1 vlan 2  GLOBAL]".
```

When a user record is configured and the entered wired interface is not an L2 switching interface, L2 aggregation port, or encapsulation sub-interface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current
interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip source binding sticky-mac

Function

Run the **ip source binding sticky-mac** command to enable the function of converting source IP address binding entries to static MAC address entries.

Run the **no** form of this command to disable this feature.

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

Syntax

ip source binding sticky-mac

no ip source binding sticky-mac

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The MAC address table records mapping between MAC addresses and interfaces. Unauthorized users can use MAC addresses of legitimate users to refresh MAC address table records, which will cause abnormal packet forwarding in the network. To prevent unauthorized users from refreshing the MAC address table to launch network attacks, configure this command in interface configuration mode to convert source IP address binding entries to static MAC address entries.

Examples

The following example enables the function of converting source IP address binding entries to static MAC address entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip source binding sticky-mac
```

Notifications

When the function of converting source IP address binding entries to static MAC address entries is enabled after the DHCP Snooping binding entry migration function is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When the function of converting source IP address binding entries to static MAC address entries is enabled on an interface after an access security control option, such as web authentication, 802.1x authentication, or port security is enabled on the interface, the following notification will be displayed:

```
%IP_SRC_GRD-STICKY_MAC: Failed to open sticky mac on interface [Interface name].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip verify source

Function

Run the **ip verify source** command to enable IP Source Guard on an interface or a VLAN.

Run the **no** form of this command to disable this feature.

IP Source Guard is disabled on an interface or a VLAN by default.

Syntax

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

no ip verify source

Parameter Description

port-security: Configures IP Source Guard based on IP address and MAC address.

Command Modes

Interface configuration mode

VLAN configuration mode

Default Level

14

Usage Guidelines

After IP Source Guard is enabled for an interface or a VLAN, users can detect IP packets passing through the interface or VLAN based on the IP address or IP address and MAC address.

This command can be configured only on L2 switching interfaces, L2 aggregation ports, encapsulation subinterfaces, and VLAN configuration mode. When this command is configured on other types of interfaces, the configuration will fail.

When IP Source Guard is enabled in VLAN configuration mode, it is effective to all L2 interfaces in the VLAN. Users need to configure the **ip verify source trust** command on the uplink interface to specify trusted interfaces. Otherwise, packet forwarding may fail.

⚠ Caution

Legitimate users of IP Source Guard come from DHCP Snooping and static user configuration. If IP Source Guard is enabled on an interface but no valid data source is configured, users who access the network through the interface cannot use the network normally.

Examples

The following example enables IP Source Guard on GigabitEthernet 0/1 and detects packets only based on the IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
```

The following example enables IP Source Guard on GigabitEthernet 0/1 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source port-security
```

The following example enables IP Source Guard on VLAN 1 and detects packets only based on the IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source
```

The following example enables IP Source Guard on VLAN 1 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source port-security
```

Notifications

When this command is configured on a DHCP trusted interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in
interface name".
```

Common Errors

- IP Source Guard is enabled. However, the source of legitimate user records is not configured.

Platform Description

N/A

Related Commands

N/A

1.4 ip verify source dai-source

Function

Run the **ip verify source dai-source** command to enable the sole role of the source IP address binding database as the source of Dynamic ARP Inspection (DAI) binding entries.

Run the **no** form of this command to remove this configuration.

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

Syntax

ip verify source dai-source

no ip verify source dai-source

Parameter Description

N/A

Command Modes

Interface configuration mode

VLAN configuration mode

Default Level

14

Usage Guidelines

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 DAI and are not assigned to hardware.

This command can be configured either in interface configuration mode or VLAN configuration mode.

Examples

The following example enables the sole role of the source IP address binding database as the source of DAI binding entries on switching interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source dai-source
```

The following example enables the sole role of the source IP address binding database as the source of DAI binding entries on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ip verify source dai-source
```

Notifications

When this command is configured on a DHCP Snooping or IP Source Guard trusted interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in
interface name".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip verify source exclude-vlan

Function

Run the **ip verify source exclude-vlan** command to specify an excluded VLAN for IP Source Guard on an interface.

Run the **no** form of this command to remove this configuration.

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

Syntax

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

vlan-id: ID of the VLAN that is not controlled by IP Source Guard on an interface. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

By using this command, the specified VLANs under an interface where the IP Source Guard function is enabled can be exempted from check and filtering.

After IP Source Guard is disabled on the interface, the specified excluded VLANs will be cleared automatically.

This command can be configured on L2 switching interfaces or encapsulation subinterfaces.

⚠ Caution

An excluded VLAN can be specified for an interface only after IP Source Guard is enabled on the interface.

Examples

The following example specifies VLAN 1 as an excluded VLAN for IP Source Guard on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
```

```
Hostname(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip verify source trust

Function

Run the **ip verify source trust** command to configure an IP Source Guard trusted interface.

Run the **no** form of this command to remove this configuration.

No IP Source Guard trusted interface is configured by default.

Syntax

ip verify source trust

no ip verify source trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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.

When an interface is configured as an IP Source Guard trusted interface, IP Source Guard is not performed for the interface and packets through this interface are released directly.

This command can be configured on L2 switching interfaces and L2 aggregation ports (link aggregation).

Caution

This command is used only to enable IPv6 Source Guard for a VLAN.

Examples

The following example configures GigabitEthernet 0/1 as an IP Source Guard trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source trust
```

Notifications

When this command is configured on an IPv6 Source Guard security interface, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict ".
```

Common Errors

- An IP Source Guard security interface is configured as an IP Source Guard trusted interface.

Platform Description

N/A

Related Commands

N/A

1.7 show ip source binding

Function

Run the **show ip source binding** command to display information of the source IP address binding database.

Syntax

show ip source binding [*ipv4-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]

Parameter Description

Ipv4-address: IPv4 address whose user binding information is displayed.

mac-address: MAC address whose user binding information is displayed.

vlan-id: VLAN whose user binding information is displayed.

interface-type interface-number: Wired access interface whose user binding information is displayed.

dhcp-snooping: Displays binding information of a dynamic user.

static: Displays binding information of a static user.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of the source IP address binding database.

```
Hostname> enable
Hostname# show ip source binding static
NO.   MACADDRESS         IPADDRESS       LEASE(SEC)   TYPE          VLAN
INTERFACE
1     0001.0002.0001     1.2.3.2         Infinite     Static        1     Global
2     0001.0002.0002     1.2.3.3         Infinite     Static        1
GigabitEthernet 0/1
3     0001.0002.0003     1.2.3.4         Infinite     Static        1     Global
4     0001.0002.0004     1.2.3.5         Infinite     Static        1     Global
Total number of bindings: 4
```

Table 1-1Output Fields of the show ip source binding Command

Field	Description
Total number of bindings	Number of bindings in the binding database
NO.	Record number
MACADDRESS	MAC address of a user
IPADDRESS	IP address of a user
LEASE(SEC)	Lease time of a record
TYPE	Record type
VLAN	VLAN to which a user belongs
INTERFACE	Interface name

Notifications

N/A

Platform Description

N/A

Related Commands

- ip source binding

1.8 show ip source binding sticky-mac

Function

Run the **show ip source binding sticky-mac** command to display information about source IP address binding entries converted to static MAC address entries.

Syntax

show ip source binding sticky-mac [**interface** *interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface under which information about source IP address binding entries converted to static MAC address entries is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about source IP address binding entries converted to static MAC address entries.

```
Hostname> enable
Hostname# show ip source binding sticky-mac
Total number of bindings: 2
NO.   MACADDRESS         TYPE          VLAN  INTERFACE
1     2018.0012.0017     Static        1     GigabitEthernet 0/1
2     2018.0012.0018     DHCP-Snooping 1     GigabitEthernet 0/1
```

Table 1-1Output Fields of the show ip source binding sticky-mac Command

Field	Description
Total number of bindings	Number of source IP address binding entries converted to static MAC address entries
NO	Record number
MACADDRESS	MAC address of a user
TYPE	Record type of a binding entry
VLAN	VLAN to which a user belongs
INTERFACE	User access interface

Notifications

N/A

Platform Description

N/A

Related Commands

- ip source binding sticky-mac

1.9 show ip verify source

Function

Run the **show ip verify source** command to display user filtering entries of IP Source Guard.

Syntax

show ip verify source [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface-type interface-number: Interface whose user filtering entries are displayed.

vlan *vlan-id*: Specifies the VLAN whose user filtering entries are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays user filtering entries of IP Source Guard.

```
Hostname> enable
Hostname# show ip verify source
NO.   INTERFACE            FilterType  FilterStatus           IPADDRESS
MACADDRESS      VLAN TYPE
1     Global               IP+MAC      Inactive-not-apply     192.168.0.127
0001.0002.0003  1 Static
2     Global               IP-ONLY     Active                 1.2.3.7
0001.0002.0007  1 Static
3     Global               IP+MAC      Active                 1.2.3.6
0001.0002.0006  1 Static
4     GigabitEthernet 0/1  UNSET       Inactive-restrict-off  1.2.3.9
0001.0002.0009  1 DHCP-Snooping
5     GigabitEthernet 0/5  IP-ONLY     Active                 Deny-All
```

Table 1-1Output Fields of the show ip verify source Command

Field	Description
Total number of bindings	Number of assigned bindings
NO.	Record number
INTERFACE	User access interface
FilterType	Record type of a binding entry
FilterStatus	Record status of a binding entry ● **Inactive-restrict-off**: IP Source Guard is disabled for the interface to which a binding record belongs. ● **Inactive-not-apply**: A bound user record cannot be converted to a filtering entry due to system errors. ● **Active**: The filtering entry corresponding to the bound user record has taken effect.
IPADDRESS	IP address of a user
MACADDRESS	MAC address of a user
VLAN TYPE	VLAN to which a user belongs

Notifications

N/A

Platform Description

N/A

Related Commands

- ip verify source