Contents

Configuring IP source guard

Overview

IP source guard (IPSG) prevents spoofing attacks by using an IPSG binding table to match legitimate packets. It drops all packets that do not match the table.

The IPSG binding table can include the following bindings:

- IP-interface.
- MAC-interface.
- IP-MAC-interface.
- IP-VLAN-interface.
- MAC-VLAN-interface.
- IP-MAC-VLAN-interface.
- IP-MAC.

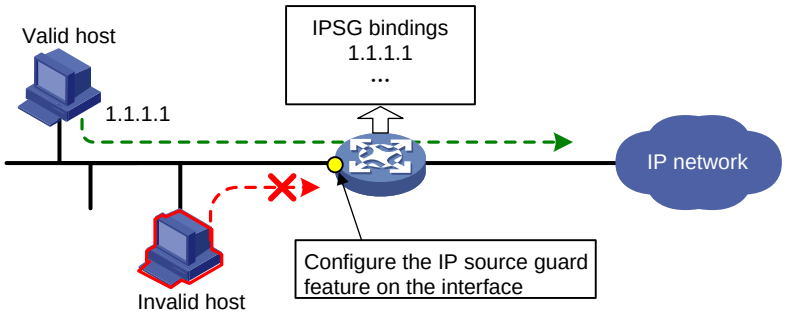
IPSG bindings include static bindings that are configured manually and dynamic bindings that are generated based on information from other modules.

NOTE:

Global IPSG supports only static IP-MAC bindings. For more information about global static IPSG bindings, see "Static IPSG bindings."

As shown in Figure 1, IPSG on the interface forwards only the packets that match one of the IPSG bindings.

Figure 1 Diagram for the IPSG feature



NOTE:

IPSG is a per-interface packet filter. Configuring the feature on one interface does not affect packet forwarding on another interface.

Static IPSG bindings

Static IPSG bindings are configured manually. They are suitable for scenarios where few hosts exist on a LAN and their IP addresses are manually configured. For example, you can configure a static IPSG binding on an interface that connects to a server. This binding allows the interface to receive packets only from the server.

Static IPSG bindings on an interface implement the following functions:

- Filter incoming IPv4 or IPv6 packets on the interface.
- Cooperate with ARP detection in IPv4 for user validity checking.

For information about ARP detection, see "Configuring ARP attack protection."

Static IPSG bindings can be global or interface-specific. IPSG first uses the interface-specific bindings to match packets. If no match is found, IPSG uses the global bindings.

- **Global static binding**—Binds the IP address and MAC address in system view. The binding takes effect on all interfaces to filter packets for user spoofing attack prevention.
- **Interface-specific static binding**—Binds the IP address, MAC address, VLAN, or any combination of the items in interface view. The binding takes effect only on the interface to check the validity of users who are attempting to access the interface.

Dynamic IPSG bindings

IPSG automatically obtains user information from other modules to generate dynamic bindings. The source modules include DHCP relay, DHCP snooping, DHCPv6 snooping, and DHCP server.

DHCP-based IPSG bindings are suitable for scenarios where hosts on a LAN obtain IP addresses through DHCP. IPSG is configured on the DHCP snooping device or the DHCP relay agent. It generates dynamic IPSG bindings based on the DHCP snooping entries or DHCP relay entries. IPSG allows only packets from the DHCP clients to pass through.

Dynamic IPv4SG

Dynamic bindings generated based on different source modules are for different usages:

Interface types	Source modules	Binding usage
Layer 2 Ethernet port	DHCP snooping	Packet filtering.
VLAN interface	DHCP relay agent	Packet filtering.
	DHCP server	For cooperation with modules (such as the ARP detection module) to provide security services.

For information about DHCP snooping, DHCP relay, and DHCP server see *Layer 3—IP Services Configuration Guide*.

Dynamic IPv6SG

IPv6SG on an interface obtains information from DHCPv6 snooping entries to generate bindings for packet filtering.

For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.

IPSG configuration task list

To configure IPv4SG, perform the following tasks:

Tasks at a glance
(Required.) Enabling IPv4SG on an interface
(Optional.) Configuring a static IPv4SG binding

To configure IPv6SG, perform the following tasks:

Tasks at a glance
(Required.) Enabling IPv6SG on an interface
(Optional.) Configuring a static IPv6SG binding

Configuring the IPv4SG feature

Enabling IPv4SG on an interface

When you enable IPSG on an interface, the static and dynamic IPSG are both enabled.

- Static IPv4SG uses static bindings configured by using the **ip source binding** command.
- Dynamic IPv4SG generates dynamic bindings from related source modules. IPv4SG uses the bindings to filter incoming IPv4 packets based on the matching criteria specified in the **ip verify source** command.

To implement dynamic IPv4SG, make sure the DHCP snooping or DHCP relay feature operates correctly on the network.

To enable the IPv4SG feature on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The following interface types are supported: • Layer 2 Ethernet interface. • VLAN interface.
3. Enable the IPv4SG feature.	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	By default, the IPv4SG feature is disabled on an interface. If you configure this command on an interface multiple times, the most recent configuration takes effect.

Configuring a static IPv4SG binding

You can configure global static and interface-specific static IPv4SG bindings.

Global static bindings take effect on all interfaces.

Interface-specific static bindings take priority over global static bindings. An interface first uses the static bindings on the interface to match packets. If no match is found, the interface uses the global bindings.

Configuring a global static IPv4SG binding

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a global static IPv4SG binding.	**ip source binding ip-address** *ip-address* **mac-address** *mac-address*	No global static IPv4SG binding exists.

Configuring a static IPv4SG binding on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The following interface types are supported: • Layer 2 Ethernet interface. • VLAN interface.
3. Configure a static IPv4SG binding.	**ip source binding** { **ip-address** *ip-address* **| ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	By default, no static IPv4SG binding is configured on an interface. The **vlan** *vlan-id* option is supported only in Layer 2 Ethernet interface view. To configure a static IPv4SG binding for the ARP detection function, the **vlan** *vlan-id* option must be specified, and ARP detection must be enabled for the specified VLAN. You can configure the same static IPv4SG binding on different interfaces.

Configuring the IPv6SG feature

Enabling IPv6SG on an interface

When you enable IPv6SG on an interface, the static and dynamic IPv6SG are both enabled.

- Static IPv6SG uses static bindings configured by using the **ipv6 source binding** command.
- Dynamic IPv6SG generates dynamic bindings from related source modules. IPv6SG uses the bindings to filter incoming IPv6 packets based on the matching criteria specified in the **ipv6 verify source** command.

To implement dynamic IPv6SG, make sure DHCPv6 snooping operates correctly on the network.

To enable the IPv6SG feature on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The following interface types are supported: • Layer 2 Ethernet interface. • VLAN interface.
3. Enable the IPv6SG feature.	**ipv6 verify source** { **ip-address** | **ip-address mac-address | mac-address** }	By default, the IPv6SG feature is disabled on an interface. If you configure this command on an interface multiple times, the most recent configuration takes effect.

Configuring a static IPv6SG binding

You can configure global static and interface-specific static IPv6SG bindings.

Global static bindings take effect on all interfaces.

Interface-specific static bindings take priority over global static bindings. An interface first uses the static bindings on the interface to match packets. If no match is found, the interface uses the global bindings.

Configuring a global static IPv6SG binding

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a global static IPv6SG binding.	**ipv6 source binding ip-address** *ipv6-address* **mac-address** *mac-address*	No global static IPv6SG binding exists.

Configuring a static IPv6SG binding on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The following interface types are supported: • Layer 2 Ethernet interface. • VLAN interface.
3. Configure a static IPv6SG binding.	**ipv6 source binding** { **ip-address** *ipv6-address* **| ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	By default, no static IPv6SG binding is configured on an interface. The **vlan** *vlan-id* option is supported only in Layer 2 Ethernet interface view. You can configure the same static IPv6SG binding on different interfaces.

Displaying and maintaining IPSG

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display IPv4SG bindings.	**display ip source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcp-relay** | **dhcp-server** | **dhcp-snooping**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]
Display IPv6SG bindings.	**display ipv6 source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

IPSG configuration examples

Static IPv4SG configuration example

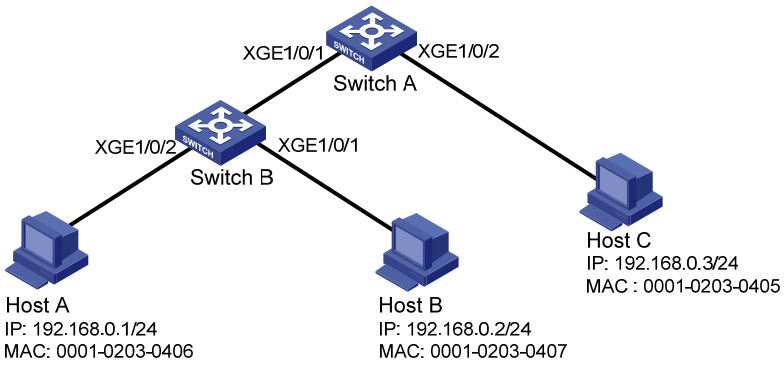
Network requirements

As shown in Figure 2, all hosts use static IP addresses.

Configure static IPv4SG bindings on Switch A and Switch B to meet the following requirements:

- Ten-GigabitEthernet 1/0/2 of Switch A allows only IP packets from Host C to pass.
- Ten-GigabitEthernet 1/0/1 of Switch A allows only IP packets from Host A to pass.
- All interfaces of Switch B allow IP packets from Host A to pass.
- Ten-GigabitEthernet 1/0/1 of Switch B allows IP packets from Host B to pass.

Figure 2 Network diagram



Configuration procedure

1. Configure Switch A:

   # Configure IP addresses for the interfaces. (Details not shown.)

   # Enable IPv4SG on Ten-GigabitEthernet 1/0/2.

   ```
   <SwitchA> system-view
   [SwitchA] interface ten-gigabitethernet 1/0/2
   [SwitchA-Ten-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   ```

   # On Ten-GigabitEthernet 1/0/2, configure a static IPv4SG binding for Host C.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3
   mac-address 0001-0203-0405
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

   # Enable IPv4SG on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   ```

   # On Ten-GigabitEthernet 1/0/1, configure a static IPv4SG binding for Host A.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1
   mac-address 0001-0203-0406
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

2. Configure Switch B:

   # Configure an IP address for each interface. (Details not shown.)

   # Enable IPv4SG on Ten-GigabitEthernet 1/0/2.

   ```
   <SwitchB> system-view
   ```

```
[SwitchB] interface ten-gigabitethernet 1/0/2
[SwitchB-Ten-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchB-Ten-GigabitEthernet1/0/2] quit
```

Configure a static IPv4SG binding for Host A.

```
[SwitchB] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

Enable IPv4SG on Ten-GigabitEthernet 1/0/1.

```
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

On Ten-GigabitEthernet 1/0/1, configure a static IPv4SG binding for Host B.

```
[SwitchB-Ten-GigabitEthernet1/0/1] ip source binding mac-address 0001-0203-0407
[SwitchB-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that the static IPv4SG bindings are configured successfully on Switch A.

```
<SwitchA> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface                 VLAN Type
192.168.0.1     0001-0203-0405 XGE1/0/2                  N/A  Static
192.168.0.3     0001-0203-0406 XGE1/0/1                  N/A  Static
```

Verify that the static IPv4SG bindings are configured successfully on Device B.

```
<SwitchB> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 N/A                     N/A  Static
N/A             0001-0203-0407 XGE1/0/1                N/A  Static
```

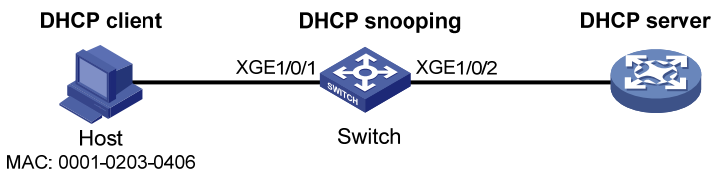
Dynamic IPv4SG using DHCP snooping configuration example

Network requirements

As shown in Figure 3, the host (the DHCP client) obtains an IP address from the DHCP server. Perform the following tasks:

- Enable DHCP snooping on the switch to make sure the DHCP client obtains an IP address from the authorized DHCP server. To generate a DHCP snooping entry for the DHCP client, enable recording of client information in DHCP snooping entries.
- Enable dynamic IPv4SG on Ten-GigabitEthernet 1/0/1 to filter incoming packets by using the IPv4SG bindings generated based on DHCP snooping entries. Only packets from the DHCP client are allowed to pass.

Figure 3 Network diagram



Configuration procedure

1. Configure the DHCP server.

For information about DHCP server configuration, see *Layer 3—IP Services Configuration Guide.*

2. Configure the switch:

   # Configure IP addresses for the interfaces. (Details not shown.)

   # Enable DHCP snooping.

   ```
   <Switch> system-view
   [Switch] dhcp snooping enable
   ```

   # Configure Ten-GigabitEthernet 1/0/2 as a trusted interface.

   ```
   [Switch] interface ten-gigabitethernet 1/0/2
   [Switch-Ten-GigabitEthernet1/0/2] dhcp snooping trust
   [Switch-Ten-GigabitEthernet1/0/2] quit
   ```

   # Enable IPv4SG on Ten-GigabitEthernet 1/0/1 and verify the source IP address and MAC address for dynamic IPSG.

   ```
   [Switch] interface ten-gigabitethernet 1/0/1
   [Switch-Ten-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   ```

   # Enable recording of client information in DHCP snooping entries on Ten-GigabitEthernet 1/0/1.

   ```
   [Switch-Ten-GigabitEthernet1/0/1] dhcp snooping binding record
   [Switch-Ten-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Verify that a dynamic IPv4SG binding is generated based on a DHCP snooping entry

```
[Switch] display ip source binding dhcp-snooping
Total entries found: 1
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 XGE1/0/1                  1    DHCP snooping
```

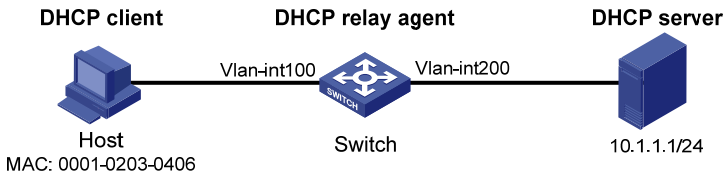
Dynamic IPv4SG using DHCP relay agent configuration example

Network requirements

As shown in Figure 4, DHCP relay agent is enabled on the switch. The host obtains an IP address from the DHCP server through the DHCP relay agent.

Enable dynamic IPv4SG on VLAN-interface 100 to filter incoming packets by using the IPv4SG bindings generated based on DHCP relay entries.

Figure 4 Network diagram



Configuration procedure

1. Configure dynamic IPv4SG:

   # Configure IP addresses for the interfaces. (Details not shown.)

   # Enable IPv4SG on VLAN-interface 100 and verify the source IP address and MAC address for dynamic IPSG.

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
[Switch-Vlan-interface100] quit
```

2. Configure the DHCP relay agent:

   # Enable the DHCP service.

   ```
   [Switch] dhcp enable
   ```

   # Enable recording DHCP relay client entries.

   ```
   [Switch] dhcp relay client-information record
   ```

   # Configure VLAN-interface 100 to operate in DHCP relay mode.

   ```
   [Switch] interface vlan-interface 100
   [Switch-Vlan-interface100] dhcp select relay
   ```

   # Specify the IP address of the DHCP server.

   ```
   [Switch-Vlan-interface100] dhcp relay server-address 10.1.1.1
   [Switch-Vlan-interface100] quit
   ```

Verifying the configuration

Verify that a dynamic IPv4SG binding is generated based on a DHCP relay entry.

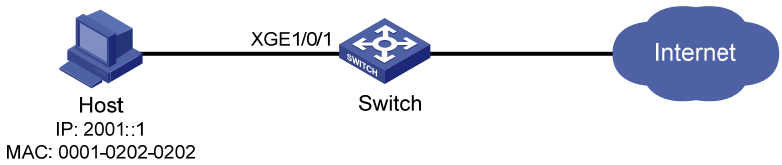
```
[Switch] display ip source binding dhcp-relay
Total entries found: 1
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 Vlan100                 100  DHCP relay
```

Static IPv6SG configuration example

Network requirements

As shown in Figure 5, configure a static IPv6SG binding for Ten-GigabitEthernet 1/0/1 of the device to allow only IPv6 packets from the host to pass.

Figure 5 Network diagram



Configuration procedure

Enable IPv6SG on Ten-GigabitEthernet 1/0/1.

```
<Switch> system-view
[Switch] interface ten-gigabitethernet 1/0/1
[Switch-Ten-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

On Ten-GigabitEthernet 1/0/1, configure a static IPv6SG binding for the host.

```
[Switch-Ten-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0001-0202-0202
[Switch-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that the static IPv6SG binding is configured successfully on the switch.

```
[Switch] display ipv6 source binding static
```

```
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              0001-0202-0202 XGE1/0/1                 N/A  Static
```

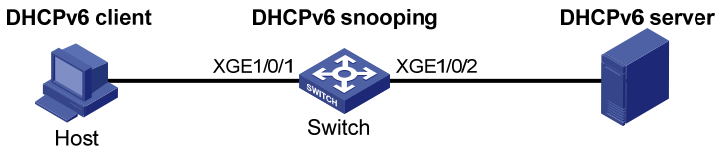
Dynamic IPv6SG using DHCPv6 snooping configuration example

Network requirements

As shown in Figure 6, the host (the DHCPv6 client) obtains an IP address from the DHCPv6 server. Perform the following tasks:

- Enable DHCPv6 snooping on the switch to make sure the DHCPv6 client obtains an IPv6 address from the authorized DHCPv6 server. To generate a DHCPv6 snooping entry for the DHCPv6 client, enable recording of client information in DHCPv6 snooping entries.
- Enable dynamic IPv6SG on Ten-GigabitEthernet 1/0/1 to filter incoming packets by using the IPv6SG bindings generated based on DHCPv6 snooping entries. Only packets from the DHCPv6 client are allowed to pass.

Figure 6 Network diagram



Configuration procedure

1. Configure DHCPv6 snooping:

   # Enable DHCPv6 snooping globally.

   ```
   <Switch> system-view
   [Switch] ipv6 dhcp snooping enable
   ```

   # Configure the interface connecting to the DHCP server as a trusted interface.

   ```
   [Switch] interface ten-gigabitethernet 1/0/2
   [Switch-Ten-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
   [Switch-Ten-GigabitEthernet1/0/2] quit
   ```

2. Enable IPv6SG:

   # Enable IPv6SG on Ten-GigabitEthernet 1/0/1 and verify the source IP address and MAC address for dynamic IPv6SG.

   ```
   [Switch] interface ten-gigabitethernet 1/0/1
   [Switch-Ten-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
   ```

   # Enable recording of client information in DHCPv6 snooping entries on Ten-GigabitEthernet 1/0/1.

   ```
   [Switch-Ten-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
   [Switch-Ten-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Verify that a dynamic IPv6SG binding is generated based on a DHCPv6 snooping entry.

```
[Switch] display ipv6 source binding dhcpv6-snooping
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              040a-0000-0001 XGE1/0/1               1    DHCPv6 snooping
```