1 IPv6 Source Guard Commands

Command	Function
ipv6 source binding	Add static user information to the IPv6 source address binding database.
ipv6 source binding sticky-mac	Enable the function of converting IPv6 source address binding entries to static MAC address entries.
ipv6 verify source	Enable IPv6 Source Guard on an interface or a VLAN.
ipv6 verify source permit link-local	Enable local link address release on an interface.
ipv6 verify source trust	Configure an interface as an IPv6 Source Guard trusted interface.
show ipv6 source binding	Display information of the IPv6 source address binding database.
show ipv6 source binding sticky-mac	Display information about IPv6 source address binding entries converted to static MAC address entries.

1.1 ipv6 source binding

Function

Run the **ipv6 source binding** command to add static user information to the IPv6 source address binding database.

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

No static user information is added by default.

Syntax

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

no ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-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.

ipv6-address: IPv6 address of a statically added user.

interface *interface-type interface-number*: Specifies the interface to which a statically added user belongs.

ip-mac: Specifies that the IPv6 address and MAC address binding type is used globally.

ip-only: Specifies that the IPv6 address binding type is used globally.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Through this command, legitimate users can pass IPv6 Source Guard detection instead of being controlled by Dynamic Host Configuration Protocol version 6 (DHCPv6).

This command can be configured only on L2 switching interfaces and L2 aggregation ports (link aggregation). 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 IPv6 Source Guard detection on all interfaces.

A configured binding record takes effect either on the access interface, VLAN, 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 IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the interface is GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 interface
gigabitethernet 0/1
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-mac
```

The following example adds a static user record to the IPv6 source address binding database. In the static user record, the MAC address is 0000.0000.0001, the VLAN ID is 1, the IPv6 address is 1::1, and the filtering type is IPv6 address that takes effect globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-only
```

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".
```

When a user record is configured and the entered access interface is not an L2 switching interface or L2 aggregation port, 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 ipv6 source binding sticky-mac

Function

Run the **ipv6 source binding sticky-mac** command to enable the function of converting IPv6 source address binding entries to static MAC address entries.

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

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

Syntax

ipv6 source binding sticky-mac

no ipv6 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 IPv6 source address binding entries to static MAC address entries.

Examples

The following example enables the function of converting IPv6 source 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)# ipv6 source binding sticky-mac
```

Notifications

When the function of converting IPv6 source 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:

```
Failed to open sticky mac on interface [Interface name].
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ipv6 verify source

Function

Run the **ipv6 verify source** command to enable IPv6 Source Guard on an interface or a VLAN.

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

IPv6 Source Guard is disabled on an interface or a VLAN by default.

Syntax

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

no ipv6 verify source

Parameter Description

port-security: Configures IPv6 Source Guard based on IPv6 address and MAC address.

Command Modes

VLAN configuration mode

Interface configuration mode

Default Level

14

Usage Guidelines

By enabling IPv6 Source Guard on an interface or a VLAN through this command, users can detect packets based on the IPv6 address or IPv6 address and MAC address.

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

⚠ **Caution**

Legitimate users of IPv6 Source Guard come from DHCPv6 Snooping/ND Snooping and static user configuration. If IPv6 Source Guard is enabled on an interface but no valid data source is configured, users who access the network through IPv6 cannot use the network normally.

Examples

The following example enables IPv6 Source Guard on GigabitEthernet 0/1 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source
```

The following example enables IPv6 Source Guard on GigabitEthernet 0/1 and detects packets based on the IPv6 address and MAC address.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source port-security
```

The following example enables IPv6 Source Guard on VLAN 1 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ipv6 verify source
```

The following example enables IPv6 Source Guard on VLAN 1 and detects packets based on the IPv6 address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan 1
Hostname(config-vlan)# ipv6 verify source port-security
```

The following example enables IP Source Guard on VLANs 2-5 and detects packets only based on the IPv6 address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-5
Hostname(config-vlan-range)# ipv6 verify source
```

The following example enables IP Source Guard on VLANs 2-5 and detects packets based on the IP address and MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vlan range 2-5
Hostname(config-vlan-range)# ipv6 verify source port-security
```

Notifications

When this command is configured on a DHCPv6 or an IPv6 Source Guard trusted interface, the following notification will be displayed:

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

Common Errors

- IPv6 Source Guard is enabled. However, the source of legitimate user records is not configured.
- IPv6 Source Guard is enabled on a VLAN. However, the uplink interface is not configured as a trusted interface.

Platform Description

N/A

Related Commands

N/A

1.4 ipv6 verify source permit link-local

Function

Run the **ipv6 verify source permit link-local** command to enable local link address release on an interface.

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

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

Syntax

ipv6 verify source permit link-local

no ipv6 verify source permit link-local

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When the local link address release function is enabled on an interface by running this command, packets with FE80::/10 or ::/128 as source addresses will not be checked.

When ND Snooping is disabled, entry addresses come from only DHCPv6 addresses and do not contain local link addresses. However, some terminals use local link addresses to access the gateway or other addresses in the same network segment. In addition, local link addresses are required for addressing, Duplicate Address Detection (DAD), and other operations before DHCPv6 exchange. Therefore, in DHCPv6 Snooping + IPv6 Source Guard scenarios, run the **ipv6 verify source permit link-local** command to release local link addresses (fe80::/10) and undefined addresses (::/128).

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

⚠ **Caution**

The local link address release function needs to be configured only when both DHCPv6 Snooping and IPv6 Source Guard are enabled and ND Snooping is disabled. The configuration command for the local link address release function is independent of the DHCPv6 Snooping, IPv6 Source Guard, and ND Snooping commands.

Examples

The following example enables local link address release on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 verify source permit link-local
```

Notifications

When this command is configured on an AP member interface, the following notification will be displayed:

```
Configure is not supported on current interface.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 verify source trust

Function

Run the **ipv6 verify source trust** command to configure an interface as an IPv6 Source Guard trusted interface.

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

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

Syntax

ipv6 verify source trust

no ipv6 verify source trust

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When an interface is configured as an IPv6 Source Guard trusted interface, IPv6 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 IPv6 Source Guard trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 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 IPv6 Source Guard security interface is configured as an IPv6 Source Guard trusted interface.

Platform Description

N/A

Related Commands

- ipv6 verify source

1.6 show ipv6 source binding

Function

Run the **show ipv6 source binding** command to display information of the IPv6 source address binding database.

Syntax

show ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]

Parameter Description

ipv6-address: IPv6 address whose user binding information is displayed.

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

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

interface *interface-type interface-number*: Specifies the interface whose user binding information is displayed.

dhcp-snooping: Displays binding information of dynamic users.

static: Displays binding information of static users.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information of the IPv6 source address binding database.

```
Hostname> enable
Hostname# show ipv6 source binding
Total entries found: 2
No.    Ipv6 Address                             Mac Address    VLAN Interface
Type
1      2017::2                                  00e0.4c36.077d 100  GLOBAL
Static/DHCPv6
2      2017::3                                  9890.96ca.c3d5 100  GLOBAL
Static
```

Table 1-1Output Fields of the show ipv6 source binding Command

Field	Description
Total number of bindings	Number of bindings in the binding database
NO	Record number
Ipv6 Address	IPv6 address of a user
Mac Address	MAC address of a user
VLAN	VLAN to which a user belongs
Interface	Interface name or global interface
Type	Record type

Notifications

N/A

Platform Description

N/A

Related Commands

- ipv6 source binding

1.7 show ipv6 source binding sticky-mac

Function

Run the **show ipv6 source binding sticky-mac** command to display information about IPv6 source address binding entries converted to static MAC address entries.

Syntax

show ipv6 source binding sticky-mac [**interface** *interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface under which information about IPv6 source 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 IPv6 source address binding entries converted to static MAC address entries.

```
Hostname> enable
Hostname# show ipv6 source binding sticky-mac
Total number of bindings: 1
NO.   MACADDRESS         VLAN  INTERFACE
1     2018.0012.0017     1     GigabitEthernet 0/1
```

Table 1-1Output Fields of the show ipv6 source binding sticky-mac Command

Field	Description
Total number of bindings	Number of assigned bindings
NO.	Record number
MACADDRESS	MAC address of a user
VLAN	VLAN to which a user belongs
INTERFACE	User access interface

Notifications

N/A

Platform Description

N/A

Related Commands

- **ipv6 source binding sticky-mac**