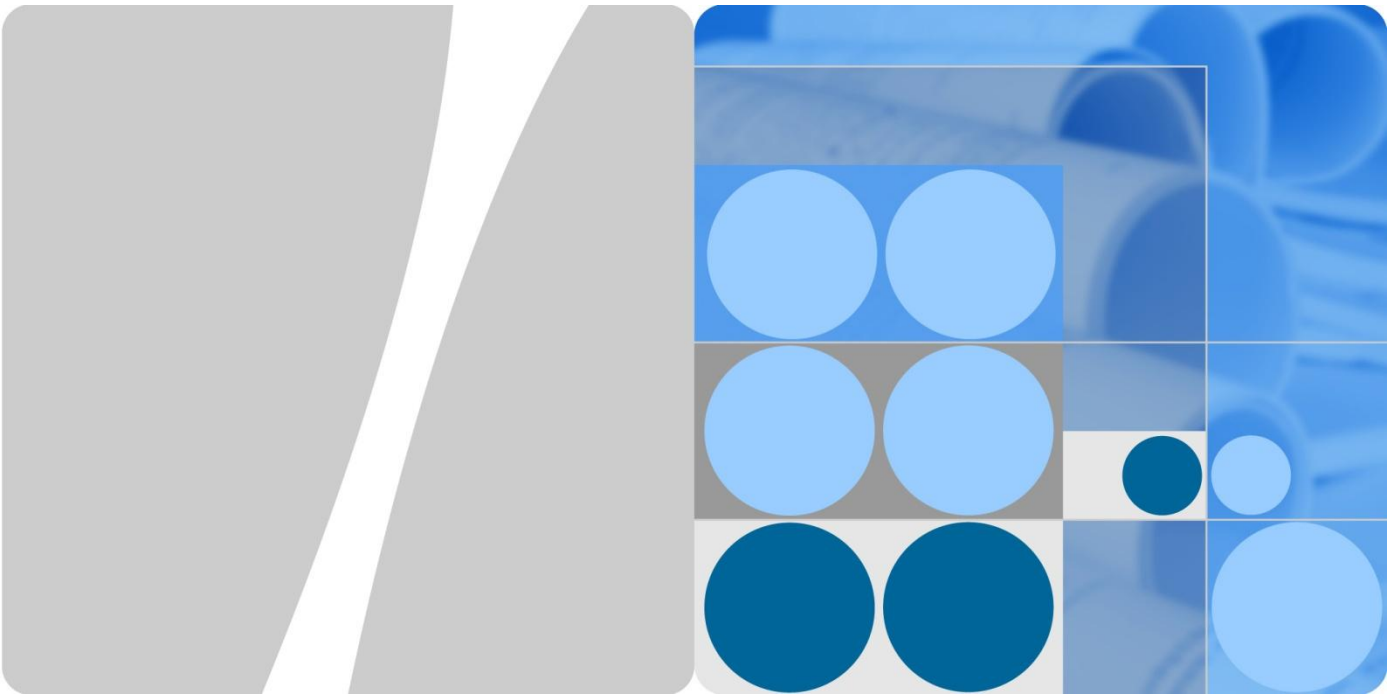


ARP Security Technology White Paper

Issue 01

Date 2012-09-10

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 ARP Security

About This Chapter

1.1 Introduction to ARP Security

Definition

Address Resolution Protocol (ARP) security prevents ARP attacks and ARP-based network scanning attacks using a series of methods such as strict ARP learning, dynamic ARP inspection (DAI), ARP anti-spoofing, and rate limit on ARP packets.

Purpose

ARP is easy to use but has no security mechanisms. Attackers often use ARP to attack network devices. The following ARP attack modes are commonly used on networks:

- ARP flood attack: ARP flood attacks, also called denial of service (DoS) attacks, occur in the following scenarios:
  - System resources are consumed when the device processes ARP packets and maintains ARP entries. To ensure that ARP entries can be queried efficiently, a maximum number of ARP entries is set on the device. Attackers send a large number of bogus ARP packets with variable source IP addresses to the device. In this case, APR entries on the device are exhausted and the device cannot generate ARP entries for ARP packets from authorized users. Consequently, communication is interrupted.
  - When attackers scan hosts on the local network segment or other network segments, the attackers send many IP packets with unresolvable destination IP addresses to attack the device. As a result, the device triggers many ARP Miss messages, generates a large number of temporary ARP entries, and broadcasts ARP Request packets to resolve the destination IP addresses, leading to CPU overload.
- ARP spoofing attack: An attacker sends bogus ARP packets to network devices. The devices then modify ARP entries, causing communication failures.

ARP attacks cause the following problems:

- Network connections are unstable and communication is interrupted, leading to economic loss.
- Attackers initiate ARP spoofing attacks to intercept user packets to obtain accounts and passwords of systems such as the game, online bank, and file server, leading to losses.

To avoid the preceding problems, the device provides multiple techniques to defend against ARP attacks.

Table 1-1 describes various ARP security techniques for defending against different ARP attacks.

Table 1-1 ARP security techniques for defending against different ARP attacks

Attack Type	Attack Defense Function	Deployment
ARP flood attack	Rate limit on ARP packets	You are advised to enable this function on the gateway.
	Rate limit on ARP Miss messages	You are advised to enable this function on the gateway.

Attack Type	Attack Defense Function	Deployment
	Gratuitous ARP packet discarding	You are advised to enable this function on the gateway.
	Strict ARP learning	You are advised to enable this function on the gateway.
	ARP entry limiting	You are advised to enable this function on the gateway.
ARP spoofing attack	ARP entry fixing	You are advised to enable this function on the gateway.
	DAI	You are advised to enable this function on an access device. **NOTE** *When ARP learning triggered by DHCP is enabled on the gateway, DAI must be enabled on the gateway.*
	ARP gateway anti-collision	You are advised to enable this function on the gateway.
	Gratuitous ARP packet discarding	You are advised to enable this function on the gateway.
	Gratuitous ARP packet sending	You are advised to enable this function on the gateway.
	MAC address consistency check in an ARP packet	You are advised to enable this function on the gateway.
	ARP packet validity check	You are advised to enable this function on the gateway or an access device.
	Strict ARP learning	You are advised to enable this function on the gateway.
	ARP learning triggered by DHCP	You are advised to enable this function on the gateway.
	ARP proxy on a VPLS network	You are advised to enable this function on a PE.

Benefits

- Reduces maintenance costs for network operating and security.
- Provides users with stable services on a secure network.

1.2 Principles

1.2.1 Rate Limit on ARP Packets

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

The device provides the following mechanisms for limiting the rate of ARP packets:

- Limiting the rate of ARP packets based on the source MAC address or source IP address

  When detecting that a host sends a large number of ARP packets in a short period, the device limits the rate of ARP packets sent from this host based on the source MAC address or source IP address. If the number of ARP packets received within a specified period exceeds the threshold, the device discards the excess ARP packets.

  - Limiting the rate of ARP packets based on the source MAC address: If a MAC address is specified, the device applies the rate limit to ARP packets from this source MAC address; otherwise, the device applies the rate limit to all ARP packets.

    Configure rate limit on ARP packets based on the source MAC address.

    1. Set the maximum rate of ARP packets from a source MAC address to 100 pps.

       ```
       [Quidway] arp speed-limit source-mac maximum 100
       ```

    2. Set the maximum rate of ARP packets from a specified MAC address 0-0-1 to 50 pps.

       ```
       [Quidway] arp speed-limit source-mac 0-0-1 maximum 50
       ```

  - Limiting the rate of ARP packets based on the source IP address: If an IP address is specified, the device applies the rate limit to ARP packets from this source IP address; otherwise, the device applies the rate limit to all ARP packets.

    Configure rate limit on ARP packets based on the source IP address.

    1. Set the maximum rate of ARP packets from a source IP address to 100 pps.

       ```
       [Quidway] arp speed-limit source-ip maximum 100
       ```

    2. Set the maximum rate of ARP packets from a specified IP address 10.0.0.1 to 50 pps.

       ```
       [Quidway] arp speed-limit source-ip 10.0.0.1 maximum 50
       ```

- Limiting the rate of ARP packets on a VLANIF interface of a super-VLAN

  A VLANIF interface of a super-VLAN is triggered to learn ARP entries in the following scenarios:

- The VLANIF interface receives IP packets triggering ARP Miss messages. For details about ARP Miss messages, see 1.2.2 Rate Limit on ARP Miss Messages.
- The VLANIF interface enabled with ARP proxy receives ARP packets with the destination IP address matching proxy conditions but matching no ARP entry.

The VLANIF interface replicates ARP Request packets in each sub-VLAN when learning ARP entries. If a large number of sub-VLANs are configured for the super-VLAN, the device generates a large number of ARP Request packets. As a result, the CPU is busy processing ARP Request packets, and other services are affected. To prevent this problem, limit the rate of ARP packets on the VLANIF interface of a super-VLAN.

You can run the following command to globally set the maximum rate of broadcast ARP Request packets on the VLANIF interface of a super-VLAN to 500 pps.

```
[Quidway] arp speed-limit flood-rate 500
```

- Limiting the rate on ARP packets globally, in a VLAN, or on an interface

  The maximum rate and rate limit duration of ARP packets can be set globally, in a VLAN, or on an interface. The configurations on an interface, in a VLAN, and globally takes effect in descending order of priority.

  In addition, the duration for blocking ARP packets can be set on an interface. If the number of ARP packets received within a specified rate limit duration exceeds the threshold (the maximum number of ARP packets), the device discards the excess ARP packets and discards all received ARP packets in a specified duration (duration for blocking ARP packets).

  - Limiting the rate of ARP packets globally: limits the number of ARP packets to be processed by the system. When an ARP attack occurs, the device limits the rate of ARP packets globally.
  - Limiting the rate of ARP packets in a VLAN: limits the number of ARP packets to be processed on all interfaces in a VLAN. The configuration in a VLAN does not affect ARP entry learning on interfaces in other VLANs.
  - Limiting the rate of ARP packets on an interface: limits the number of ARP packets to be processed on an interface. The configuration on an interface does not affect ARP entry learning on other interfaces.
  - Configure rate limit on ARP packets globally, in a VLAN, or on an interface.

    1. Configure the device to allow 200 ARP packets to pass through in 1 second globally.

       ```
       [Quidway] arp anti-attack rate-limit enable
       [Quidway] arp anti-attack rate-limit 200
       ```

    2. Configure the device to allow 200 ARP packets from VLAN 100 to pass through in 1 second.

       ```
       [Quidway] vlan 100
       [Quidway-vlan100] arp anti-attack rate-limit enable
       [Quidway-vlan100] arp anti-attack rate-limit 200
       ```

    3. Configure GE1/0/1 to allow 200 ARP packets to pass through in 10 seconds, and configure the device to discard all ARP packets received on GE1/0/1 in 60 seconds when the number of ARP packets exceeds the limit.

       ```
       [Quidway] interface gigabitethernet1/0/1
       [Quidway-GigabitEthernet1/0/1] arp anti-attack rate-limit enable
       ```

```
[Quidway-GigabitEthernet1/0/1] arp anti-attack rate-limit 200 10 block
timer 60
```

1.2.2 Rate Limit on ARP Miss Messages

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the master control board for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, the device provides multiple techniques to limit the rate on ARP Miss messages.

- Limiting the rate of ARP Miss messages based on the source IP address

  If the number of ARP Miss messages triggered by IP packets from a source IP address in 1 second exceeds the limit, the device considers that an attack is initiated from the source IP address.

  If the ARP Miss packet processing mode is set to **block**, the CPU of the device discards excess ARP Miss messages and delivers an ACL to discard all subsequent packets that are sent from this source IP address. If the ARP Miss packet processing mode is set to **none-block**, the CPU discards excess ARP Miss messages. When ARP Miss messages are discarded, corresponding ARP Miss packets are discarded.

  If a source IP address is specified, the rate of ARP Miss messages triggered by IP packets from the source IP address is limited. If no source IP address is specified, the rate of ARP Miss messages triggered by IP packets from each source IP address is limited.

  Configure rate limit on ARP Miss messages based on the source IP address.

  - Set the maximum number of ARP Miss messages triggered by each source IP address in 1 second to 50.

    ```
    [Quidway] arp-miss speed-limit source-ip maximum 50
    ```

  - Set the maximum number of ARP Miss messages triggered by the IP address 10.0.0.1 in 1 second to 100, and set the maximum number of ARP Miss messages triggered by other source IP addresses in 1 second to 50.

    ```
    [Quidway] arp-miss speed-limit source-ip maximum 50
    [Quidway] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
    ```

- Limiting the rate of ARP Miss messages globally, in a VLAN, or on an interface

  The maximum number of ARP Miss massages can be set globally, in a VLAN, or on an interface. The configurations on an interface, in a VLAN, and globally takes effect in descending order of priority.

  - Limiting the rate of ARP Miss messages globally: limits the number of ARP Miss messages processed by the system.
  - Limiting the rate of ARP Miss messages in a VLAN: limits the number of ARP Miss messages to be processed on all interfaces in a VLAN. The configuration in a VLAN does not affect IP packet forwarding on interfaces in other VLANs.
  - Limiting the rate of ARP Miss messages on an interface: limits the number of ARP Miss messages to be processed on an interface. The configuration on an interface does not affect IP packet forwarding on other interfaces.

Configure rate limit on ARP Miss messages globally, in a VLAN, or on an interface.

- Configure the device to process a maximum of 200 ARP Miss messages in 1 second.

```
[Quidway] arp-miss anti-attack rate-limit enable
[Quidway] arp-miss anti-attack rate-limit 200
```

- Configure the device to process ARP Miss messages triggered by a maximum of 200 IP packets from VLAN 100 in 1 second.

```
[Quidway] vlan 100
[Quidway-vlan100] arp-miss anti-attack rate-limit enable
[Quidway-vlan100] arp-miss anti-attack rate-limit 200
```

- Configure the device to process ARP Miss messages triggered by a maximum of 200 IP packets from GE1/0/1 in 10 seconds.

```
[Quidway] interface gigabitethernet1/0/1
[Quidway-GigabitEthernet1/0/1] arp-miss anti-attack rate-limit enable
[Quidway-GigabitEthernet1/0/1] arp-miss anti-attack rate-limit 200 10
```

- Limiting the rate of ARP Miss messages by setting the aging time of temporary ARP entries

  When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

  - In the aging time of temporary ARP entries:
  - An IP packet that is received before the ARP Reply packet and matches a temporary ARP entry is discarded and triggers no ARP Miss message.
  - After receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
  - When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages are triggered again and temporary ARP entries are regenerated. This process continues.

  When ARP Miss attacks occur on the device, you can extend the aging time of temporary ARP entries and reduce the frequency of triggering ARP Miss messages to minimize the impact on the device.

  You can run the following commands to set the aging time of temporary ARP entries to 10 seconds on VLANIF 10:

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp-fake expire-time 10
```

1.2.3 Gratuitous ARP Packet Discarding

In a gratuitous ARP packet, the source IP address and destination IP address are both the local IP address, the source MAC address is the local MAC address, and the destination MAC address is a broadcast address. When a host connects to a network, the host broadcasts a gratuitous ARP packet to notify other devices on the network of its MAC address and to check whether any device uses the same IP address as its own IP address in the broadcast domain. When the MAC address of a host changes, the host sends a gratuitous ARP packet to notify all hosts before the ARP entry ages out.

Any host can send gratuitous ARP packets, causing the following problems:

- If a large number of gratuitous ARP packets are broadcast on the network, the device cannot process valid ARP packets due to CPU overload.

- If the device processes bogus gratuitous ARP packets, ARP entries are updated incorrectly, leading to communication interruptions.

To solve the preceding problems, enable the gratuitous ARP packet discarding function on the gateway.

CAUTION

If the gratuitous ARP packet discarding function is enabled on the gateway, other hosts on the network cannot update their ARP entries when a host uses a new MAC address to connect to the network. Consequently, other hosts cannot communicate with this host. When a host changes the interface card and restarts, or the standby node takes over the active node due to faults in a two-node cluster hot backup system, a host connects to the network with a new MAC address.

Enable the gratuitous ARP packet discarding function.

- Enable gratuitous ARP packet discarding globally.

```
[Quidway] arp anti-attack gratuitous-arp drop
```

- Enable gratuitous ARP packet discarding on VLANIF 10.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp anti-attack gratuitous-arp drop
```

1.2.4 Strict ARP Learning

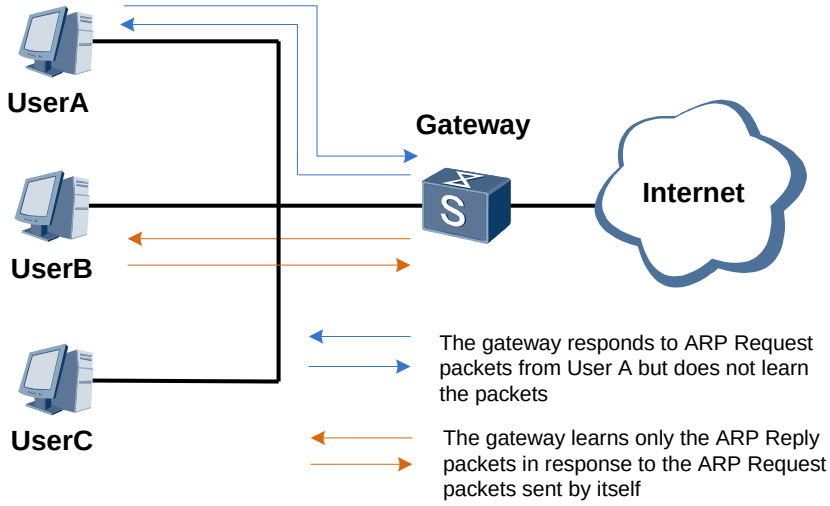
If many users send a large number of ARP packets to a device at the same time, or attackers send bogus ARP packets to the device, the following problems occur:

- Many CPU resources are consumed to process a large number of ARP packets. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- Bogus ARP packets modify ARP entries on the device. As a result, the device cannot communicate with other devices.

To avoid the preceding problems, deploy the strict ARP learning function on the gateway.

After strict ARP learning function is enabled, the device learns only ARP entries for ARP reply packets in response to ARP request packets sent by itself. In this way, the device can defend against most ARP attacks.

Figure 1-1 Strict ARP learning



As shown in Figure 1-1, after receiving an ARP Request packet from UserA, the gateway sends an ARP Reply packet to UserA and adds or updates an ARP entry matching UserA. After the strict ARP learning function is enabled on the gateway:

- When receiving an ARP Request packet from UserA, the gateway adds or updates no ARP entry matching UserA. If the ARP Request packet requests the MAC address of the gateway, the gateway sends an ARP Reply packet to UserA.
- If the gateway sends an ARP Request packet to UserB, the gateway adds or updates an ARP entry matching UserB after receiving the ARP Reply packet.

  Enable strict ARP learning.

  - Enable strict ARP learning globally.

    ```
    [Quidway] arp learning strict
    ```

  - Enable strict ARP learning on VLANIF 10.

    ```
    [Quidway] interface vlanif 10
    [Quidway-Vlanif10] arp learning strict force-enable
    ```

1.2.5 ARP Entry Limiting

The ARP entry limiting function controls the number of ARP entries that a gateway interface can learn. By default, the number of ARP entries that an interface can dynamically learn is the same as the default number of ARP entries supported by the device. After the ARP entry limiting function is deployed, if the number of ARP entries that a specified interface dynamically learned reaches the maximum, the interface cannot learn any ARP entry. This prevents ARP entries from being exhausted when a host connecting to this interface initiates ARP attacks.

Configure the ARP entry limiting function.

- Configure VLANIF 10 to dynamically learn a maximum of 20 ARP entries.

  ```
  [Quidway] interface vlanif 10
  [Quidway-Vlanif10] arp-limit maximum 20
  ```

- Configure GE1/0/1 to dynamically learn a maximum of 20 ARP entries corresponding to VLAN 10.

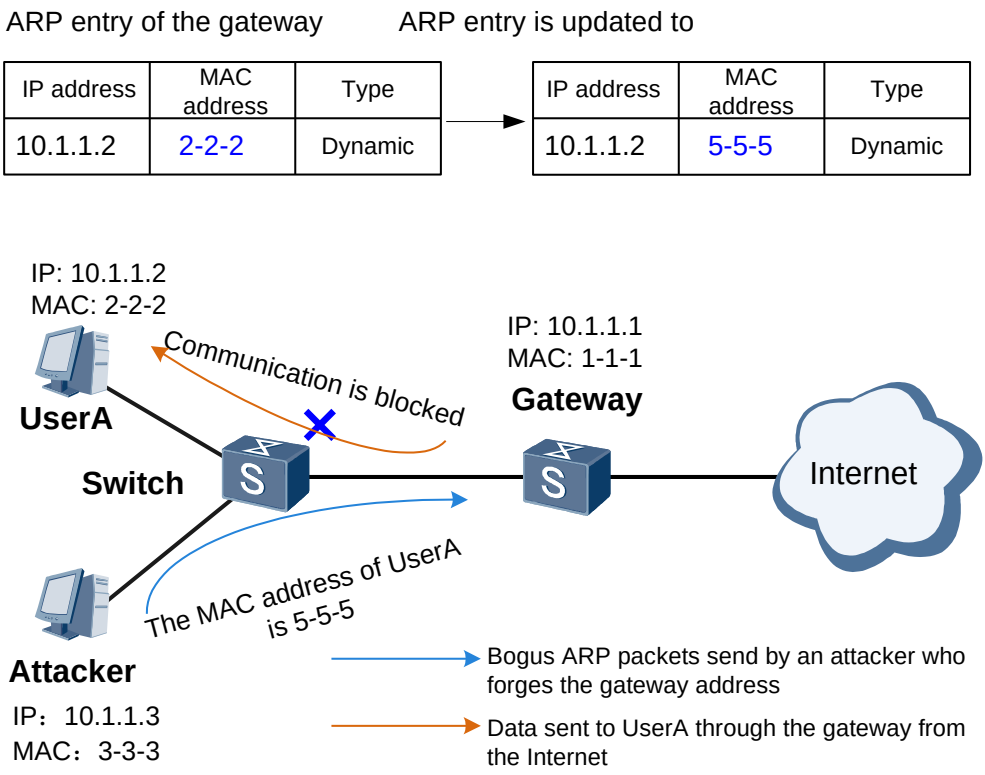
  ```
  [Quidway] interface gigabitethernet1/0/1
  ```

```
[Quidway-GigabitEthernet1/0/1] arp-limit vlan 10 maximum 20
```

1.2.6 ARP Entry Fixing

As shown in Figure 1-2, an attacker simulates UserA to send a bogus ARP packet to the gateway. The gateway then records an incorrect ARP entry for UserA. As a result, UserA cannot communicate with the gateway.

Figure 1-2 ARP gateway spoofing attack



To defend against ARP gateway spoofing attacks, deploy the ARP entry fixing function on the gateway. After the gateway with this function enabled learns an ARP entry for the first time, it does not change the ARP entry, only updates part of the entry, or sends a unicast ARP Request packet to check validity of the ARP packet for updating the entry.

The device supports three ARP entry fixing modes, as described in Table 1-2.

Table 1-2 ARP entry fixing modes

Mode	Description
fixed-all	When receiving an ARP packet, the device discards the packet if the MAC address, interface number, or VLAN ID matches no ARP entry. This mode applies to networks that use static IP addresses and have no redundant link.

Mode	Description
fixed-mac	When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry. This mode applies to networks where users need to change access interfaces.
send-ack	When the device receives ARP packet A with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user. • If the device receives ARP Reply packet B within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP entry are the same as those in ARP Reply packet B, the device considers ARP packet A as an attack packet and does not update the ARP entry. • If the device receives no ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of the ARP entry are different from those in ARP Reply packet B, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address again. – If the device receives ARP Reply packet C within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP packet A are the same as those in ARP Reply packet C, the device considers ARP packet A as a valid packet and update the ARP entry based on ARP packet A. – If the device receives no ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of ARP packet A are different from those in ARP Reply packet C, the device considers ARP packet A as an attack packet and does not update the ARP entry. This mode applies to networks that use dynamic IP addresses and have no redundant link.

Configure ARP entry fixing.

- Enable ARP entry fixing globally and specify the **fixed-mac** mode.

```
[Quidway] arp anti-attack entry-check fixed-mac enable
```

- Enable ARP entry fixing on VLANIF 10 and specify the **send-ack** mode.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp anti-attack entry-check send-ack enable
```

1.2.7 DAI

A man-in-the-middle (MITM) attack is a common ARP spoofing attack.

Figure 1-3 Man-in-the-middle attack

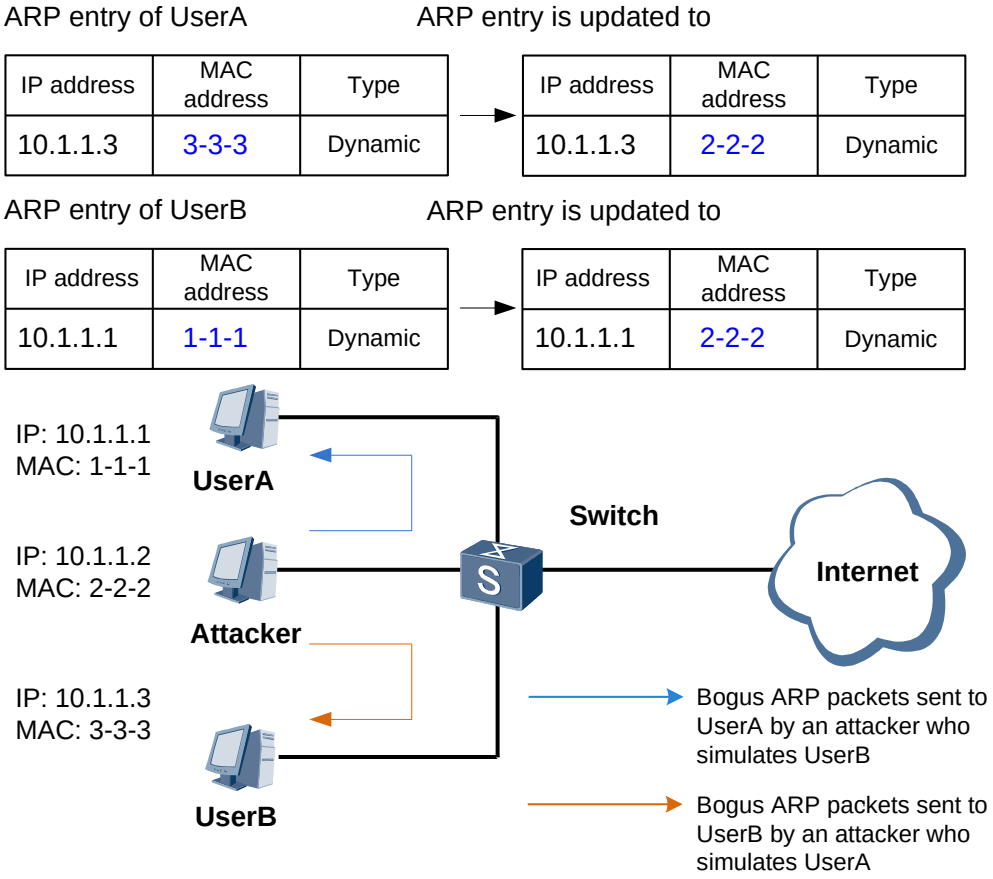


Figure 1-3 shows an MITM attack scenario. An attacker simulates UserB to send a bogus ARP packet to UserA. UserA then records an incorrect ARP entry for UserB. The attacker easily obtains information exchanged between UserA and UserB. Information security between UserA and UserB is not protected.

To defend against MITM attacks, deploy DAI on the switch.

DAI defends against MITM attacks using DHCP snooping. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

NOTE

This function is available only when DHCP snooping is configured. The device enabled with DHCP snooping generates DHCP snooping binding entries when DHCP users go online. If a user uses a static IP address, you need to manually configure a static DHCP snooping binding entry for the user.

For details about DHCP snooping, see description in *Technical White Paper for DHCP Snooping*.

When an attacker connects to the switch enabled with DAI and sends bogus ARP packets, the switch detects the attacks based on the DHCP snooping entries and discards the bogus ARP packets. When both the DAI and packet discarding alarm functions are enabled on the switch, the switch generates alarms when the number of discarded ARP packets matching no DHCP snooping entry exceeds the alarm threshold.

Configure DAI.

1. Enable DAI globally.

```
[Quidway] arp anti-attack check user-bind enable
```

2. Enable DAI in VLAN 100.

```
[Quidway] vlan 100
[Quidway-vlan100] arp anti-attack check user-bind enable
```

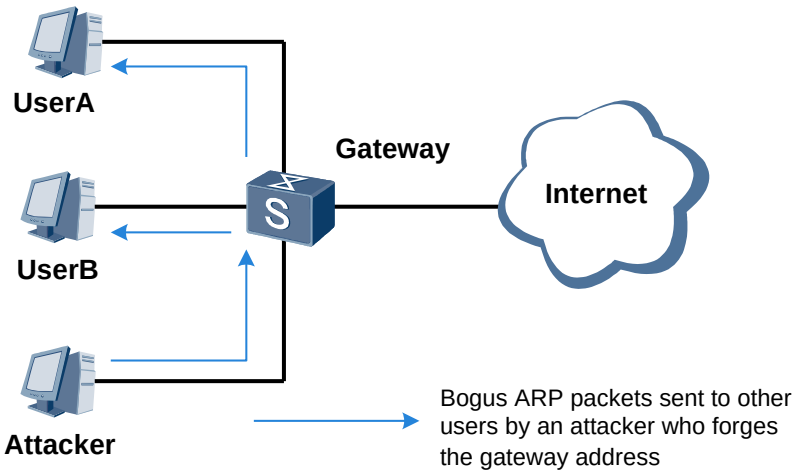
3. Enable DAI and the alarm function on GE1/0/1, and set the alarm threshold to 200.

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind enable
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind alarm enable
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind alarm threshold 200
```

1.2.8 ARP Gateway Anti-Collision

As shown in Figure 1-4, UserA and UserB connect to the gateway. An attacker forges the gateway address to send bogus ARP packets to UserA and UserB. UserA and UserB record incorrect ARP entries for the gateway. As a result, all traffic from UserA and UserB to the gateway is sent to the attacker and the attacker intercepts user information.

Figure 1-4 ARP gateway collision



To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.
- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the Virtual Router Redundancy Protocol (VRRP) group.

NOTE

A VRRP group, also called a virtual router, serves as the default gateway for hosts on a LAN. A virtual router has a virtual MAC address that is generated based on the virtual router ID. The virtual MAC address is in the format of 00-00-5E-00-01-{VRID}(VRRP). The virtual router sends ARP Reply packets using the virtual MAC address instead of the interface MAC address.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

You can run the following command to enable ARP gateway anti-collision globally:

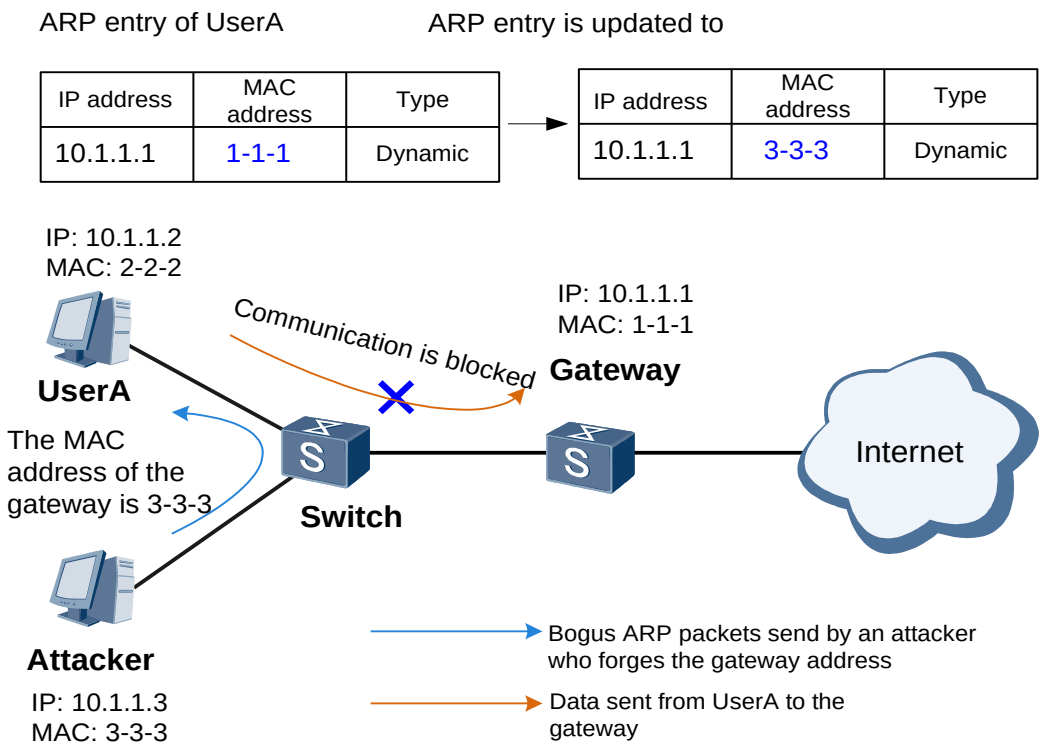
```
[Quidway] arp anti-attack gateway-duplicate enable
```

In addition, you can enable gratuitous ARP packet sending on the device to send correct gratuitous ARP packets. The gratuitous ARP packet is broadcast to all users so that incorrect ARP entries are corrected.

1.2.9 Gratuitous ARP Packet Sending

As shown in Figure 1-5, an attacker forges the gateway address to send a bogus ARP packet to UserA. UserA then records an incorrect ARP entry for the gateway. As a result, the gateway cannot receive packets from UserA.

Figure 1-5 Bogus gateway attack



To avoid the preceding problem, deploy gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

Gratuitous ARP packet sending can be enabled globally or on a VLANIF interface. If gratuitous ARP packet sending is enabled globally and on a VLANIF interface simultaneously, the configuration on the VLANIF interface takes precedence over the global configuration.

Configure gratuitous ARP packet sending.

1. Enable gratuitous ARP packet sending globally and set the interval for sending gratuitous ARP packets to 100 seconds.

```
[Quidway] arp gratuitous-arp send enable
[Quidway] arp gratuitous-arp send interval 100
```

2. Enable gratuitous ARP packet sending on VLANIF 10 and set the interval for sending gratuitous ARP packets to 100 seconds.

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp anti-attack gratuitous-arp drop
[Quidway-Vlanif10] arp gratuitous-arp send interval 100
```

1.2.10 ARP Packet Validity Check

This function allows the device to filter out packets with invalid MAC addresses or IP addresses. The device checks validity of an ARP packet based on each or any combination of the following items:

- Source MAC address: The device compares the source MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.
- Destination MAC address: The device compares the destination MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.
- IP address: The device checks the source and destination IP addresses in an ARP packet. If the source or destination IP address is all 0s, all 1s, or a multicast IP address, the device discards the packet as an invalid packet. The device checks both the source and destination IP addresses in an ARP Reply packet but checks only the source IP address in an ARP Request packet.

You can run the following command to enable ARP packet validity check base on the source and destination MAC addresses:

```
[Quidway] arp anti-attack packet-check sender-mac dst-mac
```

1.2.11 ARP Learning Triggered by DHCP

When there are a large number of DHCP users, the device needs to learn many ARP entries and age them. This affects device performance.

ARP learning triggered by DHCP prevents this problem on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface. Ensure that DHCP snooping has been enabled before using ARP learning triggered by DHCP.

You can run the following commands to enable ARP learning triggered by DHCP on VLANIF 10.

```
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp learning dhcp-trigger
```

You can also deploy DAI to prevent ARP entries of DHCP users from being modified maliciously.

1.2.12 ARP Proxy on a VPLS Network

To prevent bogus ARP packets at the PW side from being broadcast to the AC side on a VPLS network, enable ARP proxy and DHCP snooping over VPLS on a PE.

ARP packets at the PW side are sent to the master control board to process.

- If the ARP packets are ARP Request packets and the destination IP addresses in the packets match DHCP snooping binding entries, the device constructs ARP Reply packets based on the DHCP snooping binding entries and sends them to the requester at the PW side.
- If the ARP packets are not ARP Request packets or the destination IP addresses in the packets match no DHCP snooping binding entry, the device forwards these ARP packets.

You can run the following commands to enable ARP proxy on a VPLS network:

```
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping over-vpls enable
[Quidway] arp over-vpls enable
```

1.3 Applications

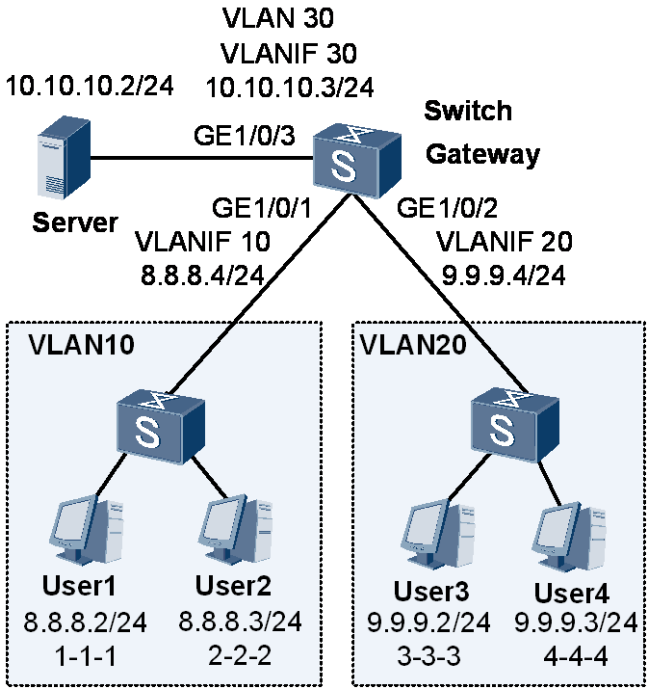
1.3.1 Example for Configuring ARP Security Functions

As shown in **Figure 1-6**, the switch functioning as the gateway connects to a server using GE1/0/3 and connects to four users in VLAN 10 and VLAN 20 using GE1/0/1 and GE1/0/2. The following ARP threats exist on the network:

- Attackers send bogus ARP packets or bogus gratuitous ARP packets to the switch. ARP entries on the switch are modified, leading to packet sending and receiving failures.
- Attackers send a large number of IP packets with unresolvable destination IP addresses to the switch, leading to CPU overload.
- User1 sends a large number of ARP packets with fixed MAC addresses but variable IP addresses to the switch. As a result, ARP entries on the switch are exhausted and the CPU is insufficient to process other services.
- User3 sends a large number of ARP packets with fixed IP addresses to the switch. As a result, the CPU of the switch is insufficient to process other services.

The administrator wants to prevent the preceding ARP flood attacks and provide users with stable services on a secure network.

Networking for configuring ARP security functions



The configuration roadmap is as follows:

1. Configure strict ARP learning and ARP entry fixing to prevent ARP entries from being modified by bogus ARP packets.
2. Configure gratuitous ARP packets discarding to prevent ARP entries from being modified by bogus gratuitous ARP packets.
3. Configure rate limit on ARP Miss messages based on the source IP address. This function defends against attacks from ARP Miss messages triggered by a large number of IP packets with unresolvable IP addresses (ARP Miss packets). At the same time, the switch must have the capability to process a large number of ARP Miss packets from the server to ensure network communication.
4. Configure ARP entry limit and rate limit on ARP packets based on the source MAC address. These functions defend against ARP flood attacks caused by a large number of ARP packets with fixed MAC addresses but variable IP addresses and prevent ARP entries from being exhausted and CPU overload.
5. Configure rate limit on ARP packets based on the source IP address. This function defends against ARP flood attacks caused by a large number of ARP packets with fixed IP addresses and prevents CPU overload.

Configuration file of Switch

```
#
vlan batch 10 20 30
#
arp learning strict
#
arp-miss speed-limit source-ip 10.10.10.2 maximum 40
arp speed-limit source-ip 9.9.9.2 maximum 10
```

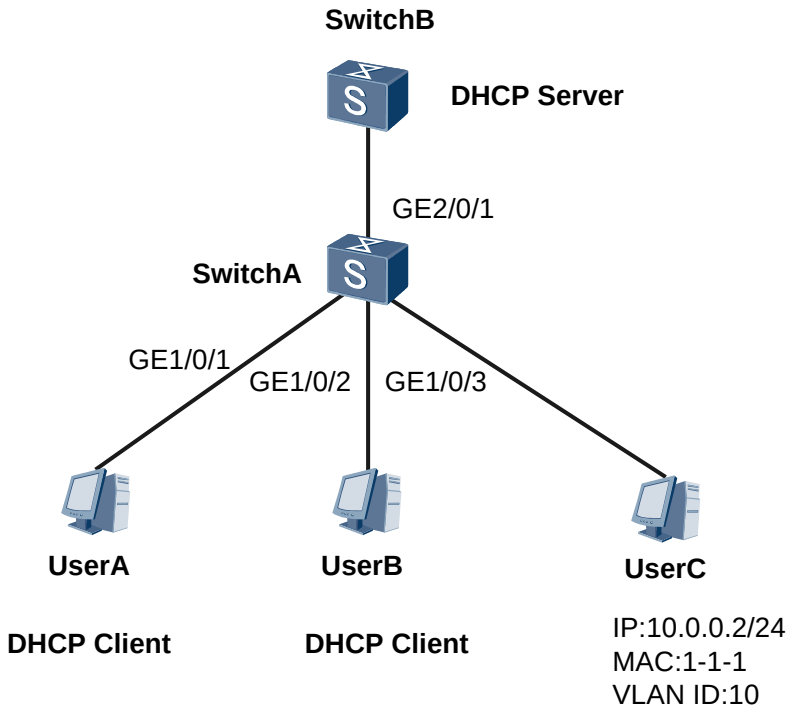
```
arp speed-limit source-mac 0001-0001-0001 maximum 10
arp anti-attack entry-check fixed-mac enable
arp anti-attack gratuitous-arp drop
#
arp-miss speed-limit source-ip maximum 20
#
interface Vlanif10
 ip address 8.8.8.4 255.255.255.0
#
interface Vlanif20
 ip address 9.9.9.4 255.255.255.0
#
interface Vlanif30
 ip address 10.10.10.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp-limit vlan 10 maximum 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

1.3.2 Example for Configuring Defense Against ARP MITM Attacks

As shown in **Figure 1-7**, SwitchA connects to the DHCP server using GE2/0/1, connects to DHCP clients UserA and UserB using GE1/0/1 and GE1/0/2, and connects to UserC configured with a static IP address using GE1/0/3. GE1/0/1, GE1/0/2, GE1/0/3, and GE2/0/1

on SwitchA all belong to VLAN 10. The administrator wants to prevent ARP MITM attacks and theft on authorized user information, and learn the frequency and range of ARP MITM attacks.

Networking diagram for defending against ARP MITM attacks



The configuration roadmap is as follows:

1. Enable DAI so that SwitchA compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. This prevents ARP MITM attacks.
2. Enable packet discarding alarm function upon DAI so that SwitchA collects statistics on ARP packets matching no DHCP snooping binding entry and generates alarms when the number of discarded ARP packets exceeds the alarm threshold. The administrator learns the frequency and range of the current ARP MITM attacks based on the alarms and the number of discarded ARP packets.
3. Enable DHCP snooping and configure a static DHCP snooping binding table to make DAI take effect.

Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 10
#
dhcp enable
#
```

```
dhcp snooping enable
user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface
GigabitEthernet1/0/3 vlan 10
#
vlan 10
 dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet1/0/3
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 dhcp snooping trusted
#
return
```

1.4 Troubleshooting Cases

1.4.1 Network Service Interruption of Authorized Users Caused by ARP Entry Modification

Common Causes

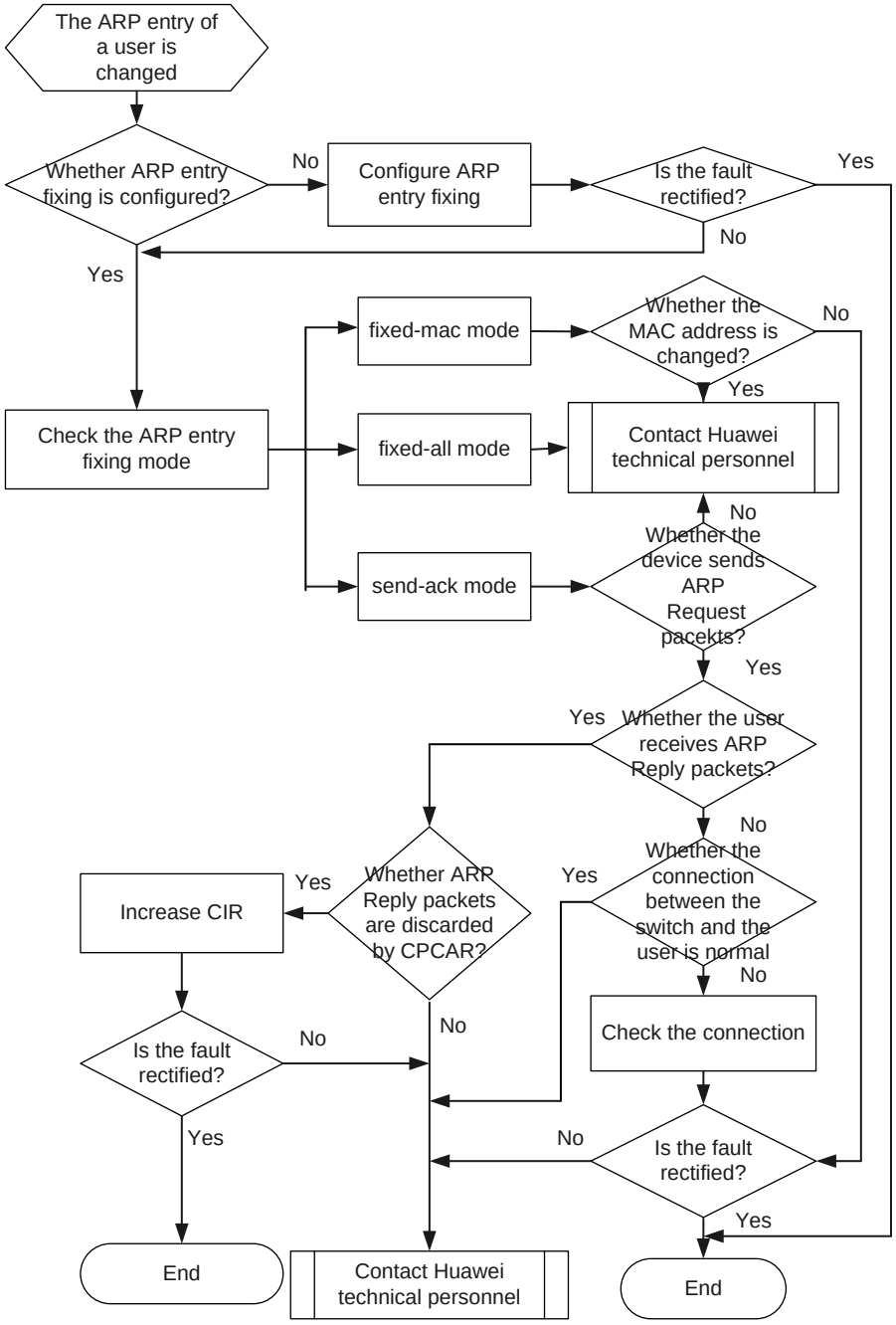
This fault is commonly caused by:

- An attacker sends bogus ARP packets to modify the ARP entry of the authorized user.

Diagnosis Process

An authorized user is disconnected from the Internet, but the links and routes are normal. The possible cause is that an attacker sends bogus ARP packets to modify the ARP entry of the user on the gateway. As a result, this user is disconnected from the network. Figure 1-6 shows the troubleshooting flowchart for malicious modification to the ARP entry of an authorized user.

Figure 1-6 Troubleshooting flowchart for malicious modification to the ARP entry of an authorized user



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display arp anti-attack configuration entry-check** command on the switch to check whether ARP entry fixing is enabled.

- If the following information is displayed, ARP entry fixing is disabled.

```
ARP anti-attack entry-check mode: disabled
```

Run the **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable** command to enable ARP entry fixing.

NOTE

Before enabling ARP entry fixing, run the **reset arp interface vlanif** *vlan-id* command to delete the ARP entries learned by the user-side interface.

- If the mode of ARP entry fixing is set to **send-ack**, go to Step 2.
- If the mode of ARP entry fixing is set to **fixed-mac**, go to Step 3.
- If the mode of ARP entry fixing is set to **fixed-all**, go to Step 4.

Step 2 Perform the following steps to locate the fault in **send-ack** mode.

1. Capture packets on the user-side interface by configuring port mirroring to check whether ARP packets are exchanged. If the switch does not send any ARP request, go to Step 4.
2. If the switch sends ARP requests but does not receive any ARP Reply packet, check whether the network connection between the switch and the user is normal.
3. If the switch receives ARP Reply packets from the user, run the **display cpu-defend statistics packet-type arp-reply** command to check whether ARP Reply packets are discarded. If the number of discarded ARP Reply packets keeps increasing, the possible cause is that the rate of ARP Reply packets exceeds the Control Plane Committed Access Rate (CPCAR) limit. In this case, increase the committed information rate (CIR) using the **car** command.
4. If the fault persists, go to Step 4.

Step 3 Run the **display arp all** | **include** *ip-address* command to check the information modified in the ARP entry of the user.

If the interface number or VLAN ID is changed, you do not need to take any action because it is normal in **fixed-mac** mode. If the MAC address is changed, go to Step 4.

Step 4 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, logs, and alarms of the member switch

----End

Related Alarms and Logs

Related Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.2

Related Logs

None

1.4.2 Traffic Interruption Caused by ARP Attacks

Common Causes

This fault is commonly caused by:

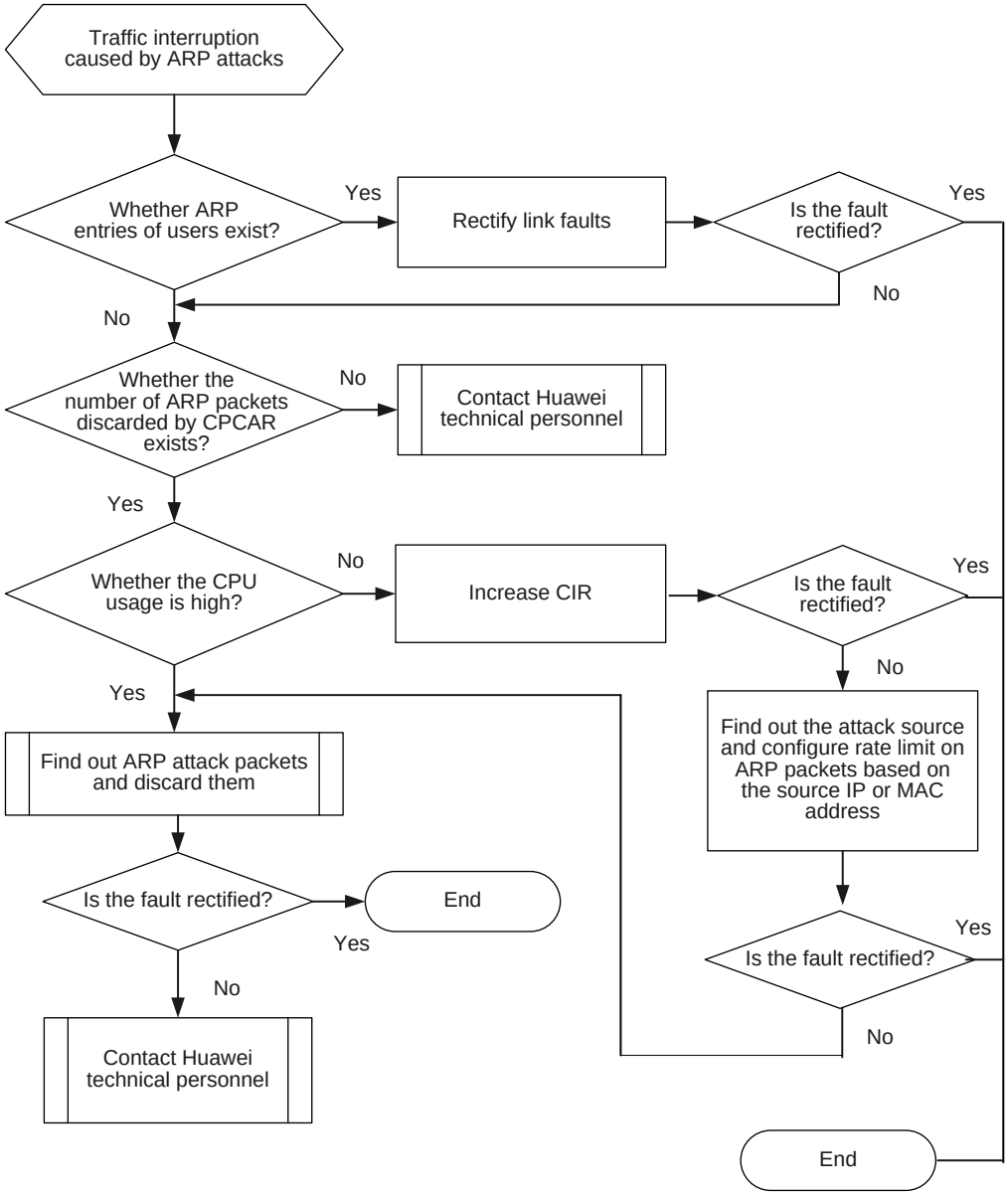
- An attacker sends a large number of bogus ARP Request packets, increasing the load of the destination network. If Layer 3 interfaces are configured on the switch, the ARP Request packets are sent to the CPU, leading to a high CPU usage. At the same time, traffic of authorized users may be interrupted and denial of service (DoS) attacks may also be initiated.

Diagnosis Process

The switch uses the CPCAR mechanism to limit the rate of ARP Request packets sent to the CPU. If an attacker sends a large number of bogus ARP Request packets, valid ARP Request packets are also discarded when the bandwidth limit is exceeded. Consequently, user traffic is interrupted.

Figure 1-7 shows the troubleshooting flowchart for traffic interruption caused by ARP attacks.

Figure 1-7 Troubleshooting flowchart for traffic interruption caused by ARP attacks



Troubleshooting Procedure

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Step 1 Run the **display arp all** command to check ARP entries of authorized users.

- If ARP entries of authorized users are displayed, the switch has learned the ARP entries, and traffic interruption is caused by a short link disconnection. In this case, rectify link faults.

- If no ARP entry is displayed, go to Step 2.

Step 2 Run the **display cpu-defend statistics packet-type arp-request** command to check the number of discarded ARP Request packets.

- If the number of discarded ARP requests is 0, no ARP Request packet is discarded. Go to Step 7.
- If the number of discarded ARP Request packets is not 0, the rate of ARP Request packets exceeds the CPCAR limit and excess ARP Request packets are discarded. ARP packets from authorized users may be discarded. Go to Step 3.

Step 3 Run the **display cpu-usage** command to check the CPU usage of the main control board.

- If the CPU usage is normal. Go to Step 4.
- If the CPU usage is high (for example, higher than 70%), the CPCAR value cannot be increased. Go to Step 6.

Step 4 Run the **car** command to increase the rate limit for ARP Request packets.

Run the **car** command in the attack defense policy view and apply the attack defense policy.

If the fault persists or the CPU usage is high after the fault is rectified, go to Step 5.

Step 5 Capture packets on the user-side interface, and find the attacker according to the source addresses of ARP Request packets.

If a lot of ARP requests are sent from a source MAC or IP address, the switch considers the source address as an attack source.

You can run the **arp speed-limit source-ip** [*ip-address*] **maximum** *maximum* command to reduce the maximum rate of ARP packets from a source IP address based on the actual network, or you can run the **arp speed-limit source-mac** [*mac-address*] **maximum***maximum* command to set the maximum rate of ARP packets from a source MAC address.

By default, rate limit on ARP packets based on the source IP address is enabled, and the maximum rate of ARP packets from the same source IP address is 30 pps. After the rate of ARP Request packets reaches this limit, the switch discards subsequent ARP Request packets. If the rate of ARP packets from each source MAC address is set to 0, the rate of ARP packets is not limited based on the source MAC address.

When the maximum rate of ARP packets from a source IP address or a source MAC address is set to a small value, for example, 5 pps:

- If the fault persists, go to Step 7.
- If the CPU usage is high after the fault is rectified, add the source address to the blacklist or configure a blackhole MAC address to discard ARP Request packets sent by the attacker. If the CPU usage is still high, go to Step 7.

Step 6 Capture packets on the user-side interface, and find the attacker according to the source addresses of ARP Request packets.

If a lot of ARP Request packets are sent from a source address, the switch considers the source address as an attack source. Then add the source address to the blacklist or configure a blackhole MAC address to discard ARP Request packets sent by the attacker.

If the fault persists, go to Step 7.

Step 7 Collect the following information and contact Huawei technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, logs, and alarms of the member switch

----End

Related Alarms and Logs

Related Alarms

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.3
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.4
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.5
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.6
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.7
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.11

Related Logs

None

1.5 References

The following table lists the references of this document.

Document	Description	Remarks
RFC826	Ethernet Address Resolution Protocol	-
RFC903	Reverse Address Resolution Protocol	-
RFC1027	Using ARP to Implement Transparent Subnet Gateways	-
RFC1042	Standard for the Transmission of IP Datagrams over IEEE 802 Networks	-