Contents

1 Configuring SAVI

1.1 Introduction

1.1.1 Overview

Source Address Validation Improvement (SAVI) establishes a binding list based on the source IPv4/IPv6 addresses, source media access control (MAC) addresses, and access device ports for access devices through Control Packet Snooping (CPS) so as to verify the source addresses of IP packets through a specified port. The binding list sources include neighbor discovery (ND) Snooping, Dynamic Host Configuration Protocol version 6 (DHCPv6) Snooping, and static address configuration. Only packets whose source addresses match binding entries will be forwarded. This ensures the authenticity of source addresses of data packets in the network.

This document mainly describes the application of SAVI in IPv6 networks in stateful address configuration (DHCPv6 generally), stateless address autoconfiguration (SLAAC), and static address configuration scenarios.

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 MAC address field in L2 packets.

- ND Snooping

  ND Snooping is used to snoop the SLAAC process of clients. The device with ND Snooping enabled extracts a client's IPv6 address and MAC address from a packet and generates a binding entry together with the port ID (interface index) and virtual local area network (VLAN) ID of the client.

- DHCPv6 Snooping

  DHCPv6 Snooping is used to snoop dynamical IPv6 address obtaining of clients through DHCPv6. The device with DHCPv6 Snooping enabled extracts a client's IPv6 address, MAC address, and lease from a packet and generates a binding entry together with the port ID (interface index) and VLAN ID of the client.

2. Checking the Source Address Fields of Packets

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

When SAVI 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 SAVI binding entries 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 SAVI binding entries can pass through the interface.

- Filtering based on the source IPv6 address and MAC address

  The source IPv6 addresses and MAC addresses of all IPv6 packets passing through an interface are checked. Only the packets whose source IPv6 addresses and MAC addresses match SAVI binding entries can pass through the interface.

1.1.3 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4861: Neighbor Discovery for IP version 6
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 6959: SAVI Threat Scope
- RFC 6620: FCFS SAVI Improvement for Locally Assigned IPv6 Addresses
- RFC 8074: SAVI for Mixed Address Assignment Methods Scenario
- RFC 7039: SAVI Framework
- RFC 7513: Solution for DHCP

1.2 Restrictions and Guidelines

- SAVI-related commands can be configured only after SAVI is enabled globally.
- Typically, SAVI 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 SAVI 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.
- Typically, SAVI is not enabled on DHCPv6 Snooping and ND Snooping trusted interfaces.
- After SAVI is enabled on an interface, the interface will deny all data packets whose source IPv6 addresses are not in the binding list. For control packets, only ICMPv6 packets of types 133, 134, 135, 136, 137, and 143 are permitted.
- After SAVI is enabled on an interface, the permit rules of IPv6 packets are related to the IPv6 address binding mode of global IP address and MAC address binding. The default address binding mode is the strict mode. In this mode, if IPv4 SAVI is enabled but IPv6 SAVI is disabled on an interface, all IPv6 packets through the interface will be intercepted. When IPv4 SAVI is enabled but IPv6 SAVI is disabled on all interfaces, it is recommended that the IPv6 address binding mode of global IP address and MAC address binding be set to the loose mode.

1.3 Configuring SAVI

(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.

savi 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) (Optional) Configure the data source of SAVI binding entries.

savi ipv6 bind-source add { **slaac** | **dhcp** }

Binding entries generated during the SLAAC and DHCPv6 processes are used as the sources of dynamic binding entries by default. Binding entries can also be statically configured.

(5) (Optional) Configure SAVI to permit local link addresses and undefined addresses.

savi ipv6 check permit link-local

Permitting local link addresses and undefined addresses is not configured by default.

After configuration, SAVI permits all IPv6 packets with fe80::/10 and ::/128 as source addresses.

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

(6) (Optional) Enable binding entry migration.

savi ipv6 station-move

The binding entry migration function is disabled by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IPv6 SAVI.

savi ipv6 check source ip-address [**mac-address**]

IPv6 SAVI is disabled by default.

(9) (Optional) Configure the excluded VLANs for SAVI on an interface.

savi ipv6 check source exclude-vlan *vlan-id*

No excluded VLANs for SAVI are configured on an interface by default.

After SAVI is enabled on an interface, you can run this command to permit IPv6 packets of some VLANs.

1.4 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 savi ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**type** { **static** | **dhcp** | **slaac** }]	Displays information of the IPv6 source address binding database.

Command	Purpose
show savi ipv6 check source [*ipv6-address* | **interface** *interface-type interface-number*]	Displays effective IPv6 SAVI filtering entries.

1.5 Configuration Examples

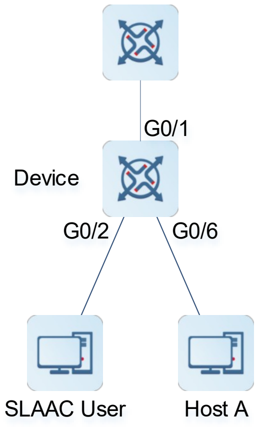
1.5.1 Configuring SAVI in an SLAAC-Only Scenario

1. Requirements

Enterprise devices connect to user hosts. No DHCPv6 server is deployed in the network, and hosts can obtain IPv6 addresses only through SLAAC. To prevent attackers from sending invalid IPv6 packets (including ND packets and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-1 Configuring SAVI in an SLAAC-Only Scenario



3. Notes

- Enable ND Snooping.
- Enable SAVI.

4. Procedure

Enable ND Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 nd snooping enable
```

Enable SAVI.

```
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-
address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-
address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

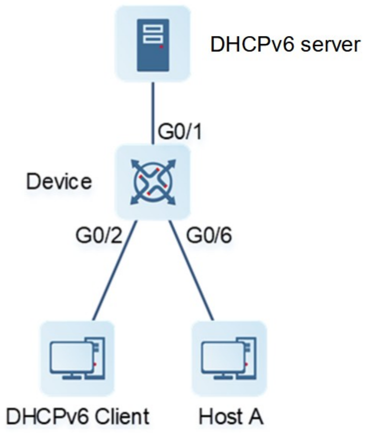
1.5.2 Configuring SAVI in a DHCPv6-Only Scenario

1. Requirements

Enterprise devices connect to user hosts. For unified IPv6 address management, hosts obtain IPv6 addresses through DHCPv6. To prevent attackers from sending invalid IPv6 packets (including DHCPv6 packets and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-1 Configuring SAVI in a DHCPv6-Only Scenario



3. Notes

- Enable DHCPv6 Snooping.
- Enable SAVI.

4. Procedure

Enable DHCPv6 Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 dhcp snooping
```

Enable SAVI.

```
Device(config)# savi ipv6 check permit link-local
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-
address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-
address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
```

```
!
ipv6 dhcp snooping
savi ipv6 check permit link-local
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

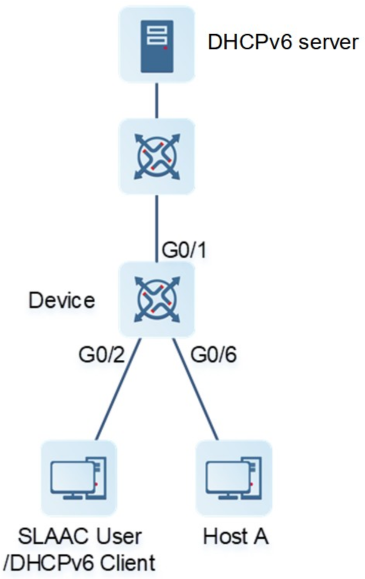
1.5.3 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario

1. Requirements

Enterprise devices connect to user hosts. Some hosts obtain IPv6 addresses through SLAAC, and some hosts obtain IPv6 addresses through DHCPv6. To prevent attackers from sending invalid IPv6 packets (including DHCPv6 packets, ND packets, and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-1 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario



3. Notes

- Enable ND Snooping and DHCPv6 Snooping.
- Enable SAVI.

4. Procedure

Enable ND Snooping and DHCPv6 Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 nd snooping enable
Device(config)# ipv6 dhcp snooping
```

Enable SAVI.

```
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
ipv6 dhcp snooping
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
 ipv6 dhcp snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

1.6 Common Errors

SAVI is enabled on a DHCPv6 Snooping/ND Snooping trusted interface.