Contents

1 Configuring DAI

1.1 Introduction

1.1.1 Overview

Dynamic ARP Inspection (DAI) is used to check the validity of received Address Resolution Protocol (ARP) packets and discard invalid ARP packets to prevent ARP spoofing and improve network stability. DAI generates ARP filtering information based on the legitimate user information (IP address or IP address and MAC address) generated by security application modules, such as IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, and port security to filter out invalid ARP packets in the network.

1.1.2 Principles

1. Interface Trust Status

A device processes ARP packets based on the trust status of each interface. It regards ARP packets received through trusted interfaces as valid and does not perform DAI on such packets, and strictly performs DAI on packets received through untrusted interfaces.

In a typical network, L2 interfaces connected to network devices should be set as trusted interfaces, and L2 interfaces connected to hosts should be set as untrusted interfaces.

Notice

- After DAI is enabled, it is recommended that the uplink interfaces be configured as DAI trusted interfaces. If the uplink interfaces are not DAI trusted interfaces but trusted interfaces of other security functions, ARP packets will be filtered out because the interfaces do not have entries required for DAI.
- If another access security control command is configured on an interface, the interface cannot be configured as a DAI trusted interface. To set the interface as a DAI trusted interface, disable the configured security control command.

2. Filtering out Invalid ARP Packets

Due to defects of ARP, ARP cannot check the validity of received ARP packets. Attackers can easily use vulnerabilities of the protocol to launch ARP spoofing.

When DAI is enabled on a specified virtual local area network (VLAN), a device will intercept all ARP requests and responses transmitted through untrusted interfaces. The device matches the source IP addresses and media access control (MAC) addresses of the ARP packets received through its interfaces with the valid user records in the security database. With successful matching, packets will be transferred, or otherwise they will be discarded.

1.1.3 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Configuring DAI

1.2.1 Restrictions and Guidelines

- DAI cannot be enabled for Dynamic Host Configuration Protocol (DHCP) Snooping trusted interfaces in a VLAN.
- When DAI is disabled, it does not take effect to all interfaces in a VLAN. When ARP Check is still effective on an interface, the device will check ARP packets transmitted through the interface.
- DAI has the same functions as ARP Check. The only difference is that DAI is enabled for VLANs, and ARP Check is enabled for interfaces.

1.2.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DAI on a VLAN.

ip arp inspection vlan { *vlan-id* | *word* }

DAI is disabled on all VLANs by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure L2 interfaces as DAI trusted interfaces.

ip arp inspection trust

L2 interfaces are DAI untrusted interfaces by default.

(6) Configure the ARP packet receiving rate.

For details, see the rate limit command of NFPP.

1.3 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 arp inspection vlan [*vlan-id* | *vlan-range*]	Displays whether DAI is enabled for a VLAN.
show ip arp inspection interface	Displays the DAI configuration status on L2 interfaces.

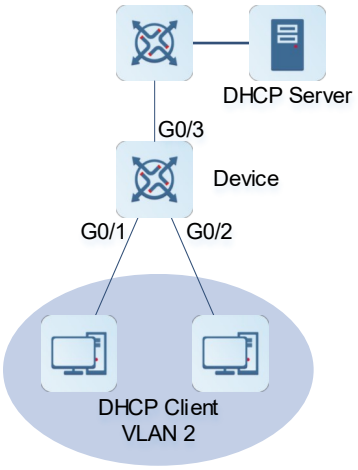
1.4 Configuration Examples

1.4.1 Requirements

Hosts can use only addresses assigned by a legitimate DHCP server to prevent ARP spoofing.

1.4.2 Topology

Figure 1-1 Configuring DAI



1.4.3 Notes

- Enable DHCP Snooping on the access device and set the interface (GigabitEthernet 0/3 in this example) connected to the legitimate DHCP server as a trusted interface.
- Enable IP Source Guard on the access device.
- Enable DAI after DHCP Snooping and IP Source Guard are enabled.

1.4.4 Procedure

Enable DHCP Snooping and IP Source Guard.

```
Device> enable
Device# configure terminal
Device(config)# interface range gigabitEthernet 0/1-2
Device(config-if-range)# switchport access vlan 2
Device(config-if-range)# ip verify source
Device(config-if-range)# exit
Device(config)# ip dhcp snooping
```

Configure DAI.

```
Device(config)# ip arp inspection vlan 2
```

Configure the trusted interface.

```
Device(config)# interface gigabitethernet 0/3
Device(config-if-GigabitEthernet 0/3)# switchport access vlan 2
Device(config-if-GigabitEthernet 0/3)# ip dhcp snooping trust
```

```
Device(config-if-GigabitEthernet 0/3)# ip arp inspection trust
```

1.4.5 Verification

Check whether DHCP Snooping, IP Source Guard and DAI are enabled, and whether the trusted interface is correct.

```
Device# show ip dhcp snooping
Switch DHCP snooping status                     :   ENABLE
DHCP snooping verify hardware address status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE

Interface                       Trusted         Rate limit (pps)
------------------------        -------         ----------------
GigabitEthernet 0/3             YES             unlimited
Default                         No              unlimited
Device# show ip verify source
NO.   INTERFACE                 FilterType FilterStatus           IPADDRESS
MACADDRESS     VLAN TYPE
----- ------------------------- ---------- ---------------------  ---------------
-------------- ---- -------------
1     GigabitEthernet 0/1       IP-ONLY    Active                 Deny-All
2     GigabitEthernet 0/2       IP-ONLY    Active                 Deny-All

Total number of bindings: 2
Device# show ip arp inspection vlan
Vlan Configuration
---- -------------
2    Enable
```

1.4.6 Configuration Files

```
hostname Device
!
ip arp inspection vlan 2
ip dhcp snooping
!
interface GigabitEthernet 0/1
 switchport access vlan 2
 ip verify source
!
interface GigabitEthernet 0/2
 switchport access vlan 2
 ip verify source
!
interface GigabitEthernet 0/3
 switchport access vlan 2
```

```
 ip arp inspection trust
 ip dhcp snooping trust
!
end
```

1.4.7 Common Errors

An interface configured with security limitations is set as a DAI trusted interface.