

Contents

Introduction	1
Prerequisites	1
Example: Configuring ARP attack protection	1
Network configuration	1
Analysis	2
Applicable hardware and software versions.....	2
Restrictions and guidelines	4
Procedures	5
Configuring VLANs and interface IP addresses	5
Enabling ARP blackhole routing	5
Enabling ARP active acknowledgment in strict mode.....	6
Disabling gratuitous ARP packet learning.....	6
Enabling ARP packet rate limit and setting the limit rate.....	6
Configuring ARP source suppression	6
Configuring source MAC-based ARP attack detection	6
Verifying the configuration	7
Configuration files	7

Introduction

This document provides configuration examples of ARP attack protection.

ARP is easy to use but it does not have any security mechanisms. Attackers can easily attack the network by sending forged ARP packets. The device provides various ARP attack protection measures to prevent, detect, and resolve ARP attacks and ARP viruses on LANs.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of ARP attack protection.

Example: Configuring ARP attack protection

Network configuration

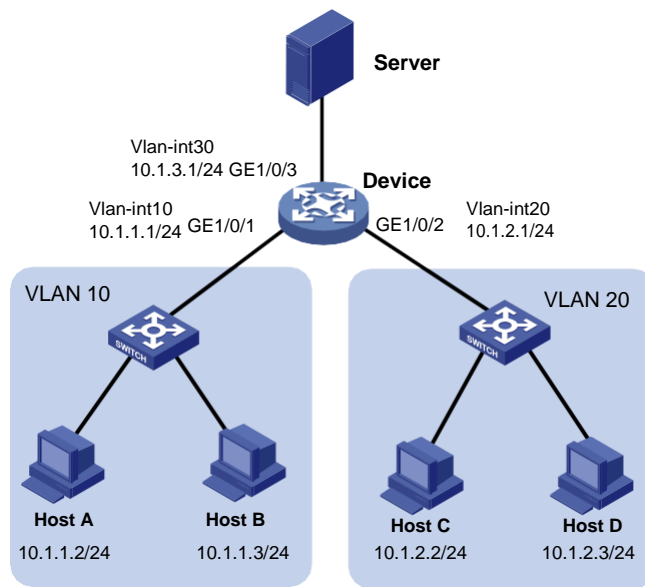
As shown in [Figure 1](#), the device connects to the server through GE1/0/3 as a gateway and connects to Host A and Host B in VLAN 10, and Host C and Host D in VLAN 20 through GE1/0/1 and GE1/0/2, respectively.

Configure ARP attack protection on the device to prevent the following ARP threats:

- Host A sends forged ARP packets and forged gratuitous ARP packets to the device to edit the ARP entries on the device maliciously. As a result, other users cannot receive data packets normally.
- Host C sends a large number of unresolvable IP packets to attack the device, causing the following results:
 - The device CPU is busy, affecting normal service processing.
 - The device sends a large number of ARP requests, overloading the target subnets.
- Host D launches ARP flood attacks by sending a large number of ARP packets with different source IP addresses but fixed MAC address. Such attacks run out the ARP table resources on the device and cause a busy CPU, affecting normal service processing.

Besides, Host B might send a large number of ARP packets to the device. This is normal ARP behavior required by services. Do not filter out packets sent from Host B when you configure ARP attack protection.

Figure 1 Network diagram



Analysis

To meet the network requirements, configure the device as follows:

- To prevent forged ARP packets sent by Host A from updating the ARP entries on the device, configure ARP blackhole routing and ARP active acknowledgement in strict mode.
- To prevent the forged gratuitous ARP packets sent by Host A from updating the ARP entries on the device, disable gratuitous ARP packet learning.
- To avoid unresolvable packets sent by Host C, enable ARP source suppression and set the maximum number of unresolvable packets that the device can process per source IP address within 5 seconds.
- To avoid ARP flood attacks caused by ARP packets with the same IP address, enable ARP packet rate limit and set the limit rate. When Host C launches ARP flood attacks on the device by sending a large number of ARP packets with the same source IP address, the device discards the packets that exceed the limit rate to avoid a busy CPU.
- To avoid ARP flood attacks caused by ARP packets with different IP addresses but fixed MAC address sent by Host D, configure source MAC-based ARP attack detection. If you fail to configure this feature, the ARP table resources run out and the CPU is busy. To avoid filtering out packets sent by Host B, exclude the MAC address of Host B from this detection.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
S6520X-HI switch series SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

Restrictions and guidelines

When you configure ARP attack protection, follow these restrictions and guidelines:

- When you configure ARP active acknowledgement in strict mode, make sure ARP blackhole routing is enabled.
- After you disable gratuitous ARP packet learning, the device does not create ARP entries when receiving gratuitous ARP packets, but updates the existing corresponding ARP entries. If you do not want the device to create ARP entries for gratuitous ARP packets, disable gratuitous ARP packet learning to save ARP entry resources.

Procedures

Configuring VLANs and interface IP addresses

(Optional.) Configure the operating mode of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as Layer 2.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-mode bridge
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-mode bridge
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port link-mode bridge
[Device-GigabitEthernet1/0/3] quit
```

Create VLAN 10, and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
```

Create VLAN-interface 10, and assign IP address 10.1.1.1/24 to it.

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
[Device-Vlan-interface10] quit
```

Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.

```
[Device] vlan 20
[Device-vlan20] port gigabitethernet 1/0/2
[Device-vlan20] quit
```

Create VLAN-interface 20, and assign IP address 10.1.2.1/24 to it.

```
[Device] interface vlan-interface 20
[Device-Vlan-interface20] ip address 10.1.2.1 255.255.255.0
[Device-Vlan-interface20] quit
```

Create VLAN 30, and assign GigabitEthernet 1/0/3 to the VLAN.

```
[Device] vlan 30
[Device-vlan30] port gigabitethernet 1/0/3
[Device-vlan30] quit
```

Create VLAN-interface 30, and assign IP address 10.1.3.1/24 to it.

```
[Device] interface vlan-interface 30
[Device-Vlan-interface30] ip address 10.1.3.1 255.255.255.0
```

Enabling ARP blackhole routing

```
<Device> system-view
[Device] arp resolving-route enable
```

Enabling ARP active acknowledgment in strict mode

```
<Device> system-view
[Device] arp active-ack strict enable
```

Disabling gratuitous ARP packet learning

```
<Device> system-view
[Device] undo gratuitous-arp-learning enable
```

Enabling ARP packet rate limit and setting the limit rate

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] arp rate-limit 50
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] arp rate-limit 50
[Device-GigabitEthernet1/0/2] quit
```

Configuring ARP source suppression

```
[Device] arp source-suppression enable
[Device] arp source-suppression limit 40
```

Configuring source MAC-based ARP attack detection

The following switch series in R661x version do not support this feature:

- SC 5525 switch series.
- SC 5520 switch series.

Enable source MAC-based ARP attack detection, and specify the handling method as filter.

```
<Device> system-view
[Device] arp source-mac filter
```

Set the threshold to 30.

```
[Device] arp source-mac threshold 30
```

Set the lifetime for ARP attack entries to 60 seconds.

```
[Device] arp source-mac aging-time 60

# Exclude MAC address 0c68-d691-0606 from this detection.
[Device] arp source-mac exclude-mac 0c68-d691-0606
```

Verifying the configuration

Display the current configuration information about ARP source suppression. ARP source suppression is enabled and the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds is 40.

```
<Device> display arp source-suppression
ARP source suppression is enable
Current suppression limit: 40
```

Display the ARP attack entries for Host D when Host D sends more than 30 ARP requests to the device within 5 seconds. The command output shows that an ARP attack entry has been generated for Host D. With this ARP attack entry, the device cannot create ARP entries for Host D.

```
<Device> display arp source-mac slot 1

Source-MAC      VLAN ID Interface      Aging time (sec)  Packets dropped
0c68-be82-0206  20      GE1/0/2              10                244
```

```
<Device> display arp
Type: S-Static  D-Dynamic  O-Openflow  R-Rule  M-Multiport  I-Invalid
IP address      MAC address  VLAN/VSI name Interface      Aging Type
```

Display the ARP attack entries when Host B sends more than 30 ARP requests to the device within 5 seconds. No ARP attack entries for Host B exist, so the device can create ARP entries for Host B.

```
<Device> display arp source-mac slot 1

Source-MAC      VLAN ID Interface      Aging time (sec)  Packets dropped
<Device> display arp
Type: S-Static  D-Dynamic  O-Openflow  R-Rule  M-Multiport  I-Invalid
IP address      MAC address  VLAN/VSI name Interface      Aging Type
10.1.1.3        0c68-d691-0606  10          GE1/0/1          1197  D
```

Stop sending ARP packets from Host D to the device and wait the lifetime of the ARP attack entry for Host D expires. Then, configure Host D to send ARP packets to the device. Use the following command to display ARP entries on the device. The output shows that the device has created ARP entries for Host D.

```
<Device> display arp
Type: S-Static  D-Dynamic  O-Openflow  R-Rule  M-Multiport  I-Invalid
IP address      MAC address  VLAN/VSI name Interface      Aging Type
10.1.1.3        0c68-d691-0606  10          GE1/0/1          944   D
10.1.2.3        0c68-be82-0206  20          GE1/0/2          1195  D
```

Configuration files



IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 1

#
```



```

vlan 10

#
vlan 20

#
vlan 30

#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0

#
interface Vlan-interface20
 ip address 10.1.2.1 255.255.255.0

#
interface Vlan-interface30
 ip address 10.1.3.1 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 arp rate-limit 50

#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 arp rate-limit 50

#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
 undo gratuitous-arp-learning enable
 arp source-mac filter
 arp source-mac aging-time 60
 arp source-mac exclude-mac 0c68-d691-0606
 arp active-ack strict enable
 arp source-suppression enable
 arp source-suppression limit 40

```